***To be completed by the Principal.***

|  |
| --- |
| Order Object |

The Contractor shall perform the following services for the Principal:

Use of softgarden's applicant management system

The scope, type and purpose of the collection, processing and/or use of personal data by the Contractor for the Principal are described in the following Contract:

<Enter description/date>

- Collection of personal data

- Processing/saving of personal data at the computer centers described hereafter

- Use of data for communication with applicants

- Presentation of data to the Principal, structured presentation of candidate data

- If applicable, further storage of candidate data following approval in the talent pool, deletion of the data   
 6 months after the completion of the application process

- If a candidate does not consent to further storage of his data in the talent pool

- Assessment of applicant data for reports

**Order Duration**

The duration of this order corresponds to the duration of the above-stated contract.

|  |
| --- |
| Principal's Persons With the Authority to Issue Directives |

The Principal hereby authorizes the following persons to issue directives to the Contractor: *Please state name and function*



|  |
| --- |
| Principal's Data Protection Officer |

The Principal's data protection officer is: *Please state name and contact details!*



|  |
| --- |
| Representatives of Data Subjects |

The following groups are data subjects regarding the processing for the order:

* Prospective clients
* Recruiters
* Applicants when using the offer on the websites

|  |
| --- |
| Type of Data/Data Categories |

The following data or data categories constitute the object of the collection, processing and/or use of personal data:

* Contact data of the applicant (street, house number, ZIP code, city, country, state, telephone number, fax number, mobile number, email address)
* Personal data of the applicant (title, academic title, first name, last name, nationality, date of birth)
* Application letter
* Work experience of the applicant (company, industry, position, career level, type of employment, company size, website, type of company, from, until, description)
* Education / training of the applicant (from, until, (higher) educational institution, field, degree, main focus, language skills (language, level))
* Application picture of the applicant
* CV
* Driver's license of the applicant
* Willingness of the applicant to travel
* Other annexes and information in accordance with the existing service contract
* IP address

***To be completed by the Contractor***

|  |
| --- |
| Data Processing Locations |

The Contractor will process data at the following locations:

**Location of the Contractor's offices:**

softgarden e-recruiting GmbH

Tauentzien Strasse 14

10789 Berlin, Germany

**If applicable, Contractor's computer center locations:**

* myLoc managed IT AG Am Gatherhof 44 40472 Duesseldorf Germany
  + Service provider's computer center locations:
    - Am Gatherhof 44 40472 Duesseldorf Germany
    - In der Steele 40599 Duesseldorf Germany
* PlusServer GmbH Welser Strasse 14 51149 Cologne Germany
  + Service provider's computer center locations:
    - In der Steele 40599 Duesseldorf Germany
    - Welser Strasse 14 51149 Cologne Germany

Changes to the locations where the Principal's data is processed and/or used require the Principal's written permission.

|  |
| --- |
| Contractor's Persons Who May Receive Directives |

The Contractor authorized the following persons to receive directives from the Principal:

* Mr. Philipp Mager, Vice President Service

softgarden e-recruiting GmbH, Tauentzien Strasse14, 10789 Berlin, Germany

|  |
| --- |
| Contractor's Data Protection Officer |

The Contractor's data protection officer is:

Marco Tessendorf, procado Consulting, IT- & Medienservice GmbH

Warschauer Strasse 58a

10243 Berlin, Germany

|  |
| --- |
| Subcontractor Agreements |

At the time of Contract conclusion, sub-contractual relationships exist with the following subcontractors providing assisting services under the main agreement (e.g. computer centers):

|  |  |
| --- | --- |
| Subcontractor's name and address | Order contents (brief description of performed services) |
| myLoc managed IT AG Am Gatherhof 44  40472 Duesseldorf Germany | Co-location and managed services  Rack rental and providing of   * Redundant firewalls and load balancers * Redundant power supply via emergency power generator, USP(n+1 redundancy) and A/B supply to server racks * Multiple redundant IP connections and redundant network infrastructure * Separate backup and administration networks * Redundant, energy-efficient cooling (n+1 redundancy) * Dedicated servers * SSL certificates * Replacement of defective server hardware * Other support services for all server systems (e.g., as part of proactive monitoring) |
| PlusServer GmbH  Welser Strasse 14  51149 Cologne Germany |

Subsequent commissioning of additional subcontractors requires the Principal's **prior written permission**.

**Subcontractors based in Germany/the EU/the EEA**

The Contractor confirms that he concluded separate data protection agreements with the stated subcontractors in accordance with Art. 28(3) of the General Data Processing Regulation and that they correspond to the Contractual data protection regulations between the Principal and the Contractor.

Please state the contract type (e.g., EU standard agreement):

* Agreement on commissioned data processing or order processing:
  + myLoc managed IT AG
  + PlusServer GmbH

|  |
| --- |
| **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:

|  |
| --- |
| **Confidentiality** |

**Entrance Controls**

The Contractor ensures that unauthorized persons may not access his offices, server rooms and archives. This is achieved through:

|  |  |
| --- | --- |
| **Contractor's Duties**  (Offices (O) and computer center (CC)[[1]](#footnote-1) of the Contractor) | Remarks |
| Central reception area (reception) | CC & O |
| Entrance with an alarm system with security service | CC |
| Entry using coded keys issued only to authorized persons | CC & O |
| Determination of entrance authorization, including documentation of employees and non-company persons (maintenance staff, visitors) / porter, security | CC |
| Non-company persons, maintenance staff and visitors may only enter if accompanied by an employee | CC & O |
| Legitimation of persons with entrance authorization (key, PIN code) | CC & O |
| Withdrawal of entrance-means after expiration of authorization | CC & O |
| Security areas with various types of entrance authorization | CC & O |

**Admission Control**

The Contractor prevents unauthorized use of the EDP systems.   
This is achieved through:

|  |  |
| --- | --- |
| **Contractor's Duties**  (Offices (O) and computer center (CC) of the Contractor) | Remarks |
| Creation of user accounts per user | CC & O |
| Authentication of persons authorized for data processing through a password procedure (using special characters, minimum length of 8 characters, passwords changed after 90 days (CC) or 180 days (O)) | CC & O |
| Automatic user account blocking after repeated incorrect entries of access data | CC |
| Automatic workplace blocking following inactivity | CC & O |
| Immediate authorization blocking when employees leave the company (guidelines/work directives) | CC & O |
| Regular authorization validity controls | CC & O |
| Use of lockable cabinets for storing paper files | CC & O |
| Secure transfer or authentication credentials on the network using TLS/HTTPS, SSH, VPN (IPSec, openVPN) | CC & O |
| Access identifiers for workplace computers are blocked manually in case of prolonged absence of an employee (30 days) and must be unblocked manually by the IT administration when the employee returns. | CC & O |

**Retrieval Controls**

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:

|  |  |
| --- | --- |
| **Contractor's Duties**  (Offices (O) and computer center (CC) of the Contractor) | Remarks |
| Determination of data access authorization (creation of an authorization concept) | CC & O |
| Determination of knowledge, input, editing or deletion authorization for data processed by the Contractor as part of an order | CC & O |
| Regular access, input, editing and deletion controls | CC |
| Disposal of data carriers no longer needed in accordance with data protection regulations (guidelines/work directives) | CC & O |
| Written rules for copying data (IT security guidelines/work directive) | CC & O |
| Granting of minimal authorization (need-to-know principle) | CC & O |
| No granting of generic group identifiers or passwords | CC & O |
| Prevention of functional concentration—functional separation of administrative tasks among various qualified persons | CC & O |
| Keeping a log of the history of administrative changes | CC |

**Separation Controls**

The Contractor ensures that data collected for different purposes can be processed separately. There is no need for physical separation; logical separation of data is sufficient. This is achieved through:

|  |  |
| --- | --- |
| **Contractor's Duties**  (Offices (O) and computer center (CC) of the Contractor) | Remarks |
| Labeling collected data (file number, ID, client/transaction number) | CC & O |
| Logical separation of data processed for different clients, functional separation/production/test | CC & O |
| The personal data of the respective clients is logically separated through assignments to the respective user accounts. | O |

|  |
| --- |
| **Integrity** |

**Transfer Controls**

The Contractor 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:

|  |  |
| --- | --- |
| **Contractor's Duties** (Offices (O) and computer center (CC) of the Contractor) | Remarks |
| Determining the persons authorized to make transmissions of or to transport (electronic, manual) data | CC & O |
| Reviewing the data's completeness after transport, transmission or storage | CC |
| Implementation of security gateways at network interconnection points | CC & O |
| Use of a recognized encryption process that encrypts all communication between the applicant and the Contractor's servers | CC & O |
| Incoming and outgoing data streams are filtered through a modern, cascaded firewall solution | CC & O |
| If data carriers are sent through transport companies, these data carriers will only be forwarded following the authentication of the transport company. | CC & O |
| Paper and data carriers with personal data are disposed of by a qualified disposal company in accordance with data protection regulations. | CC & O |
| The complete and permanent deletion in accordance with data protection regulations of data or data carriers with personal data is documented. These records are saved for at least 12 months in a revision-proof manner. | CC & O |

**Input Controls**

The Contractor 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:

|  |  |
| --- | --- |
| **Contractor's Duties**  (Offices (O) and computer center (CC) of the Contractor) | Remarks |
| Documenting access authorization (work directives, access groups and access authorization) | CC & O |
| Recording activities as part of the order | CC & O |
| Sample-based controls and reviewing record data for misuse | CC |
| A history of all users who use according application programs to process personal data is kept that records which users performed which action when for actions that modify personal data. | O |

|  |
| --- |
| **Availability and Resilience** |

**Availability Controls**

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

|  |  |
| --- | --- |
| **Contractor's Duties**  (Offices (O) and computer center (CC) of the Contractor) | Remarks |
| Uninterruptible power supply (UPS) | CC & O |
| Virus protection (on workplaces) | CC & O |
| Virus protection (on servers) | CC & O |
| Firewall | CC & O |
| Emergency plan | CC |

**Restorability**

The Contractor 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:

|  |  |
| --- | --- |
| **Contractor's Duties**  (Offices (O) and computer center (CC) of the Contractor) | Remarks |
| Backup process (daily change backup, weekly full backup) | CC & O |
| Storage of backup files in data security cabinets, safes and in other fire compartments | CC & O |

|  |
| --- |
| **Regular Review, Assessment and Evaluation Process** |

**Data Protection Management**

The Contractor guarantees a process for regular reviews and assessments of the effectiveness of the technical and organizational protective measures. This is achieved through:

|  |  |
| --- | --- |
| **Contractor's Duties**  (Offices (O) and computer center (CC) of the Contractor) | Remarks |
| Instructing all employees about and subjecting them to data protection secrecy obligations (Art. 28(3) Letter b of the General Data Protection Regulation) | CC & O |
| Regular data protection level reviews by the data protection group | CC & O |
| Requiring third parties to sign a non-disclosure agreement | CC & O |
| Applying and documenting the four-eyes principle for functional overlaps due to organizational reasons | O |
| Defined rules of representation within functional groups | O |

**Appropriate Level of Security Assessment (Art. 32(2) of the General Data Protection Regulation)**

The Contractor guarantees documented assessments of the appropriateness of security levels regarding risks—especially destruction, loss, editing or unauthorized disclosure or access—for the processing of personal data processed on commission.   
This is achieved through:

|  |  |
| --- | --- |
| **Contractor's Duties**  (Offices (O) and computer center (CC) of the Contractor) | Remarks |
| Performance of risk analyses for the processing of personal data | CC & O |
| Creation of need-for-protection categories | CC & O |
| Basing processes on "privacy by design & default" | O |
| Performing data protection impact assessments if necessary | CC & O |

**Order Controls (Art. 32(3 & 4) of the General Data Protection Regulation)**

The Contractor guarantees that personal data processed on commission will only be processed in accordance with the Principal's directives and for the fulfillment of the Contractually defined usage purpose.

The Principal may prove this through a process under Art. 40 or through an approved certification process under Art. 42 of the General Data Protection Regulation. If certification is not submitted, proof may be provided through:

|  |  |
| --- | --- |
| **Contractor's Duties**  (Offices (O) and computer center (CC) of the Contractor) | Remarks |
| Clear agreements with subcontractors | CC & O |
| Formalizing the awarding of orders (forms) | CC & O |
| Regular activity controls | CC |
| The Principal's persons authorized to issue directives and the persons who may receive directives are contractually defined and directives are only issued in writing. | CC & O |
| The Contractor notifies the Principal without undue delay about any severe operative disruptions, discovered errors or other irregularities when handling the Principal's data. | CC & O |
| Orders are recorded as support tickets (minimum information: client, action/partial order, exact specification of processing steps/parameters, persons who handle requests, appointments and, if applicable, recipients) where performed work is documented. Support ticket numbers and client orders are assigned uniquely. | CC & O |
| The Contractor notifies the Principal without undue delay about any severe operative disruptions, discovered errors or other irregularities when handling the Principal's data. | O |

|  |
| --- |
| **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 |

1. [↑](#footnote-ref-1)