

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 3; (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 with a copy to dpo@smartrecruiters.com, or (ii) if you are an existing customer, to dpo@smartrecruiters.com.

This Data Processing Addendum (the “**Addendum**”) is between _____ (“**Customer**”) located at _____, and the SmartRecruiters entity set forth in the Agreement (“**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. 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.

1. Definitions.

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

“**Agreement**” shall mean the master subscription agreement or other subscription agreement between Customer and SmartRecruiters governing Customer’s access to SmartRecruiters’ software.

“**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, and any other applicable data protection laws.

2. Subject Matter of this Addendum. This Addendum stipulates the rights and obligations of Customer and SmartRecruiters regarding the Processing of Customer’s Personal Data under the Agreement. 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 is a Data Controller.

3. Data Processing Obligations.

3.1. Individual Accounts Not in Scope. Any individual has the option to set up a personal account in SmartRecruiters’ software. With this personal account, an individual is able to coordinate different application profiles and application processes for multiple companies. The collection and processing of personal data for an individual’s personal account is not done by SmartRecruiters for Customer. Instead, it is done solely for the individual by SmartRecruiters. Therefore, the relationship between an individual with an individual account and SmartRecruiters is not governed by this Addendum.

3.2. 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 licenses 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.

3.3. 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.

3.4. Appropriate Personnel. SmartRecruiters shall only engage personnel who have committed themselves to observe 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.

3.5. Technical and Organizational Measures. SmartRecruiters has taken appropriate technical and organizational measures according to Article 32 GDPR to keep Personal Data secure and protected against unauthorized or unlawful

processing and accidental loss, destruction or damage, and undertakes to continue doing so during the term of this Addendum. In particular, SmartRecruiters has implemented the technical and organizational measures further described in **Annex 2 to the Standard Contractual Clauses**. SmartRecruiters may implement alternative measures as long as the security level of the measures as specified in **Annex 2** hereto is not reduced. 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 scrutinize and confirm the processing of Customer's Personal Data is in accordance with this Addendum.

3.6. Data Breach. No later than twenty-four hours after SmartRecruiters has a reasonable degree of certainty about the occurrence of accidental or unlawful destruction, loss or alteration of, unauthorized 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 applicable law with respect to the Personal Data Breach, and take steps to remediate the Personal Data Breach.

4. Standard Contractual Clauses. "**Standard Contractual Clauses**" means the Standard Contractual Clauses contained in the European Commission's Implementing Decision 2021/914 of June 4, 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. The Standard Contractual Clauses and Module Two thereof are incorporated into this Addendum by reference. All other modules in the Standard Contractual Clauses are excluded by this Data Processing Addendum. The necessary population of the Standard Contractual Clauses is contained in Annex 1, 2, and 3. Under Clause 18 of the Standard Contractual Clauses, the Parties agree that the courts shall be the courts of the country in which the Controller is located.

5. Subprocessors.


5.1. Subprocessor Approval. In accordance with Clause 9, subsection (a) option 2 of Module Two of the Standard Contractual Clauses, Customer hereby provides its general authorization to SmartRecruiters to appoint any Sub-processors identified by SmartRecruiters on the following list (the "**Sub-processor List**") to Process Personal Data on SmartRecruiters' behalf: <https://www.smartrecruiters.com/legal/subprocessors>. 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. Customer agrees that SmartRecruiters may provide notification of any change to the Sub-processor List by updating the Sub-processor list at the foregoing link. Any updates to the Sub-processor List shall occur at least ten days prior to SmartRecruiters utilizing the entity as a sub-processor for Customer.

5.2. Sub-processor Objections. If Customer has a legitimate 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 thirty days of such addition. If the Parties cannot mutually agree to a reasonable resolution to Customer's objection within fourteen business days of SmartRecruiters' receipt of Customer's objection, either Party may terminate the Agreement upon written notice to the other Party.

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 SmartRecruiters may replace an audit requested by Customer by providing up-to-date attestations, reports or extracts from independent bodies (e.g., ISO 27001

reports/certificates) that scrutinizes and confirms the processing of Customer’s Personal Data is in accordance with the agreed to measures herein.

- 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: (i) subject to the terms of the Standard Contractual Clauses incorporated into this Addendum, or (ii) to a country that has received a binding adequacy decision by the European Commission or otherwise under Data Protection Laws (collectively, with the Standard Contractual Clauses, 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.
- 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”).** If SmartRecruiters Processes a California resident’s Personal Data on behalf of Customer, SmartRecruiters does so as a service provider under the CCPA. SmartRecruiters agrees it will not use Personal Data other than for the business purpose set forth in the Agreement. SmartRecruiters will not sell Customer Personal Data. SmartRecruiters represents that it understands the restrictions in this Addendum and will comply with them.
- 10. **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.

Customer	SmartRecruiters
By:	By: 
Printed Name:	Printed Name: Jerome Ternynck
Title:	Title: CEO
Date:	Date: August 1, 2021

ANNEX 1 TO THE STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer controller to processor

Data exporter:

The data exporter is (please specify briefly 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.
- **Role:** controller

Data importer:

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

- **Data Importer:** SmartRecruiters, Inc., a software provider that provides its customers access to a talent Acquisition software platform.
- **Address:** 225 Bush St, San Francisco, CA 94104.
- **Activities relevant to data transfer:** Providing talent acquisition software specified in the Agreement between Data Exporter and Data Importer.
- **Contact Person's name, position, and contact details:** Stephen Hanthorn, DPO, dpo@smartrecruiters.com
- **Role:** processor

Description of Transfer:

- Module Two: controller to processor.

Data subjects:

- Customers' employees 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.

Categories of Personal Data Transferred:

- **Personnel Data** (e.g., name, title, career history, education, work certificates, personal interests, photo, date of birth, sex, etc.)
- **Organizational 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).

Sensitive categories of data transferred (if appropriate): If a customer requires sensitive categories of personal data, or a candidate provides sensitive categories of personal data voluntarily, then SmartRecruiters may also process sensitive categories of personal data. However, SmartRecruiters Applications are not designed or intended for processing sensitive categories of personal data.

Data Transfer Frequency: continuous basis.

Purposes of the Data Transfer and Further Processing:

- **Purpose:** as set forth in the Agreement.
- **Further Processing:** collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination,



restriction, erasure or destruction.

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

Sub-processor Processing:

- **Subject Matter:** the types of data described above.
- **Nature of Processing:** collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Duration:** as set forth in the Agreement.

Competent Supervisory Authority:

- **Germany:** The Federal Commissioner for Data Protection and Freedom of Information

ANNEX 2 TO THE STANDARD CONTRACTUAL CLAUSES**TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA****MODULE TWO: Transfer controller to processor**

1. Access control to premises and facilities. Technical and organizational 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 re-use, 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 unauthorized access.
- It is ensured that only authorized 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 organizational (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 authorized 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 session 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 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 unauthorized 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/organizational) 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 authorized 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 Organizational Security Measures

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

ANNEX 3 TO THE STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer controller to processor

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

Except for the subprocessors listed in the table below, because SmartRecruiters' subprocessors are similarly situated software companies, or are implementation partners performing similar processing activities, the processing operations are the same as for SmartRecruiters.

Description of processing: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Subprocessor	Description of Processing
Amazon Web Services Inc.	Storage, erasure or destruction
SendGrid, Inc.	Collection, recording, organisation, structuring, storage, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Textkernel BV	Collection, recording, organisation, structuring, storage, adaptation or alteration, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination.