JOBVITE

JOBVITE DATA PROCESSING ADDENDUM AND

STANDARD CONTRACTUAL CLAUSES

Instructions and Effectiveness. This Addendum has been pre-signed on behalf of Jobvite. To enter into this Addendum, Customer must:

- **Be a Customer of the Services;**
- **Complete the signature block below by signing; and**
- **Submit the completed and signed Addendum to Jobvite at privacy@employinc.co or directly to your Customer Success Manager.**
- **This Addendum will only be effective (as of the Effective Date) if executed and submitted to Jobvite accurately. If you make any deletions or other revisions to this Addendum, it will be null and void.**
- **Customer signatory represents to Jobvite that he or she has the legal authority to bind the Customer and is lawfully able to enter into contracts (e.g., is not a minor).**
- **This Addendum will terminate automatically upon termination of the Agreement or as earlier terminated pursuant to the terms of this Addendum.**

This Data Processing Addendum ("Addendum") amends and supplements the Master Subscription Agreement or Master Product Agreement, as applicable ("*Agreement*"), between the Customer and Employ, Inc. ("Jobvite") and is effective on the last date of signature set forth below. The terms of the Agreement apply to this Addendum; provided, however***, if there is any conflict between the terms of this Addendum and the Agreement regarding the Parties' respective privacy and security obligations, the provisions of this Addendum will control.***

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement**. Nothing in this Addendum is intended to alter or have any adverse effect on the Standard Contractual Clauses incorporated into this Addendum in EXHIBIT 1 ("Standard Contractual Clauses"). In the event that a competent government authority determines that a conflict exists between the Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail. If there is a conflict between any other agreement between the Parties including the Agreement and this Addendum, the terms of this Addendum will control.**

1. **Introduction**

1.1. **Definitions.**

1.1.1."*controller*", "*processor*", "*data subject*", "*personal data*" and "*processing*" (and "*process*") means the meanings given in Applicable Data Protection Law. For the purposes of the California Consumer Privacy Act ("CCPA") and California Privacy Rights Act ("CPRA") personal data will mean "*Personal Information*", controller will mean "*Business*", processor

will mean "*Service Provider*", and data subject will mean "*Consumer*" as defined in the CCPA and/or CPRA.

1.1.2. "*Applicable Data Protection Law*" means data protection laws in the United States, Canada, United Kingdom, Switzerland, and the European Union including Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and the UK GDPR and the Data Protection Act 2018 ("*General Data Protection Regulation*" or "*GDPR*").

1.1.3. **"***Customer Account Data***"** means personal data that relates to Customer's relationship with Jobvite, including the names and/or contact information of individuals authorized by Customer to access Customer's Jobvite Product account and billing and/or contact information of individuals that Customer has associated with its Jobvite Product account.

1.1.4. **"***Customer Usage Data***"** means data processed by Jobvite for the purposes of managing the use of the Jobvite Product; including data used to trace and identify the activities of a user of the Jobvite Product, and the date, time, duration and the type of use.

1.1.5. **"***Customer Data***"** means data provided to Jobvite by Customer for processing by the Jobvite Product including the results of such processing.

1.1.6. *"Security Objectives"* means protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (in particular where the processing involves the transmission of data over a network) and against all other unlawful forms of processing.

1.1.7. *"Jobvite Data"* means any personal data provided to Customer by Jobvite related to the activities contemplated under the Agreement or this Addendum, such as personal data Customer may obtain in the course of performing a permitted audit of Jobvite.

1.1.8. **"***Jobvite Product***"** means the Jobvite Services as defined in the Agreement.

1.2. **Relationship of the Parties.** The parties acknowledge and agree that with regard to the processing of Customer Data, Customer is a controller or processor, as applicable, and Jobvite is a processor. With regard to the processing of Customer Account Data and Customer Usage Data, Customer is a controller, and Jobvite is an independent controller, not a joint controller with Customer.

2. **Jobvite Obligations**

2.1. Obligation: Jobvite will comply with Applicable Data Protection Laws which impose an obligation directly upon Jobvite as a Processor by virtue of the specific Processing of Customer Data that Jobvite is doing related to Jobvite Products. Jobvite is not responsible for determining the requirements of laws or regulations applicable to Customer's business, or whether a Jobvite Product and related Processing by Jobvite meets the requirements of any such applicable laws or regulations. As between the parties, Customer is responsible for the lawfulness of the Processing of the Customer Data. Customer will not use the Jobvite Product or request Processing by Jobvite in a manner that would violate Applicable Data Protection Laws.

2.2. Details of the processing.

JOBVITE

2.2.1. Subject Matter: Jobvite's provision of the Jobvite Product to Customer.

2.2.2. Purpose of the Processing: The purpose of the data processing under this Addendum is the provision of the Jobvite Product as initiated by Customer from time to time.

2.2.3. Restriction: Jobvite shall not: (a) sell Customer personal data; (b) retain, use, or disclose Customer personal data for any purpose other than for the specific purpose of providing the Jobvite Product in accordance with the Agreement; (c) retain, use, or disclose personal data for a commercial purpose other than providing the Jobvite Product; or (d) retain, use, or disclose Customer personal data outside of the direct business relationship between Customer and Jobvite. Jobvite certifies that Jobvite understands the restrictions in this Section and will comply with them in accordance with the requirements of Applicable Data Protection Laws, including the CCPA.

2.3. **Customer Instructions.** Customer appoints Jobvite as a processor to process Customer Data on behalf of, and in accordance with, Customer's instructions as set out in the Agreement and this Addendum, as otherwise necessary to provide the Jobvite Product, or as otherwise agreed in writing ("*Permitted Purposes*"). Additional instructions outside the scope of the Agreement, this Addendum, or as otherwise needed to provide the Jobvite Product may result in additional fees payable by Customer to Jobvite for carrying out those instructions. Customer shall ensure that its instructions comply with all laws, regulations and rules applicable to the Customer Data and the related processing, and that Jobvite's processing of the Customer Data in accordance with Customer's instructions will not cause Jobvite to violate any applicable law, regulation or rule, including Applicable Data Protection Law. Jobvite agrees not to retain, use, or disclose Customer Data, except to provide, operate, maintain or operate the Jobvite Product as provided for in the Agreement, or as necessary to comply with the law or other binding governmental order. Jobvite shall inform Customer if it becomes aware or reasonably believes that Customer's data processing instructions violate Applicable Data Protection Law.

2.4. **Confidentiality of Customer Data and Responding to Third Party Requests.**

2.4.1. Data Subject Requests. If Jobvite receives a request from any Data Subject made under Data Protection relating to Customer Data, Jobvite will provide a copy of that request to the Customer within two (2) business days of receipt. Jobvite provides Customer with tools to enable Customer to respond to a Data Subjects' requests to exercise their rights under the Data Protection Laws. To the extent Customer is unable to respond to Data Subject's request using these tools, Jobvite will provide reasonable assistance to the Customer in responding to the request.

2.4.2. Supervisory Authority Requests. Jobvite will assist Customer in addressing any communications and abiding by any advice or orders from the Supervisory Authority relating to the Customer Data.

2.4.3. Retention. Jobvite will retain Customer Data only for as long as the Customer deems it necessary for the Permitted Purpose, or as required by applicable laws. At the termination of this DPA, or upon Customer's written request, Jobvite will either destroy or return the Customer Data to the Customer, unless legal obligations require storage of the Customer Data.

2.4.4. Disclosure to Third Parties and Confidentiality. Jobvite will not disclose the Customer Data to third parties except as permitted by this DPA or the Agreement, unless Jobvite is required to disclose the Customer Data by applicable laws, in which case Jobvite shall (to the extent permitted by law) notify the Customer in writing and liaise with the Customer before complying with such disclosure request. Jobvite treats all Customer Data as strictly confidential and requires all employees, agents, and Sub-processors engaged in Processing the Customer Data to commit themselves to confidentiality, and not Process the Customer Data for any other purposes, except on instructions from Customer.

2.4.5. Assistance. Taking into account the nature of the Processing and the information available, Jobvite will provide assistance to Customer in complying with its obligations under GDPR Articles 32-36 (inclusive) (which address obligations with regard to security, breach notifications, data protection impact assessments, and prior consultation). Upon request, Jobvite will provide Customer a list of processing operations.

2.5. **Subcontracting.** Customer consents to Jobvite engaging third party sub-processors to process Customer Data for Permitted Purposes provided that:

2.5.1. A current list of Jobvite's sub-processors can be found at www.jobvite.com/terms-of-use/sub-processors/. Jobvite shall provide details of any change in sub-processors at least ten (10) days prior to any such change either by email or via the Jobvite Product;

2.5.2. Jobvite imposes data protection terms on any sub-processor it appoints that require it to protect the Customer Data to the standard required by Applicable Data Protection Law; and

2.5.3. Jobvite remains liable for any breach of this Addendum that is caused by an act, error, or omission of its sub- processor on the same basis as if it had made such act, error, or omission.

2.5.4. If Customer has a reasonable basis to object to Jobvite's use of a new Sub-processor, Customer will notify Jobvite promptly in writing within 15 days after receipt of a New Sub-processor Notice. Jobvite will use reasonable efforts to make available to Customer a change in the affected Services or recommend a commercially reasonable change to Customer's configuration or use of the affected Services to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Jobvite is unable to make available such change within a reasonable period of time, which

JOBVITE

will not exceed 30 days, Customer may terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the objected-to new Sub-processor by providing written notice to Jobvite.

2.6. **Deletion of Customer Data.** Following termination or expiry of the Agreement, Jobvite, in accordance with the Agreement, shall provide Customer with a copy of the Customer Data and delete the same. This requirement will not apply to the extent that Jobvite is required by law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Jobvite shall securely isolate and protect from any further processing until deletion in accordance with the Agreement, except to the extent required by law.

2.7. **Third Party Certifications & Audit Obligations.**

2.7.1. **Jobvite Certification/SOC Report**. In addition to the information contained in this DPA, upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement place, Jobvite will make available the following documents and information regarding the System and Organization Controls (SOC) 2 Report (or the reports or other documentation describing the controls implemented by Jobvite that replace or otherwise available by Jobvite), so that Customer can reasonably verify Jobvite's compliance with its obligations under this DPA

2.7.2. **Jobvite's Audit Program.** To the extent the reports provided in Section 2.7.1 do not verify Jobvite's compliance with its obligations under this DPA, and subject to the audit requirements described in Clause 8 of the Standard Contractual Clauses, Customer may audit Jobvite's compliance with this DPA up to once per year, unless requested by a Supervisory Authority or in the event of a Security Incident. Such audit will be conducted by an independent third party ("Auditor") reasonably acceptable to Jobvite. Jobvite will work cooperatively with Customer and Auditor to agree on a final audit plan in advance of the audit. The results of the inspection and all information reviewed during such inspection will be deemed Jobvite's confidential information and shall be protected by Auditor in accordance with the confidentiality provisions to be made between Jobvite and Auditor. Notwithstanding any other terms, the Auditor may only disclose to the Customer specific violations of the Addendum, if any, and the basis for such findings, and shall not disclose to Customer any of the records or information reviewed during the inspection.

3. **Security**

3.1. **Security Measures.** Jobvite has implemented and shall maintain appropriate technical and organizational measures ("*Security Standards*") to protect Customer Account Data, Customer Usage Data, and Customer Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to such data (a "*Security Incident*"). Security Standards are described in Annex II.

JOBVITE

3.2. **Determination of Security Requirements.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR. Jobvite is not responsible for determining the requirements of laws applicable to Customer's business or that Jobvite's provision of the Services meet the requirements of such laws.

3.3. **Security Incident Notification.** Jobvite shall, to the extent permitted by law, prompyly after becoming aware of any Security Incident. Jobvite's notification of a Security Incident to the Customer to the extent known should include: (a) the nature of the incident; (b) the date and time upon which the incident took place and was discovered; (c) the number of data subjects affected by the incident; (d) the categories of Customer Data involved; (e) the measures, such as encryption, or other technical or organizational measures, that were taken to address the incident, including measures to mitigate the possible adverse effects; (f) whether such proposed measures would result in a disproportionate effort given the nature of the incident; (g) the name and contact details of the data protection officer or other contact; and (h) a description of the likely consequences of the incident. The Customer alone may notify any public authority..

4. **International Transfers of Data and GDPR Transfers**

4.1. Customer is responsible to ensure that the transfer of personal data out of the jurisdiction it originated to Jobvite complies with Applicable Data Protection Law ("**Legal Basis for Transfer**"). The Parties agree the Standard Contractual Clauses, as identified in Exhibit A (including Annex IV), will apply to Customer Data that is transferred outside the EEA or UK, either directly or via onward transfer, to any country not recognized by the European Commission as providing as adequate level of protection for personal data (as described by the GDPR).

5. **UK GDPR**. As applicable to Annex IV, references in Exhibit A to the Supervisory Authority shall be construed to include the The Information Commissioner as the UK's independent data protection authority. The governing law for interpretation of claims arising under the UK GDPR shall be the laws of England and Wales.

6. **Switzerland Transfers**. To the extent applicable, Personal Data transferred from Switzerland for which Swiss law governs the international nature of the transfer, (i) references to the GDPR in Clause 4 of the Standard Contractual Clauses are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority shall include the Swiss Federal Data Protection and Information Commissioner; and (ii) as so amended, the Standard Contractual Clauses are incorporated herein by reference and shall apply, form a part of this DPA, and take precedence over this DPA to the event ofany conflict.

7. Miscellaneous.

7.1. **Obligations Post-termination**. Termination or expiration of this DPA shall not discharge the Parties from their obligations meant to survive the termination or expiration of this DPA.

JOBVITE

7.2. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invaliding the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The Parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this DPA.

7.3. **Updating to Reflect Changes to Applicable Data Protection Laws.** To the extent required, the Parties undertake to reasonably re-negotiate this Addendum to reflect changes made to a Party's obligations under Applicable Data Protection Laws. The Parties acknowledge that substantial changes to a Party's obligations may be subject to changes in Fees for the Jobvite Services or may not be able to be made. For example, a data protection law in a country that would require Customer Data to be stored physically separate from other third-party data, or to be stored and processed solely on servers physically located in such country.

6.2. **Liability**. Any claims brought under pursuant to this Addendum or any Exhibit hereto will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

6.3. **Entire Agreement**. This Addendum supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing or security addenda entered into between Jobvite and Customer.

Accepted and agreed to as of the Effective Date by the authorized representative of each party:

Employ, Inc.

By: DocuSigned by: David Hollady DC5570F83C534CC...

Name: David Hollady

Title: VP of Legal & DPO

Date: 01/03/2023

Customer Name: _____

By: _____

Name: _____

Title: _____

Date: _____

JOBVITE

EXHIBIT 1

EXHIBIT A

Controller to Processor Standard Contractual Clauses

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

This data transfer agreement is between

Customer who has executed the Agreement into which the above Data Protection Addendum is incorporated, hereafter "data exporter"

And

Employ, Inc., 20 North Meridian Street, Suite 300, Indianapolis, IN 46204-3028 USA hereinafter "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.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional (Excluded)

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete

all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([1]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fourteen (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses,

including in terms of third-party beneficiary rights for data subjects. ([2]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([3]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of

appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

JOBVITE

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

JOBVITE

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor):

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Employ, Inc.

Address: 20 N. Meridian Street, Suite #300 Indianapolis, Indiana 46204

Contact person's name, position and contact details: David Hollady, VP of Legal and DPO, privacy@employinc.com

Activities relevant to the data transferred under these Clauses:

The Personal Data will be processed for the provision of "Functions" as agreed upon by the Parties and as set out in the Agreement. The duration of processing; specific processing activities; categories of data subjects and categories of data processed; and the sub-processors who will have access to the Personal Data are described in this agreement.

Jobvite is a talent acquisition platform, used by its Customers to attract or recruit talent. The data is used to manage the recruitment process.

Signature and date: _____ DocuSigned by: David Hollady DC5570F83C534CC... 01/03/2023

Role (controller/processor): Processor

2. …

JOBVITE

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Natural persons who submit personal data to the data importer via use of the Services (including via online job applications and email communication hosted by the data importer on behalf of the data exporter) (“ Applicants”).
- The data exporter’s users who are authorized by the data exporter to access and use the Services.

Categories of personal data transferred

Data relating to individuals provided to Jobvite via the Services, by or at the direction of Customer. The Customer may submit Customer Data to the Services, and may request for Applicants to submit Customer Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, without limitation:

- Customer Data of all types that may be submitted by Applicants to the Customer via user of the Services (such as via job applications). For example: name, geographic location, age, contact details, IP address, profession, gender, employment history, employment references, salary and other preferences and other personal details that the data exporter solicits or desires to collect from its Applicants.
- Customer Data of all types that Jobvite may include in forms hosted on the Services for the Customer (such as may be included in a job application or interview feedback forms), or may be requested by Customer via customizable fields.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Applicants may submit special categories of Personal Data to the data exporter via the Services, the extent of which is determined and controlled by the data exporter. For clarity, these special categories of Personal Data may include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous bases.

Nature of the processing

Jobvite provides recruiters with the tools they need to find, market to, and hire top talent more effectively. Our technology also enables job seekers to navigate career sites more easily, identify authentic corporate cultures, and ultimately connect with meaningful employment. Purpose(s) of the data transfer and further processing

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Jobvite Customers can configure data retention policies specific to their needs in the platform using built-in product functionality. Customers can configure automatic anonymization or deletion actions for personal data records based on geographic regions to meet varying privacy regulations. Jobvite does not delete Customer data or configure retention policies for Customers.

JOBVITE

Jobvite initiates the deletion of all Customer data from the production systems 30 days following contract termination so that such data is deleted by 45 days after contract termination.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Jobvite uses various sub-processors to deliver it's talent acquisition platform. The sub- processors provide various services like datacentre/hosting, sending emails/text messages etc. Refer to Annex III of this DPA, for a list of sub-processors and the functionalities they provide. Data retention as defined above also applies for sub-processors when applicable.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Customer's competent supervisory authority is: Irish Data Protection Commission.

JOBVITE

ANNEX II

The technical and organizational measures adopted by Jobvite to ensure the security of data can be found at: https://www.jobvite.com/security-exhibit/

JOBVITE

ANNEX III

LIST OF SUB-PROCESSORS

The current list of Jobvite's subprocessors is available at: www.jobvite.com/terms-of-use/sub-processors/.

The controller has authorised the use of the following sub-processors:

Jobvite uses third party Jobvites for operational and business efficiency and to extend service functionality to our Customers. We maintain vendors for the following services:
- Website analytics tools
- Sales relationship management and Customer Support software
- Tools used to manage Customer support requests - HRIS integration partner
- Staff augmentation/Contractors
- Cloud Hosting provider
- Employee referral add-on (100% owned subsidiary)
- Recruitment marketing add-on (100% owned subsidiary)
- Provider of text service/function within the Jobvite application (100% owned subsidiary)

The current list of our affiliates, subcontractors, their purpose, and geographic location is available on our website at: www.jobvite.com/terms-of-use/sub-processors/
All subprocessors used are subject to an annual vendor review process to ensure that they have appropriate security controls for the processing and data access that they have and that there is an appropriate legal basis for the transfer of EU data, where applicable, to them for processing (i.e. privacy shield, EU standard contractual clauses, adequacy decision).

JOBVITE

ANNEX IV

International Data Transfer Addendum to the EU Standard Contractual Clauses

1. Part 1: Tables

Table 1: Parties

Start date	As of full execution of this Addendum	
The Parties	**Exporter (who sends the Restricted Transfer).**	**Importer (who receives the Restricted Transfer).**
Parties' details	Full legal name: _____ Main address: _____ _____ _____	Full legal name: Employ, Inc Main address: 20 N. Meridian St., Suite #300 Indianapolis, IN 46204 Official registration number (if any): N/A
Key contact	Name: _____ Title: _____ Contract: _____	David Hollady, VP of Legal & DPO privacy@employinc.com
Signature (if required for the purposes of Section 2)	See execution page.	See execution page.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
Module	**Module in operation?**	**Clause 7 (Docking Clause)**	**Clause 11 (Option)**	**Clause 9a (Prior Authorisation or General Authorisation)**	**Clause 9a (Time period)**	**Is personal data received from the Importer combined with other personal data collected by the Exporter?**

JOBVITE

1	No					
2	Yes	No	No	General authorization	30 days	
3	No					
4	No					

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties	See the details set out in Table 1 above.
Annex 1B: Description of Transfer	***Categories of data subjects whose personal data is transferred*** Data subjects include: - Natural persons who submit personal data to the Importer via use of the Services (including via online job applications and email communication hosted by the data importer on behalf of the data exporter) ("Applicants"). - The Exporter's users who are authorized by the Exporter to access and use the Services. ***Categories of personal data transferred*** Data relating to individuals provided to Jobvite via the Services, by or at the direction of the Exporter. The Exporter may submit Customer Data to the Services, and may request for Applicants to submit Customer Data to the Services, the extent of which is determined and controlled by the Exporter in its sole discretion, and which may include, without limitation: - Customer Data of all types that may be submitted by Applicants to the Exporter via use of the Services (such as via job applications). For example: name, geographic location, age, contact details, IP address, profession, gender, employment history, employment references, salary and other preferences and other personal details that the data exporter solicits or desires to collect from its Applicants. - Customer Data of all types that Jobvite may include in forms hosted on the Services for the Exporter (such as may be included in a job application or interview feedback forms), or may be requested by Exporter via customizable fields. ***Sensitive data transferred (if applicable)*** Applicants may submit special categories of Personal Data to the data exporter via the Services, the extent of which is determined and controlled by the data exporter. For clarity, these special categories of Personal Data may

JOBVITE

	include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. ***Frequency of the transfer*** Continuous ***Nature of the processing*** The Importer and the Exporter have entered into a Master Services Agreement ("**MSA**") governing the Importer's use of the recruitment software provided by the Exporter. The data set out above will be routinely accessed from the Importer's systems pursuant to the provision of the Services. Any use of capitalised terms in this Addendum which are not otherwise defined herein shall have the meanings given to them in the MSA. ***Purposes of the data transfer and further processing*** For the purposes of delivering the Services (including administration, operations, technical and Customer support). ***The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*** During the Service Term identified in the Order Form. ***For transfers to (sub-)processors, specify the subject matter, nature and duration of the processing*** Same as per the above.
Annex II: Technical and organisational measures	The Importer shall comply with the technical and organisational measures set out in Part 3 of this Addendum.

<u>Table 4:</u> Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	**Which Parties may end this Addendum as set out in Section 19:** Only Importer may end or modify this Addendum except by mutual written agreement.

2.

3. <u>Part 2: Mandatory Clauses</u>

JOBVITE

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to *"Regulation (EU) 2016/679"*, *"Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"* and *"that Regulation"* are all replaced by *"UK Data Protection Laws"*. References to specific Article(s) of *"Regulation (EU) 2016/679"* are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

    h. References to the *"European Union"*, *"Union"*, *"EU"*, *"EU Member State"*, *"Member State"* and *"EU or Member State"* are all replaced with the *"UK"*;

    i. The reference to *"Clause 12(c)(i)"* at Clause 10(b)(i) of Module one, is replaced with *"Clause 11(c)(i)"*;

    j. Clause 13(a) and Part C of Annex I are not used;

    k. The *"competent supervisory authority"* and *"supervisory authority"* are both replaced with the *"Information Commissioner"*;

l. In Clause 16(e), subsection (i) is replaced with:

> *"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;"*;

m. Clause 17 is replaced with:

> *"These Clauses are governed by the laws of England and Wales."*;

n. Clause 18 is replaced with:

> *"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."*; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 *"Ending the Addendum when the Approved Addendum changes"*, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or

    b. its risk under the Addendum,

JOBVITE

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

4. Part 3: Technical and Organisational Measures

The technical and organisational measures adopted by the Importer shall include the following:
See Annex II.