|  |  |  |
| --- | --- | --- |
| On behalf of |  | processed by the |
|  |  | softgarden e-recruiting GmbH  Tauentzien Strasse 14  10789 Berlin, Germany |
| - hereafter referred to as the "**Principal**" - |  | - hereafter referred to as the "**Contractor**" - |

collectively referred to hereafter as **Contract Partners**.

**Preamble**

This Data Protection Contract shall regulate the protection of personal data when processed on commission.

If a controller (Principal) has personal data processed by another controller (Contractor), Art. 28 of the General Data Protection Regulation requires the conclusion of a written contract for the commissioned data processing. In addition to storage, edits, transfers, blocking and deletion, data processing also includes the providing of data for third-party inspections or retrieval.

The Principal shall be responsible for processing the personal data in accordance with data protection regulations. Under Art. 29 of the General Data Protection Regulation, the Contractor may only process the data if directed to do so by the Principal. In case of violations by the Contractor, e.g., by determining purposes of the processing himself, under Art. 28(10) of the General Data Protection Regulation, the Contractor will become the controller for the data subject.

Therefore, the Contract Parties shall agree to the following:

# Object of this Order

The object of the order shall follow from the agreement described in **Annex 1**. This agreement, hereafter referred to as the "main agreement" shall be referred to hereafter.

# Order Content Specification

1. The specification of the order contents, the data and of the circle of persons affected by the data collection, processing or use can be found in **Annex 1** to this Data Protection Contract.
2. The data shall only be processed and used in the territory of the Federal Republic of Germany, in a Member State of the European Union or in another state party to the EEA Agreement. Any outsourcing to a third country shall require the Principal's prior written permission and may only be performed if the special requirements of Art. 44 to Art. 50 of the General Data Protection Regulation are fulfilled.

# Technical and Organizational Measures

1. Before the processing, the Contractor must document the implementation of the technical and organizational described prior to the awarding of the order, especially regarding the specific performance of the order, and submit the documentation to the Principal for review. Following the Principal's acceptance, the documented measures shall form the basis of the order. If the review/an audit by the Principal finds need for adjustments, these must be implemented mutually.
2. The measures to be taken must ensure the confidentiality, integrity, availability and resilience of the systems and services for the processing of personal data; measures for quickly restoring the availability of and access to personal data in case of physical or technical incidents and measures that guarantee the effectiveness of these measures through regular reviews, assessments and evaluations (for specifics, see **Annex 2**).
3. 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.
4. The Principal may, at any time, review or have the concluded agreement reviewed by a competent third party regarding the technical and organizational measures.

# Authorization, Data Blocking and Erasure

1. The Contractor may only rectify, erase or block the data processed on commission in accordance with the Principal's directives. If a data subject contacts the Contractor directly for the rectification or erasure of his data, the Contractor must forward this request to the Principal without undue delay.
2. If covered by the service scope, the erasure concept, the "right to be forgotten" and the right to rectification, access, "data portability" and to object must be ensured directly by the Contractor in accordance with documented directives of the Principal.
3. Any actions under Section 4 of this Contract must be recorded and submitted to the Principal in writing.

# Duties of the Contractor

The Contractor shall have the following duties:

1. If required under Art. 37 *et seq*. of the General Data Protection Regulation, the appointment of a data protection officer whose contact details must be provided to the Principal to allow the Principal contact the data protection officer directly (**Annex 1**).
2. The duty to subject all persons who may access the Principal's data for the order to confidentiality obligations (Art. 28(3) Sentence 2 Letter b of the General Data Protection Regulation) and to inform these persons about the data protection regulations of the order and about the subjection to directives and the purposes for the processing.
3. The duty to implement and maintain any technical and organizational measures required for this order in accordance with Art. 32 of the General Data Protection Regulation (see Art. 28(3) Sentence 2 Letter c of the General Data Protection Regulation).
4. The duty to take any required technical and organizational measures to allow the Principal to comply with the data subject rights under Chapter III of the General Data Protection Regulation (information, access, rectification and erasure, data portability and to object and, in individual cases, automated decision-making) at any time during the legally required period (see Art. 28(3) Sentence 2 Letter e of the General Data Protection Regulation). For this, the Contractor must provide any required information to the Principal. This requires the Principal to have issued   
   a corresponding written directive to the Contractor and this assistance to not violate the Contractor's non-disclosure obligations to third parties. The Contractor shall reserve the right to pass on any costs incurred thereby to the Principal separately.
5. The duty to assist the Principal to comply with the obligations under Art. 32 to Art. 36 of the General Data Protection Regulation (data security measures, reporting infringements on the protection of personal data to supervisory authorities, notification in case of violations of the protection of personal data of data subjects, data protection impact assessments, prior consultation) (see Art. 28(3) Sentence 2 Letter f of the General Data Protection Regulation).
6. The duty to inform the Principal without undue delay about any control actions and measures by supervisory authorities (see Art. 31 & Art. 51 *et seq*. of the General Data Protection Regulation). This shall also apply if the competent authorities under Art. 83 & Art. 84 of the General Data Protection Regulation investigate the Contractor.
7. The Contractor must state in writing the intended location(s) of his offices or of the Principal's computer centers used for using the Principal's data for the order (**Annex 2**). Contractor informs the principal without delay of any change or new signing in regard to a subcontractor. Principal is allowed to raise an objection against any of these changes (Art. 28 Sec. 2 GDPR). Such objection may not be issued without significant reason (e.g. (planed) involvement of a principal´s competitor, former known data privacy violations). Such notice in regard to a change in subcontractors has to be issued within two weeks prior to the change of subcontractors to the principal´s instructor. If principal does not issue any objection within two weeks after notice, the principal´s permission is deemed as given. The Contractor must ensure that third-party access to the Principal's data processed at the Contractor's locations stated in Annex 2 is excluded.
8. The Contractor may state the person(s) authorized to receive the Principal's directives to the Principal. Persons of the Contractor who may issue directives must be documented in **Annex 2**.
9. In case of a data transfer to an unsafe third country, the transfer must be made permissible using the legal options provided by the European Commission.

# Subcontractual Relationships

The inclusion of subcontractors in the processing or use of the Principal's personal data shall be permitted if the following requirements are met:

1. The inclusion of subcontractors who directly use the Principal's data on the Contractor's behalf is documented in writing in **Annex 1**. For the named subcontractors within Annex 1 Principal´s consent is deemed as given by singing of this contract. Use in the sense of this Contract includes read access to personal data and any further activities.
2. Agreements concluded between the Contractor and subcontractors must correspond to the data protection regulations of the Contractual relationship between the Principal and the Contractor. Proof of the conformity of such agreements must be submitted to the Principal in writing on request.
3. Contractor informs the principal without delay of any change or new signing in regard to a subcontractor. Principal is allowed to raise an objection against any of these changes (Art. 28 Sec. 2 GDPR). Such objection may not be issued without significant reason (e.g. (planed) involvement of a principal´s competitor, former known data privacy violations). Such notice in regard to a change in subcontractors has to be issued within two weeks prior to the change of subcontractors to the principal´s instructor. If principal does not issue any objection within two weeks after notice, the principal´s permission is deemed as given. If a subcontractor uses this data in an unsafe third country, the legal means provided by the European Commission for ensuring an adequate level of data protection must be applied.

Third-party services utilized by the Contractor as ancillary services for assistance with order performance shall not be considered sub-contractual relationships in the sense of this regulation. For example, this shall include cleaning services, pure telecommunications services that do not specifically relate to services performed by the Contractor for the Principal, mailing or courier services, transport services or security services. The Contractor must ensure that appropriate precautions and technical and organizational measures are taken to guarantee the protection of personal data, including for ancillary services. IT system maintenance and inspection shall represent sub-contractual relationships requiring permission if IT systems needed for the performance of services for the Principal are involved.

# Control Rights of the Principal

1. The Principal shall have the right to perform order controls at his own expense, during regular business hours in consultation with the Contractor without disrupting business operations or to have such order controls performed by inspectors to be appointed in individual cases if they are not competitors of the Contractors and if the Contractor has no legitimate objections. On request, the Contractor shall provide any information and corresponding proof to the Principal required for fulfilling his order control obligations.
2. For the Principal's control obligations under Art. 28(1) of the General Data Protection Regulation prior to data processing and during the duration of the order, the Contractor shall ensure that the Principal can review compliance with the implemented technical and organizational measures. For this, the Contractor shall demonstrate the implementation of the technical and organizational measures in accordance with Art. 32 of the General Data Protection Regulation to the Principal on request. Proof of the implementation of such measures that only concern the respective order may also be provided through current certificates, reports or excerpts thereof (e.g., from an auditor, audit, data protection officer, IT security department, data protection auditors, quality auditors) or suitable certification for an IT security or data protection audit (e.g., under BSI IT-Grundschutz) or through adherence to an approved code of conduct (so-called BCR). The Contractor shall reserve the right to pass on any costs incurred thereby to the Principal separately.
3. If the Principal discovers errors or irregularities regarding data protection regulations, the Principal shall notify the Contractor about this without undue delay.

# Contractor Violation Reports

1. The Contractor shall notify the Principal if the Contractor or his employees violate any data protection regulations applicable to the Principal's data or to the specifications of the order.
2. It is known that under Art. 33 of the General Data Protection Regulation, third parties may have to be notified if personal data concerning them may have been lost or transmitted unlawfully or if knowledge of the personal data may have been obtained unlawfully. Therefore, such incidents must be reported to the Principal without undue delay, irrespective of their cause. This shall also apply in case of severe operational disruptions and suspicions of other violations of personal data protection regulations or of other irregularities when handling the Principal's personal data. The Contractor must in consultation with the Principal, take appropriate measures for securing the data and reducing any disadvantageous consequences for the data subjects. The Contractor must assist the Principal with the fulfillment of any obligations under Art. 33 or Art. 34 of the General Data Protection Regulation to which the Principal may be subject.

# Principal's Authority to Issue Directives

1. Data shall be treated exclusively in accordance with the concluded agreements and the Principal's directives (see Art. 28(3) Sentence 2 Letter a) of the General Data Protection Regulation). As part of the order description under this Contract, the Principal shall reserve an extensive right to issue directives on the type, scope and procedure for data processing which may be further specified through individual directives. Changes to the processing object and procedural changes must be jointly coordinated and documented in writing. The Contractor may only provide information to third parties or data subjects with the Principal's prior written permission.
2. The Principal shall confirm any oral directives in writing or by email (in text form) without undue delay. The Contractor may not use the data for any other purposes and may especially not provide the data to third parties. Copies or duplicates of the data may not be created without the Principal's knowledge. However, this shall not apply to backup copies required for ensuring orderly data processing or to data necessary for compliance with legal storage obligations.
3. The Principal may appoint persons with the authority to issue directives. If the Contractor processes sensitive data for the Principal, the Principal shall directly appoint the persons with the authority to issue directives who must legitimize themselves when exercising their authority. The Principal's persons with the authority to issue directives shall be documented in **Annex 1**. Any changes to the Principal's or Contractor's persons with the authority to issue directives shall be reported in writing and recorded in **Annex 1**.
4. The Contractor must notify the Principal in accordance with Art. 28(3) Sentence 3 of the General Data Protection Regulation without undue delay if the Contractor believes that a directive of the Principal violates data protection regulations. The Contractor may suspend the performance of the respective directive until the directive is confirmed or changed by the Principal.

# Data Deletion and Data Carrier Returning When Activities End

1. After the completion of the processing or after this Contract ends at the latest, the Contractor must hand over any documents, processing or usage results, personal data copied or produced for service performance and any other confidential data related to the order and in the Contractor's possession to the Principal or delete or destroy them in coordination with the Principal and in compliance with data protection regulations. Test and scrap material must be destroyed in compliance with data protection regulations or handed over to the Principal without undue delay. This obligation shall apply to the same measure to any commissioned subcontractors. Data and copies thereof required for the fulfillment of liability and guarantee claims shall remain unaffected.
2. The Contractor must save any documentation used for the order or for orderly data processing or that may not be deleted for legal reasons, e.g., due to storage obligations, after this Contract ends for the respective storage periods and must be safely deleted thereafter. The Principal must be   
   notified about the type and scope of the data saved under Subsection (1) or (2). The Contractor may hand over these data to the Principal for his relief when this Contract ends.
3. The Contractor must confirm the safe deletion or safe destruction of any documents in his possession to the Principal in writing after this Contract ends.

# Contract Duration and Termination

1. The Contractual relationship shall enter into effect upon being signed by both Contract Partners and shall be concluded indefinitely, at least for the same duration as the main contract's duration. Ordinary termination rights shall correspond to those under the main agreement.
2. To supplement the main agreement, it shall be regulated that violations of legal or Contractual data protection regulations by the Contractor shall represent a compelling reason for exercising the extraordinary termination rights reserved under the main agreement for the Principal. Accordingly, the Principal may terminate the main agreement for a compelling reason without notice.
3. If the basis for Contract fulfillment is significantly changed or removed due to legal or rights changes or intervention or other measures by supervisory authorities, both parties shall be entitled to Contractual adjustments to the new circumstances to the extent possible and reasonable for both parties. If Contractual adjustments are not possible or reasonable for a party, this shall represent a compelling reason for both parties for termination without notice. Subsection (2) shall remain unaffected.

# Final Provisions

1. Should a regulation of this Contract be or become invalid, the validity of the remainder of the Contract shall remain affected. In such cases, a regulation that most closely approximates the intent of the invalid regulation shall be agreed between the parties.
2. Changes or additions to this Contract, individual agreements or any parts thereof must be issued in written form. This shall also apply to any waiver of this written form requirement.
3. The defense of rights of retention in the sense of Section 273 of the German Civil Code [Bürgerliches Gesetzbuch, BGB] for the processed data and according data carriers shall be excluded.
4. The legal relationships of the Contract Partners shall be governed by the law of the Federal Republic of Germany under exclusion of the UN sales convention and under exclusion of any regulations under German law that refer to a legal system other than the German legal system.
5. For any disputes under or in relation to this Contract, the place of jurisdiction of the main   
   agreement shall apply as far as permissible.
6. If regulations of this Contract apply beyond the Contractual duration, these regulations shall   
   remain effective even after the Contract ends.
7. The included Annexes shall be essential parts of this Contract.

**Annex 1: Commissioned Data Processing Contract**

**Annex 2: Technical and Organizational Measure Determination Agreement**

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