Data Processing Agreement

between

“**Customer**”

and

SmartRecruiters Inc.

225 Bush Street
Suite #300
San Francisco CA 94104

- hereinafter “**SmartRecruiters**” -

both Customer and SmartRecruiters hereinafter individually referred to as a “**Party**”, and jointly referred to as the “**Parties”**

Table of Contents

Explanatory note

This Data Processing Agreement defines the rights and obligations of the Customer and SmartRecruiters regarding the Processing of Customer's Personal Data in connection with the SmartStart Services provided by SmartRecruiters. It shall apply to all activities within the scope of and related to the Main Agreement in the context of which SmartRecruiters' employees or Subprocessors may process Customer's Personal Data.

This Data Processing Agreement includes:

- the main body of the Data Processing Agreement;
- the Annex 1 "Standard Contractual Clauses" (Processors);
- the Annex 2 "Technical and organizational measures"
- the Annex 3 "List of Subprocessors"

This Data Processing Agreement and the standard contractual clauses in Annex 1 have been pre-signed by SmartRecruiters, Inc. Upon receipt of a completed and signed Data Processing Agreement by the Customer, this Data Processing will be legally binding.

How to get a binding Data Processing Agreement? Next steps:

1. You (i.e. the Customer or Data Exporter) shall **complete** the Data Processing Agreement as follows:

    a. the signatory information on page 11;
    b. the information as "data exporter" on page 12 (Annex 1);
    c. the signatory information on page 18;
    d. a short description of your activities on page 19;
    e. the signatory information as data exporter on page 19

2. You shall **sign** on pages 11, 18 and 19.

3. Please send the completed and signed DPA to your sales representative at SmartRecruiters with a copy to dpo@smartrecruiters.com

1. Definitions

“**Customer’s Personal Data**“ shall mean Personal Data of which Customer is the Data Controller.

“**Data Controller**” shall have the meaning of “controller” as defined in Article 2 lit. (d) of the Directive and as of May 25th 2018 in Article 4 No. 7 of the GDPR.

“**Data Exporter**” shall have the meaning as defined in Clause 1 (b) of the Standard Contractual Clauses (Processors).

“**Data Importer**” shall have the meaning as defined in Clause 1 (c) of the Standard Contractual Clauses (Processors).

“**Data Processor**”, “**Data Processing**”, “**Processing**” shall have the meaning of “processor” and “processing” as defined in Article 2 lit. (b) and (e) of the Directive and as of May 25th 2018 in Article 4 No. 2 and No. 8 of the GDPR.

“Data Protection Law” means the statutory data privacy and protection regulations applicable to Customer protecting the fundamental rights and freedoms of persons with regard to data privacy and the Processing of Customer’s Personal Data by SmartRecruiters.

“**Data Subject**” shall have the meaning of “data subject” as defined in Article 2 lit. (a) of the Directive and as of May 25th 2018 in Article 4 No. 1 of the GDPR.

“**Directive**” shall mean the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

“**EEA**” shall mean the Treaty on the European Economic Area.

“**EU**” shall mean European Union.

“**GDPR**” means the Regulation (EU) 2016/679 (General Data Protection Regulation).

“**Instruction**” shall mean an instruction issued by Customer to SmartRecruiters and directing SmartRecruiters to perform a specific action with regard to the Processing of Customer’s Personal Data in order to achieve compliance with Data Protection Law.

“**Location(s)**” are locations where or from which SmartRecruiters performs its Services involving the Processing of Customer’s Personal Data.

“**Main Agreement**” shall mean the terms and conditions between Customer and SmartRecruiters under which this Exhibit is made.

“**Personal Data**” shall have the meaning as defined in Article 2 lit. (a) of the Directive and as of May 25th 2018 in Article 4 No. 1 of the GDPR related to the Services.

“**Service(s)**” shall mean the SmartStart services SmartRecruiters shall provide pursuant to the Main Agreement.

“**Standard Contractual Clauses (Processors)”** or **“Clauses”** shall mean the clauses approved by the European Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in Third Countries or any EU Commission-approved clauses that may replace the aforementioned clauses in the future.

“**Subprocessing**” shall mean the Processing of Personal Data as a subcontractor of a Data Processor.

“**Subprocessor**” shall mean an entity that Processes Personal Data as a subcontractor of a Data Processor.

“**Third Country(ies)**” shall mean any country outside the European Union and the European Economic Area not recognized by the European Commission as providing an adequate level of protection for Personal Data.

2. Subject Matter of the Data Processing Agreement

This Data Processing Agreement stipulates the rights and obligations of Customer and SmartRecruiters regarding the Processing of Customer’s Personal Data in connection with the Services. It shall apply to all activities within the scope of and related to the Main Agreement in the context of which SmartRecruiters’ employees or Subprocessors may come into contact with Customer’s Personal Data.

3. Data Processing – Scope, Nature, Purposes and Duration

3.1 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 Main Agreement.

3.2 Customer as Data Controller shall be responsible for complying with Data Protection Law, including, but not limited to, the lawfulness of the Processing and the lawfulness of the transmission (if any) of Customer’s Personal Data to SmartRecruiters.

3.3 SmartRecruiters shall Process and use Customer’s Personal Data only to the extent required and with the purpose of fulfilling SmartRecruiters’ obligations under the Main Agreement and in accordance with Customer’s Instructions pursuant to Section 11 below. the candidate will have the option to set up a personal account. With this personal account, he/she will be able to coordinate different application profiles and application processes for different job offerings of the Customer and of other companies. The collection, processing and use of data for creating and using this personal account is not done on behalf of the Customer, but lies in the sole responsibility of the candidate and SmartRecruiters and is therefore not regulated by this Data Processing Agreement

3.4 Except where this Data Processing Agreement expressly stipulates any surviving obligation, this Data Processing Agreement shall follow the term of the Main Agreement.

3.5 The affected categories of Customer’s Personal Data and the affected Data Subjects are as follows:

a) Categories of Personal Data

SmartRecruiters stores both candidate and user data as follows:

a. Personnel Data (e.g. name, title, details about career history, education, work certificates, personal interests, photo, date of birth, sex etc.)
b. Organizational data of e. g. internal applicants or managers and HR personnel responsible for applications

c. 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)
d. Online Data (e.g. IP address, User ID, mobile device used, operating system, internet provider, date and time of logon and logoff)
e. Communication Data (e.g. Email address, private and business address, private and business phone numbers, Skype ID, social network IDs, email content)
f. Online Usage Data related to the SmartRecruiters Platform (e.g. cookie IDs, Digital Fingerprints, IP addresses, URL history, etc.)
g. 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)

It is possible that special categories of data are processed according to this Agreement in individual cases. Special categories of personal data shall mean information revealing person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as person's genetic data, biometric data for the purpose of uniquely identifying a natural person, person's data concerning health or data concerning a natural person's sex life or sexual orientation.

It is possible that all kind of sensitive personal data are processed. This depends on the information that the candidates and applicants include in their profile and the documents they upload to the platform.

b) Categories of Data Subjects

The affected Data Subjects include users and candidates.

Users include employees of Customer for the sole purpose of managing their engagement in the hiring process, applying to jobs internally, and/or referring potential hires.

External candidates include individuals who do not currently work for Customer but who have applied to jobs with Customer.

4. Standard Contractual Clauses

4.1 SmartRecruiters hereby enters into the Standard Contractual Clauses (Processors) hereto attached as **Annex 1 - Standard Contractual Clauses (Processors)** as Data Importer with Customer as Data Exporter.

4.2 For the sake of clarification this Data Processing Agreement shall not modify or change the Standard Contractual Clauses (Processors) hereto attached as **Annex 1 - Standard Contractual Clauses (Processors)** in any manner. This Data Processing Agreement shall only supplement and interpret the Standard Contractual Clauses (Processors) hereto attached as **Annex 1 - Standard Contractual Clauses (Processors)** in more detail. In case of any contradictions between this Data Processing Agreement and the Standard Contractual Clauses (Processors) hereto attached as **Annex 1 - Standard Contractual Clauses (Processors)**, the Standard Contractual Clauses (Processors) hereto attached as **Annex 1 - Standard Contractual Clauses (Processors)** shall prevail.

5. Technical and organizational measures

5.1 SmartRecruiters declares that it 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 Data Processing Agreement. In particular, SmartRecruiters shall take and regularly check the following technical and organizational measures, as further described in **Annex 2 – Technical and Organisational Measures**:

(a) Physical access control (technical and organizational measures to control access to premises and facilities, particularly to check authorization)

(b) Access control (unauthorized access to Data Processing systems must be prevented*)*

(c) Access limitation control (activities in Data Processing systems not covered by the allocated access rights must be prevented)

(d) Transmission control (aspects of the disclosure of Personal Data must be controlled: electronic transfer, data transport, transmission control, etc.)

(e) Input control (documentation of Personal Data management and maintenance must be maintained*)*

(f) Job control (Data Processing must be carried out according to Instructions)

(g) Availability control (the Personal Data must be protected against accidental destruction or loss)

(h) Data separation (Personal Data collected for different purposes must also be processed separately*)*

Customer is aware of these technical and organizational measures and is responsible for ensuring that they provide an appropriate level of protection for the risks of the Personal Data to be processed.

5.2 SmartRecruiters is allowed to implement adequate alternative measures as long as the security level of the measures as specified in **Annex 2 – Technical and Organizational Measures** is maintained. Any significant changes shall be documented by SmartRecruiters.

5.3 SmartRecruiters shall appropriately document the technical and organizational measures actually implemented (including each update) for the Processing of Customer's Personal Data under the Main Agreement and will hand out the then current version of such documentation to Customer upon Customer's request (e.g., for audit purposes).

5.4 For the purpose of documentation, SmartRecruiters shall be entitled to provide evidence for the implementation of appropriate technical and organisational measures by providing up-to-date attestations, reports or extracts from independent bodies (e.g. SSAE16-SOC2, ISO 27001 reports/certificates) that scrutinizes and confirms the processing of Customer's Personal Data is in accordance with the agreed to measures herein.

6. Correction, deletion and blockings of Personal Data

6.1 SmartRecruiters may be required to correct, erase and/or block 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 or block Personal Data unless instructed by Customer.

6.2 Unless mandatory Data Protection Law provide otherwise, there shall not be any direct communication between Data Subjects and SmartRecruiters. In the event that a Data Subject does apply directly to SmartRecruiters in writing, e.g., to request the correction or deletion of his/her Personal Data, SmartRecruiters shall forward this request to Customer without undue delay and shall not respond directly to the Data Subject.

7. Other SmartRecruiters' Obligations

7.1 SmartRecruiters shall appoint a data protection officer if it is legally obliged to do so or, if it is not obliged to do so, a contact person for data protection issues.

7.2 SmartRecruiters shall provide Customer, in writing, with the name and contact details of its data protection officer or the contact person for data protection issues.

7.3 SmartRecruiters shall only engage personnel who have demonstrably committed themselves to observe data secrecy. SmartRecruiters shall regularly train those employees to whom it grants access to Customer's Personal Data on IT security and privacy law compliance. The undertaking to data secrecy shall continue after the termination of this Data Processing Agreement.

7.4 SmartRecruiters shall monitor the Data Processing by way of regular reviews concerning the performance of and compliance with the Main Agreement, particularly this Data Processing Agreement.

7.5 At Customer's written request, SmartRecruiters shall reasonably support Customer in dealing with requests from individual Data Subjects and/or a supervisory authority with respect to the Data Processing of Personal Data hereunder.

8. Subprocessors

8.1 Customer hereby authorizes SmartRecruiters to engage Subprocessors as further specified in **Annex 3 – Subprocessors**, provided that SmartRecruiters remains responsible for any acts or omissions of its Subprocessors in the same manner as for its own acts and omissions hereunder.

8.2 SmartRecruiters may remove or appoint suitable and reliable other Subprocessors at its own discretion in accordance with this Section 8.2:

(a) SmartRecruiters shall inform Customer 30 days in advance of any envisaged changes to the list of Subprocessors.

(b) If Customer has a legitimate data protection related reason to object to SmartRecruiters' use of a Subprocessor, Customer shall notify SmartRecruiters within fourteen (14) days after receipt of SmartRecruiters' notice according to Section (a)8.2(a) above. If Customer does not object during this time period, the new Subprocessor(s) shall be deemed accepted. If Customer objects to the use of the Subprocessor(s) concerned, SmartRecruiters shall have the right to cure the objection through one of the following options (to be selected at SmartRecruiters' sole discretion): (a) SmartRecruiters will abort its plans to use the Subprocessor with regard to Customer's Personal Data; or (b) SmartRecruiters will take corrective steps and proceed to use the Subprocessor with regard to Customer's Personal Data. If SmartRecruiters decides not to implement option (a) or (b) above, SmartRecruiters shall notify Customer without undue delay. In this case

Customer shall be entitled within further fourteen (14) days to notify in writing SmartRecruiters about its termination of the Main Agreement and any such termination would become effective upon the expiry of the second (2nd) calendar month after SmartRecruiters' receipt of the termination notice.

(c) For the avoidance of doubt, irrespective of any Customer objection according to lit. (b) above, SmartRecruiters shall be entitled to engage any Subprocessor, it being understood that Customer's termination right in accordance with lit. (b) above remains unaffected.

8.3 SmartRecruiters shall pass on to its subcontractors acting as Subprocessors SmartRecruiters' obligations under this Data Processing Agreement.

9. Auditing Rights

SmartRecruiters shall be entitled to replace an audit requested by Customer by providing up-to-date attestations, reports or extracts from independent bodies (e.g. SSAE16-SOC2, ISO 27001 reports/certificates) that scrutinizes and confirms the processing of Customer's Personal Data is in accordance with the agreed to measures herein.

10. Notifications

10.1 SmartRecruiters shall inform the Customer without undue delay if it becomes aware of any breaches of Customer's Personal Data protection. In consultation with Customer, SmartRecruiters must take appropriate measures to secure Customer's Personal Data and limit any possible detrimental effect on the Data Subjects. Where obligations are placed on Customer under Data Protection Law, SmartRecruiters shall provide commercially reasonable assistance in meeting them.

10.2 If SmartRecruiters receives a request, subpoena or court order (including through an obligation due to legal provisions or official injunctions from state authorities) requiring to provide any Customer's Personal Data Processed under this Data Processing Agreement 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.

10.3 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.

11. Instructions

11.1 The Instructions to SmartRecruiters are initially laid out in the Main Agreement, in particular, this Data Processing Agreement. However, Customer shall be entitled to issuing modifications to Instructions and to issue new Instructions, subject to feasibility.

11.2 Customer shall designate a person competent to issue Instructions. Modifications or new Instructions shall be issued in writing to Data Privacy Officer (dpo@smartrecruiters.com) and shall need to be agreed between the Parties as a contract modification/change request under the Main Agreement.

11.3 SmartRecruiters shall notify Customer if SmartRecruiters considers an Instruction to be in violation of Data Protection Law. SmartRecruiters shall not be obligated to perform a comprehensive legal examination and shall in no event render any legal services to Customer.

11.4 SmartRecruiters shall not be responsible for any consequences of an Instruction issued by Customer and Customer shall indemnify and hold SmartRecruiters harmless against any damages and third-party claims resulting from a Customer Instruction.

11.5 Unless otherwise agreed, SmartRecruiters shall be entitled to charge any efforts incurred in connection with a Customer Instruction on time and material basis.

12. Additional Clauses Applicable as of May 25th, 2018

12.1 As of May 25th, 2018, the following Sub-Clauses of this Clause 12 shall apply to this Data Processing Agreement in addition to the Clauses 1-11, 13 of this Data Processing Agreement. The provisions of this Clause 12 shall take precedence to any conflicting provisions set out in the Clauses 1-11, 13 of this Agreement.

12.2 SmartRecruiters shall

(a) assist the Customer, with the implementation of appropriate technical and organizational measures in order to respond to applications by Data Subjects for the exercise of their rights (in particular Art. 13 to 23 GDPR);

(b) support the Customer with

i. complying with and ensuring of the security of the processing as required pursuant to Art. 32 GDPR;

ii. providing at minimum the information set out in Article 33(3) GDPR in the case of a Personal Data protection breach;

iii. the communication to the data subjects after a Personal Data protection breach, in particular pursuant to Article 34 GDPR;

iv. the performance of prior (i.e. before the start of the processing) checking according to data protection impact assessments pursuant to Art. 35 GDPR;

v. a prior consultation with a supervisory authority pursuant to Art. 36 GDPR.

The provision of services pursuant to (ii) and (iii) shall be provided free of charge for the Customer. For the provision of services pursuant to (i), (iv) and (v), the costs including SmartRecruiters' ones shall be borne by Customer.

12.3 SmartRecruiters commits to observe any and all other duties that imposed to processors pursuant to Article 28 GDPR

12.4 SmartRecruiters shall collaborate with the data protection officer of the Customer to generate the records of processing activities, pursuant to Article 30 GDPR, and provide all the necessary details to the Customer.

13. Miscellaneous

13.1 No modification of this Data Processing Agreement shall be valid and binding unless made in writing and then only if such modification expressly states that such modification applies to the regulations of this Data Processing Agreement. The foregoing shall also apply to any waiver or modification of this mandatory written form.

13.2 This Data Processing Agreement shall take precedence over any conflicting provisions of the Main Agreement.

13.3 This Data Processing Agreement shall be governed by the laws of the country where Customer is established.

SmartRecruiters, Inc.

Signature:

Print Name: Jerome Ternynck

Titel: CEO & Founder

Date: 24 April 2018

Customer legal name:

Signature

Print Name:

Titel:

Date:

Annex 1 - Standard Contractual Clauses (Processors)

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: ....

Address:...

Tel.: ....; fax:....................................; e-mail:.....................................

Other information needed to identify the organisation:

……………………………………………………………

(the data **exporter**)

And

Name of the data importing organisation: SmartRecruiters, Inc.

Address: 225 Bush Street, Suite #300, San Francisco CA 94104

e-mail: dpo@smartrecruiters.com

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law***'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature:

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Jerome Ternynck

Position: CEO & Founder

Address: 225 Bush Street, Suite #300, San Francisco CA 94104

Signature:

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

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

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
The data importer is SmartRecruiters, Inc., a service provider for HR recruitering services operating the SmartStart Talent Acquisition Platform. The SmartStart Talent Acquisition Platform receives the personal data of candidates / potential employees of the Data exporter for the purposes of providing services as set forth in the Main Agreement.

Data subjects
Reference is made to section 3.5 of the Data Processing Agreement.

Categories of data
Reference is made to section 3.5 of the Data Processing Agreement.

Special categories of data (if appropriate)
Reference is made to section 3.5 of the Data Processing Agreement.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify): The processing operation are in general as follows: Recruiting – Talent Acquisition process (storage, hosting and process activites) further speficied in the Main Agreement between Data Exporter and Data Importer.

DATA EXPORTER

Name:………………………………

Authorised Signature: ……………………

DATA IMPORTER

Name: Jerome Ternynck

Authorised Signature :

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please refer to Annex 2 of the Data Processing Agreement signed between Data Exporter and SmartRecruiters, Inc.

Annex 2 – Technical and Organizational Measures

1. Access control to premises and facilities

Technical and organizational measures to control access to premises and facilities, particularly to check authorization:

a) Security perimeters are defined and used to protect areas that contain either sensitive or critical information and information processing facilities
b) Physical security for offices, rooms and facilities are designed and applied
c) Physical protection against natural disasters, malicious attack or accidents are designed and applied
d) Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities
e) 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
f) Mobile equipment has appropriate protections (encryption)
g) A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities is adopted
h) Equipment is sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access
i) It is ensured that only authorized persons can access premises and company buildings where customers' data is stored or processed
j) 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:

a) An access control policy is established, documented and reviewed based on business and information security requirements
b) Users are provided with access to the network and network services that they have been specifically authorized to use
c) The allocation and use of privileged access rights is restricted and controlled
d) A formal user access provisioning process is implemented to assign or revoke access rights for all user types to all systems and services
e) The allocation of secret authentication information is controlled through a formal management process
f) 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
g) Password policy is known and implemented by every employee of SmartRecruiters
h) Password management system ensures quality passwords
i) The Local Administrator and other privileged accounts passwords never appear unscrambled on the network
j) Inactive session are shut down after a defined period of inactivity

k) Access to Information and application system functions by users and support personnel are restricted in accordance with the defined access control policy

l) 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:

a) An access control policy to customer's data is established, documented and reviewed based on business and information security requirements

b) SmartRecruiters implemented a comprehensive encryption solution for data in transit (incl. Network)

c) Database storages are encrypted.

d) Operating Systems are hardened to enforce required security controls

e) SmartRecruiters ensures that procedures are established which guarantee correctness, integrity and availability of SmartRecruiters data throughout all stages of data processing

f) 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:

a) Access to systems that keep or process customer's data is allowed via secured network connections

b) Logging facilities and log information is protected against tampering and unauthorized access

c) 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:

a) Security related application events are logged on application level

b) Log entries identify the individual whose action is being audited, the individual affected by the action and the time of the action

c) 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):

a) Unambiguous wording of the Data Processing Agreement between SmartRecruiters and the Customer with clear specifications of SmartRecruiters' and the Customer's obligations

b) Careful selection of SmartRecruiters as processor by the Customer

c) Monitoring of the performance of the Data Processing Agreement on a regular basis by SmartRecruiters and the Customer

7. Availability control

Measures to assure data security (physical/logical):

a) SmartRecruiters developed a disaster recovery plan, which contains all the procedures and support Information required for business resumption
b) SmartRecruiters' procedures are established which guarantee correctness, integrity and availability of SmartRecruiters data throughout all stages of data processing
c) Access to backups is restricted to authorized personnel only
d) Backups are encrypted
e) 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:

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

Annex 3 –Subprocessors

Name of Company:	Location:	Order of the Processing:
SmartRecruiters Sp. z o.o.	Fabryczna 20, 31-553 Krakow Poland	Operation, maintenance, support and testing of the e-Recruiting system.
Amazon Web Services Inc.	10 Terry Avenue North Seattle, WA 98109-5210 USA	Hosting of the data. Hosting location is the cluster AWS Germany (Frankfurt, Germany, EU), exact address is not disclosed by AWS.
SendGrid Inc.	1801 California Street, Suite 500 Denver Colorado 80202 USA	This subcontractor is used to power the sending and receiving of emails from the platform to the candidate/applicant and users of the Customer. The contents of that email can be partly templated by the Customer to include tags to personalize (e.g. First Name, title, job applied for etc.).
TextKernel BV	Nieuwendammerkade 28A17 Amsterdam, Noord-Holland 1022 AB Netherlands	This subcontractor will take a candidate’s uploaded CV/documents and parse' the data into the database (so it scans the document for first name and adds that data to the database field etc).