Data Processing Addendum

How to get a binding Addendum: (1) Complete the signatory information below these instructions; (2) complete and sign in the signature box on page 6; (3) send the completed and signed DPA to SmartRecruiters as follows, either: (i) if you are a new customer, to your sales representative at SmartRecruiters, or (ii) if you are an existing customer, to legal@smartrecruiters.com.

This Data Processing Addendum (the "**Addendum**" or "**DPA**") is between ______________________________ ("**Customer**") located at ____, and the SmartRecruiters entity set forth in the Agreement (as hereinafter defined) ("**SmartRecruiters**"). Both Customer and SmartRecruiters are individually referred to as a "**Party**", and jointly referred to as the "**Parties**".

This Addendum has been pre-signed by the SmartRecruiters entity set forth above. Any hand-written or other changes to this Data Processing Addendum made without SmartRecruiters prior written approval will not be binding against SmartRecruiters. This Addendum is subject to the document signed between the Parties governing Customer's subscription to SmartRecruiters' software (the "**Agreement**"). If there is no Agreement between the Parties, executing this Addendum will have no force or effect between SmartRecruiters and the person or entity that countersigns this Addendum. This Addendum supersedes and replaces any earlier versions of the Addendum that may have been signed between the Parties.

1. Definitions.

Terms such as **"Controller**,**" "Data Subject**,**" "Personal Data**,**" "Process"** (including its variants) and **"Processor"** have the meanings given in the GDPR.

"**Agreement**" shall mean (i) the master subscription agreement or other subscription agreement between Customer and SmartRecruiters governing Customer's access to SmartRecruiters' software, and/or (ii) any service agreement between Customer and SmartRecruiters governing the provision of professional services by SmartRecruiters if such professional services are linked to access to Customer's Personal Data by SmartRecruiters.

"Data Protection Law(s)" means Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 repealing Directive 96/46/EC (General Data Protection Regulation 2016/679 ("**GDPR**")), national laws implementing GDPR, the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), the Swiss Federal Act on Data Protection as updated on 25 September 2020 and its corresponding ordinances ("**Swiss FADP**"), any other applicable data protection laws, and each case as may be amended or superseded from time to time, as well as all laws and regulations of the United States applicable to the processing of Personal Data under the Agreement, including (a) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 - 1798.199, 2022) and its implementing regulations (collectively, the "CCPA"), (b) the Virginia Consumer Data Protection Act, when effective, (c) the Colorado Privacy Act and its implementing regulations, when effective, (d) the Utah Consumer Privacy Act, when effective; and (e) Connecticut SB6, an Act Concerning Personal Data Privacy and Online Monitoring, when effective, as well as any other applicable law or regulation related to the protection of Customer Personal Data in the United States already in force or that may come into force during the term of the Agreement.

"**Restricted Transfer**" means: (i) where the EU GDPR or Swiss FADP applies, a transfer of Personal Data from the European Economic Area or Switzerland (as applicable) to a country outside of the European Economic Area or Switzerland (as applicable) which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not subject to adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("UK SCCs").

2. **Subject Matter of this Addendum**.

2.1. Data Processor and Controller. This Addendum stipulates the rights and obligations of Customer and SmartRecruiters regarding the Processing of Customer's Personal Data under the Agreement, and if applicable, Customer's Affiliates. This DPA applies to all activities within the scope of and related to the Agreement. As between SmartRecruiters and Customer, SmartRecruiters is a Data Processor and Customer, and if applicable Customer's Affiliates that Customer permits to use SmartRecruiters' Applications and Services under the Agreement, act as Data Controllers.

2.2. Governance. Customer acts as a single point of contact. Where authorizations, consent, instructions, or permissions are provided by Customer, these are provided not only on behalf of the Customer but also on behalf of any Customer Affiliates using SmartRecruiters' Applications and Services under the Agreement. Where SmartRecruiters informs or gives notice to Customer, such information or notice is deemed received by Customer Affiliates permitted by Customer to use SmartRecruiters' software/professional services under the Agreement. Customer shall forward such information and notices to such Customer Affiliates. This DPA does not constitute a third-party beneficiary agreement.

2.3. The Addendum does not affect the agreed scope of the services under the Agreement. To the extent that its obligations under this Addendum require SmartRecruiters to perform any additional services or activities that are not included in the scope the Agreement, SmartRecruiters shall be entitled to charge for these additional services or activities on a time and material basis according to SmartRecruiters then current price list.

3. **Data Processing Obligations**.

3.1. Processing Scope. SmartRecruiters shall Process Customer's Personal Data on behalf of Customer as Customer's Data Processor. The scope as well as the extent and nature of the Processing of Customer's Personal Data is for the sole purpose of managing the hiring process for both internal and external Customer hires as further specified in the Agreement and in **Annex 1 - Processing Details**.

3.2. Instructions. The initial instructions to SmartRecruiters are laid out in the Agreement and this Addendum. Customer shall be entitled to issue modifications to its instructions and to issue new instructions. Because of the nature of SmartRecruiters' services as multi-client services, Customer shall take the technical and operational feasibility of following its instructions into account. SmartRecruiters will use reasonable efforts to follow any Customer instructions if they are required by Data Protection Law and technically and operationally reasonably feasible. If carrying out an instruction is not required by Data Protection Law and/or technically and/or operationally reasonably feasible, or SmartRecruiters considers the instruction unlawful, SmartRecruiters will notify Customer without undue delay. The Parties will then discuss the matter and work together in good faith to find a solution that is feasible and addresses the underlying legal issue or other concern or interest of the Customer.

3.3. Customer Warranty. Customer hereby warrants and represents, on a continuous basis throughout the Term of the Agreement, that all Personal Data provided or made available by Customer to SmartRecruiters for Processing in connection with the Agreement was collected by Customer and transmitted to SmartRecruiters in accordance with applicable Data Protection Laws and Customer has obtained all necessary approvals, consents, authorizations and licences from each and every Data Subject required under Data Protection Laws to enable SmartRecruiters to Process Personal Data pursuant to the Agreement and to exercise its rights and fulfil its obligations under the Agreement.

3.4. Assistance. SmartRecruiters shall provide Customer with reasonable assistance with data protection impact assessments, prior consultations with data protection authorities that Customer is required to carry out under Data Protection Laws, dealing with requests from Data Subjects, and any other assistance obligations required by applicable law. If SmartRecruiters receives a request from a Data Subject in relation to the Personal Data processing hereunder, SmartRecruiters will promptly ask the Data Subject to redirect its request to Customer.

3.5. Appropriate Personnel. SmartRecruiters shall only engage personnel who have committed themselves to observing data privacy obligations. SmartRecruiters shall regularly train those employees to whom it grants access to Customer's Personal Data on security and privacy law compliance.

3.6. Technical and Organisational Measures. SmartRecruiters has taken appropriate technical and organisational measures according to Article 32 GDPR to keep Personal Data secure and protected against unauthorised or unlawful processing and accidental loss, destruction, or damage, and undertakes to continue doing so during the term of this Addendum. SmartRecruiters has implemented the technical and organisational measures further described in **Annex 2 - Technical and Organisational Measures**. SmartRecruiters may implement alternative measures provided the security level of the measures as specified in **Annex 2 - Technical and Organisational Measures** hereto is not reduced. Upon Customer's request, SmartRecruiters shall provide updated versions of **Annex 2 - Technical and Organisational Measures.** To evidence compliance with this Addendum, Customer agrees SmartRecruiters may provide up-to-date attestations, reports or extracts from independent bodies (e.g. ISO 27001 reports/certificates) that scrutinise and confirm the processing of Customer's Personal Data is in accordance with this Addendum.

3.7. Data hosting. Unless otherwise selected by the Customer, SmartRecruiters shall host Personal Data in the European Union.

3.8. Data Breach. No later than twenty-four business hours after SmartRecruiters has a reasonable degree of certainty about the occurrence of accidental or unlawful destruction, loss or alteration of, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by SmartRecruiters pursuant to this Addendum (a "**Personal Data Breach**"), SmartRecruiters shall notify Customer of the Personal Data Breach, provide such information as Customer may reasonably require to meet its obligations under Data Protection Laws regarding the Personal Data Breach, and take steps to remediate the Personal Data Breach. SmartRecruiters may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by SmartRecruiters.

3.9. Correction, deletion, or blocking of Personal Data. SmartRecruiters may be required to correct, erase and/or block Customer Personal Data if and to the extent the functionality of the Service does not allow the Customer to do so. However, SmartRecruiters shall not correct, erase and/or block Personal Data unless instructed by Customer.

3.10. Data Return. Unless otherwise agreed by the Parties in the Agreement, for 30 days after termination or expiration of the Agreement, SmartRecruiters will free of charge allow Customer to access SmartRecruiters' Customer Application Programming Interface ("**API**"), so that Customer can retrieve its data, including, without limitation, Customer Content and Candidate Content, in a format described on https://dev.smartrecruiters.com/customer-api/overview/. After 30 days, Customer agrees that no access to SmartRecruiters' Customer API will be granted to Customer any further, and SmartRecruiters will remove Customer's access and delete Customer's data.

4. Standard Contractual Clauses.

4.1. **SmartRecruiters as Data Exporter**. To the extent that SmartRecruiters acts as a data exporter, it has entered the Standard Contractual Clauses and Module 3 (Processor to Processor) thereof with the respective Sub-processor acting as a data importer or will do so prior to the start of Sub-processing. SmartRecruiters has procured or, for new Sub-processors, will procure that pursuant to Clause 17 Option 2 of the Standard Contractual Clauses, they will be governed by the law of the EU Member State in which the data exporter is established.

4.2. **Sub-processor of SmartRecruiters as Data Exporter**. To the extent a Sub-processor of SmartRecruiters acts as data exporter, SmartRecruiters has procured or will procure that such Sub-Processor executes the Standard Contractual Clauses and Module 3 (Processor to Processor) thereof with each Sub-processor prior to the start of the Sub-processing. Section 4.1, sentence 2 applies accordingly.

4.3. **Restricted Transfers**. The Parties agree that when the transfer of Customer Personal Data from Customer to SmartRecruiters is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

4.3.1. In relation to Customer Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows: (a) Module Two will apply; (b) in Clause 7, the optional docking clause will apply; (c) in Clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes shall be as set out in Clause 5 of this Data Protection Addendum; (d) in Clause 11, the optional language will not apply; (e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of the EU Member State in which the data exporter is established ; (f) in Clause 18(b), disputes shall be resolved before the courts of the member state where the data exporter is established; (g) Annex 1 of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this Data Protection Addendum; and (h) Annex 2 of the EU SCCs shall be deemed completed with the information set out in Annex 2 to this Data Protection Addendum.

4.3.2. In relation to Customer Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

(1) For so long as it is lawfully permitted to rely on Standard Contractual Clauses for the transfer of Personal Data to processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 ("**Prior C2P SCCs**") for transfers of Personal Data from the United Kingdom, the Prior C2P SCCs shall apply between Customer and SmartRecruiters on the following basis: (a) Appendix 1 shall be completed with the relevant information set out in Annex 1 to this Data Protection Addendum; (b) Appendix 2 shall be completed with the relevant information set out in Annex 2 to this Data Protection Addendum; and (c) the optional illustrative indemnification Clause will not apply.

(2) Where sub-clause 4.3.2(1) above does not apply, but the Customer and SmartRecruiters are lawfully permitted to rely on the EU SCCs for transfers of Personal Data from the United Kingdom subject to completion of a "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then: (a) The EU SCCs, completed as set out above in clause 4.3.1 of this Data Protection Addendum shall also apply to transfers of such Customer Personal Data, subject to the following sub-clause (b); and (b) the UK Addendum shall be deemed to form part of this Data

Protection Addendum, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Customer Personal Data.

4.3.3. In relation to Customer Personal Data that is protected by the Swiss FADP (as amended or replaced) the EU SCCs, completed as set out in clause 4.3.1. of this DPA, shall apply to transfers of such Customer's Personal Data, except that:

(1) The competent supervisory authority in respect of such Customer's Personal Data shall be Swiss Federal Data Protection and Information Commissioner.

(2) In Clause 17 the governing law shall be the law of Switzerland

(3) The references to "Member State(s)" shall be interpreted to refer to Switzerland, and Data Subjects located in Switzerland shall be entitled to exercise and enforce their rights under the EU SCCs in Switzerland.

(4) References to GDPR in the EU SCCs shall be understood as references to Swiss FADP.

4.4. If any provision of this Data Protection Addendum or the Agreement contradicts, directly or indirectly, with the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

4.5. If a new or modified version of the Standard Contractual Clauses or an alternative mechanism supersedes these Standard Contractual Clauses, such new or modified version of the Standard Contractual Clauses or an alternative mechanism shall be deemed to be incorporated into this Addendum.

5. Sub-processors.

5.1. Sub-processor Approval. In accordance with Art. 28 (2) sentence 2 GDPR, Customer hereby provides its general authorization to SmartRecruiters to appoint any Sub-processors identified by SmartRecruiters in **Annex 3 - Sub-Processor List** (the "**Sub-Processor List**") to Process Personal Data on SmartRecruiters' behalf. SmartRecruiters shall ensure that Sub-processors on the Sub-processor List are contractually obligated to protect Personal Data in compliance with Data Protection Laws and consistent with the obligations imposed on SmartRecruiters in this Addendum. SmartRecruiters shall remain responsible for the acts and omissions of each Sub-processor on the Sub-processor List as if they were the acts and/or omissions of SmartRecruiters and shall insure that, where applicable, it has entered the appropriate Standard Contractual Clauses with its Sub-processors. Customer agrees that SmartRecruiters may provide written notification of any change to the Sub-processor List by updating the Sub-processor List at the following link: https://www.smartrecruiters.com/legal/subprocessors. Any updates to the Sub-processor List shall occur thirty days prior to SmartRecruiters utilising the entity as a sub-processor for Customer ("**30 Days Period**"). Customer may subscribe to notifications for Sub-Processor List sub-processor changes here: https://status.smartrecruiters.com.

5.2. Sub-processor Objections. If Customer has a legitimate and material data protection reason to object to a Sub-processor added to the Sub-processor List, Customer may object by sending Customer's objection and the basis for such objection to legal@smartrecruiters.com within fifteen days of such addition. If the Parties cannot mutually agree to a reasonable resolution to Customer's objection within further fifteen days of SmartRecruiters' receipt of Customer's objection, Customer may terminate the Agreement and this Addendum upon written notice to SmartRecruiters. For the avoidance of doubt Customer's objection and/or the discussions between the Parties do not affect SmartRecruiters' right to use the new Sub-processor after the 30 Days Period. If the Customers terminates, the termination shall take effect at the time determined by the Customer which shall be no later than 60 days from the date of SmartRecruiters' notice to Customer informing Customer of the new Sub-processor. If Customer does not terminate within this 60-day period, Customer is deemed to have accepted the new Sub-processor.

5.3. Emergency Replacement. SmartRecruiters may replace a Sub-processor without advance notice where the reason for the change is outside of SmartRecruiters' reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SmartRecruiters will inform Customer of the replacement Sub-processor as soon as possible following its appointment, and Customer will have the same rights to object to such replacement Sub-processor as outlined in section 5.2 of this Addendum.

6. Auditing Rights. If Customer is subject to an audit or investigation from a data protection regulator, SmartRecruiters shall, when required, respond to any information requests, and/or agree to submit its premises and operations to audits, including inspections by Customer and/or the competent data protection regulator, in each case for the purpose of evidencing its compliance with this Addendum, provided that: (v) Customer shall ensure that all information obtained or generated in connection with any information request, audit or inspection is kept strictly confidential (unless disclosure to a competent data protection regulator or as otherwise required by applicable law), (w) Customer shall ensure that any information request, audit or inspection is undertaken within normal business hours (unless such other time is mandated by a competent data protection regulator) with minimal disruption to SmartRecruiters' business, and acknowledging that such information request, audit or inspection shall be subject to any reasonable policies, procedures or instructions of SmartRecruiters for the purposes of preserving security and confidentiality; (x) Customer shall give SmartRecruiters at least 15 days' prior written notice of an information request and/or audit or inspection (unless the competent data protection regulator provides Customer with less than 15 days' notice, in which case Customer shall provide SmartRecruiters with as much notice as practically possible), (y) a maximum of one information request, audit and/or inspection may be requested by Customer in any twelve (12) month period unless an additional information request, audit and/or inspection is mandated by a competent data protection regulator in writing, and (z) Customer shall pay SmartRecruiters' reasonable costs for any assistance or facilitation of any audit or inspection or other work undertaken unless such costs are incurred due to SmartRecruiters' breach of its obligations under this Addendum. If any audit request is not at the request of a data protection regulator, Customer agrees (1) to request information in the first instance in written form, (2) SmartRecruiters may respond to such requests by providing up-to-date attestations, reports or extracts from independent bodies (e.g., ISO 27001 reports/certificates) that scrutinises and confirms the processing of Customer's Personal Data is in accordance with the agreed to measures herein, it being understood that Customer may demand additional clarifications and perform on-site inspections where necessary to satisfy Data Protection Law requirements, or (3) on SmartRecruiters' request, to conduct the audit through a certified auditor the Parties jointly agree on.

7. **International Data Transfers**. This Section 7 applies when SmartRecruiters or its sub-processors Processes Customer's Personal Data in countries outside the EEA or Switzerland ("**International Transfer**"). SmartRecruiters shall undertake (and shall ensure that its sub-processors undertake) an International Transfer only if the requirements according to Art. 44 seqq. GDPR are met (collectively the "**International Transfer Mechanisms**"). When this Section 7 applies, the terms of this Addendum shall be read in conjunction with the applicable International Transfer Mechanism. Nothing in this Addendum shall be construed to prevail over any conflicting clause of the applicable International Transfer Mechanism. Should the Standard Contractual Clauses be invalidated, replaced, annulled, or otherwise designed in such a way that they no longer constitute adequate safeguards for data transfers to third countries, SmartRecruiters shall undertake, together with Customer, to find an alternative solution that complies with the applicable Data Protection Laws and ensures the lawfulness of processing Personal Data in third countries.

8. **Notifications**.

8.1. If SmartRecruiters receives a request, subpoena, or court order (including through an obligation due to legal provisions or official injunctions from state authorities) requiring SmartRecruiters to provide any Customer's Personal Data Processed under this Addendum to an authority, SmartRecruiters shall attempt to redirect the relevant authority to request that data directly from the Data Controller, and notify Customer without undue delay, unless SmartRecruiters is prohibited from doing so.

8.2. Where Customer's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in SmartRecruiters' control, SmartRecruiters' shall notify Customer of such action without undue delay. SmartRecruiters shall, without undue delay, notify to all pertinent parties in such action, that any Personal Data affected thereby is in Customer's sole property and area of responsibility, that Personal Data is at Customer's sole disposition, and that Customer is the Data Controller.

9. **California Consumer Privacy Act ("CCPA"); California Privacy Rights Act ("CPRA")**. If SmartRecruiters Processes a California resident's Personal Data on behalf of Customer, SmartRecruiters does so as a service provider under the CCPA, or the CPRA when applicable. SmartRecruiters agrees it will not use Personal Data other than for the business purpose set forth in the Agreement, or for a commercial purpose other than providing the services specified in the Agreement. SmartRecruiters shall not sell Customer Personal Data. SmartRecruiters represents that it understands the restrictions in this Addendum, and its obligations under the CCPA & CPRA, and will comply with them. SmartRecruiters shall only notify Customer if it can no longer comply with the CCPA or CPRA. SmartRecruiters shall comply with the CCPA & CPRA as a service provider and provide the level of protection the CCPA and CPRA requires as applicable.

10. **Term.** This Addendum shall follow the term of the Agreement ("**Term**").

11. **Miscellaneous**. No modification of this Addendum shall be valid and binding unless made in writing and then only if such modification expressly states that such modification applies to this Addendum. The foregoing shall also apply to any waiver or modification of this mandatory written form. This Addendum shall take precedence over any conflicting provisions of the Agreement. The Standard Contractual Clauses shall take precedence over any conflicting provisions in the main body of this Addendum and the Agreement.

Customer	SmartRecruiters
By:	By: Jeremy Johnson
Printed Name:	Printed Name: Jeremy Johnson
Title:	Title: CFO
Date:	Date: 8/17/2023

ANNEX 1 - PROCESSING DETAILS

A.

Categories of Personal Data Processed:

- **Personnel Data** (e.g., name, title, career history, education, work certificates, personal interests, photo, date of birth, sex, etc.)
- **Organisational data of Customer** (e.g., internal applicants or managers and HR personnel responsible for applications.)
- **Application Process Data** (e.g., questions in job interviews, feedback, reason for hiring, number of applications, company ID, internal application as well as notes to and from candidates/applicants by using existing emailing services of the application including notifications).
- **Online Data** (e.g., IP address, User ID, mobile device used, operating system, internet provider, date and time of logon and logoff).
- **Communication Data** (e.g., Email address, private and business address, private and business phone numbers, Skype ID, social network IDs, email content).
- **Online Usage Data related to the SmartRecruiters Platform** (e.g., cookie IDs, Digital Fingerprints, IP addresses, URL history, etc.).
- **Logging Data** (e.g., User ID, password, activation date, creation date, failed login count, modification date, state type, verification date and state, and information that enables to check whether and by whom Personal Data have been input into the SmartRecruiters Platform or was modified or removed therein).

Data subjects:

- Customers' Authorised Users (as defined in the Agreement) using the software described in Agreement.
- Candidates using the software described in the Agreement to apply for jobs.
- Customer's employees who have applied to internal jobs with Customer.

Special categories of data (if appropriate): If a customer requires special categories of Personal Data, or a candidate provides special categories of Personal Data voluntarily, then SmartRecruiters may also process special categories Personal Data.
Data Transfer Frequency: continuous basis.

Nature of processing: Processing necessary to provide the Services to Customer in accordance with the documented instructions provided in the Agreement and this DPA.

The Period for which the Personal Data will be retained: as set forth in the Agreement.

B.

Applicable when a Restricted Transfer is taking place (i.e., where SmartRecruiters, Inc. is the contracting entity and this Annex 1 is being read as Annex 1 of the Standard Contractual Clauses):

Data exporter:
The data exporter is (please briefly specify your activities relevant to the transfer):

- **Customer Name**: Customer as listed above and as set forth in the Agreement.
- **Customer Address**: Customer's address is set forth in the Agreement.
- **Activities relevant to data transfer**: use of SmartRecruiters' software to attract talent.
- **Contact Person's name, position, and contact details**: as set forth in the Agreement.
- **Customer Role**: controller.

Data importer:

The data importer is (please briefly specify activities relevant to the transfer):

- **Data Importer**: SmartRecruiters, Inc., a software provider that provides its customers access to a talent Acquisition software platform.
- **Address**: is 166 Geary St, San Francisco, CA 94108, USA
- **Activities relevant to data transfer**: Providing talent acquisition software specified in the Agreement between Data Exporter and Data Importer.

- **Role**: processor.

  Description of Transfer:
- Module Two: controller to processor.

C.

Purposes of the Data Transfer and Further Processing:
- **Purpose**: as set forth in the Agreement.
- **Further Processing**: as set forth at: https://www.smartrecruiters.com/legal/subprocessors.

Sub-processor Processing:
- **Subject Matter**: the types of data described above.
- **Nature of Processing**: as set forth at: https://www.smartrecruiters.com/legal/subprocessors.
- **Duration**: as set forth in the Agreement.

Competent Supervisory Authority: The competent supervisory authority that Customer has registered with.

ANNEX 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

1. Access control to premises and facilities. Technical and organisational measures to control access to premises and facilities, particularly to check authorization:

- Security perimeters are defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
- Physical security for offices, rooms and facilities are designed and applied.
- Physical protection against natural disasters, malicious attack or accidents are designed and applied.
- Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.
- For the purposes of secure disposal or reuse, equipment containing storage media that may possibly contain Personal Data are treated as though it does.
- Mobile equipment has appropriate protections (encryption).
- A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities is adopted.
- Equipment is sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.
- It is ensured that only authorised persons can access premises and company buildings where customers' data is stored or processed.
- SmartRecruiters protects its premises and facilities with alarm systems and video/CCTV monitoring.

2. Access control to systems. Technical (ID/password security) and organisational (user master data) measures for user identification and authentication:

- An access control policy is established, documented, and reviewed based on business and information security requirements.
- Users are provided with access to the network and network services that they have been specifically authorised to use.
- The allocation and use of privileged access rights is restricted and controlled.
- A formal user access provisioning process is implemented to assign or revoke access rights for all user types to all systems and services.
- The allocation of secret authentication information is controlled through a formal management process.
- Temporary passwords are given to users in a secure manner. The use of third parties or unprotected (clear text) electronic mail messages must be avoided.
- Password policy is known and implemented by every employee of SmartRecruiters.
- Password management system ensures quality passwords.
- The Local Administrator and other privileged accounts passwords never appear unscrambled on the network.
- Inactive sessions are shut down after a defined period of inactivity.
- Access to Information and application system functions by users and support personnel are restricted in accordance with the defined access control policy.
- Access to source code is protected and restricted to a level commensurate with the level of risk.

3. Access control to data. Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:

- An access control policy to customer’s data is established, documented, and reviewed based on business and information security requirements.
- SmartRecruiters implemented a comprehensive encryption solution for data in transit (incl. Network).
- Database storages are encrypted.
- Operating Systems are hardened to enforce required security controls.
- SmartRecruiters ensures that procedures are established which guarantee correctness, integrity, and availability of SmartRecruiters data throughout all stages of data processing.
- Media are disposed of securely when no longer required, using formal procedures.

4. Disclosure control. Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

- Access to systems that keep or process customer's data is allowed via secured network connections.
- Logging facilities and log information is protected against tampering and unauthorised access.
- When Information is sent or received, it is checked for the infection by viruses and if necessary, bear details of the authenticator and / or the integrity check (Digital signature).

5. Input control. Measures for subsequent checking whether data have been entered, changed, or removed (deleted), and by whom:

- Security related application events are logged on application level.
- Log entries identify the individual whose action is being audited, the individual affected by the action and the time of the action.
- The log policy regulates that the log entries shall not contain any sensitive information.

6. Job Control. Measures (technical/organisational) to segregate the responsibilities between SmartRecruiters (as processor) and Customer (as data controller):

- Unambiguous wording of the Addendum between SmartRecruiters and Customer with clear specifications of SmartRecruiters' and Customer's obligations.
- Careful selection of SmartRecruiters as processor by Customer.
- Monitoring of the performance of the Addendum on a regular basis by SmartRecruiters and Customer.

7. Availability control. Measures to assure data security (physical/logical):

- SmartRecruiters developed a disaster recovery plan, which contains all the procedures and support Information required for business resumption.
- SmartRecruiters' procedures are established which guarantee correctness, integrity, and availability of SmartRecruiters data throughout all stages of data processing.
- Access to backups is restricted to authorised personnel only.
- Backups are encrypted.
- Files that are uploaded to the platform are scanned against viruses.

8. Segregation control. Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

- The environments used for development, testing and production purposes are physically separated.
- Usage of production un-anonymized data on development environment is not allowed.

Sub-processor Technical and Organisational Security Measures

The technical and organisational security measures utilised by sub-processors are substantially similar to those set forth above.

ANNEX 3 SUB-PROCESSOR LIST

Customer has authorised the following sub-processors:

https://www.smartrecruiters.com/legal/subprocessors

Description of processing: The description of processing is set forth at the link above in this Annex 3.