



EMPLOY GDPR DATA PROCESSING ADDENDUM AND STANDARD CONTRACTUAL CLAUSES

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

- **Be a Customer of the Services;**
- **Complete the signature block below by signing; and**
- **Submit the completed and signed DPA to Employ at privacy@employinc.co or directly to your Customer Success Manager.**
- **This DPA shall be effective the later of: (a) the date Employ receives a complete and executed DPA from the Customer indicated in the signature block above (the “Effective Date”).**
- **Customer signatory represents to Employ 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 Data Protection Addendum ("Addendum") is entered into as of _____, (the “Effective Date”), by and between the Customer specified in the table below (“Customer”) and Employ, Inc., on behalf of itself and its Affiliates (collectively, “Employ”).

<p>Employ, Inc.</p> <p>Signature: _____  <small>AF44F7A36CBF4E4...</small></p> <p>Name: <u>David Hollady</u></p> <p>Title: <u>VP Legal</u></p>	<p>Customer</p> <p>Name</p> <p>Signature: _____</p> <p>Name: _____</p> <p>Title: _____</p>
<p>Address: 20 North Meridian Street, Suite 300, Indianapolis, IN 46204-3028 USA</p>	<p>Address: Customer street address, City, State, zip</p>
<p>DPO/Contact for data protection enquiries: Name: Privacy Team</p> <p>Email: <u>privacy@employinc.com</u></p>	<p>DPO/Contact for data protection enquiries Name/Role: _____</p> <p>Email: _____</p>

This Addendum amends and supplements the Master Subscription Agreement or Master Product Agreement, as applicable, between the Parties (“Agreement”). 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.

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.

1.1.2. "Applicable Data Protection Law" means data protection laws in the United States, 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 Employ, including the names and/or contact information of individuals authorized by Customer to access Customer's Employ Product account and billing and/or contact information of individuals that Customer has associated with its Employ Product account.

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

1.1.5. "Customer Data" means data provided to Employ by Customer for processing by the Employ 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. "Employ Data" means any personal data provided to Customer by Employ 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 Employ.

1.1.8. "Employ Product" means the Employ 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 Employ is a processor. With regard to the processing of Customer Account Data and Customer Usage Data, Customer is a controller, and Employ is an independent controller, not a joint controller with Customer.

2. Employ Obligations

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

2.2. Details of the processing.



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

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

2.2.3. Data Processing, Transfer, and sales. Employ will process Customer Data only as necessary to perform the services.

2.2.4. Restriction: Employ shall not: Collect, combine, disclose, share, use, retain, access, transfer, or otherwise use Customer Data except as required to provide the Services. Employ will refrain from any action that would cause any transfer of Customer Data to qualify as sharing or selling personal data, as that term is defined under Applicable Law, except that Employ will not be responsible for any third party Customer may integrate with the services. Employ shall not combine Customer Data with data obtained from source including Employ's own internal sources. Employ certifies that Employ 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 Employ 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 Employ 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 Employ Product may result in additional fees payable by Customer to Employ 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 Employ's processing of the Customer Data in accordance with Customer's instructions will not cause Employ to violate any applicable law, regulation or rule, including Applicable Data Protection Law. Customer is responsible for providing the necessary notice to the Data Subjects under the Data Protection Laws. Customer is responsible for obtaining, and demonstrating evidence that it has obtained, all necessary consents, authorizations and required permissions under the Data Protection Laws in a valid manner for Employ to perform the Services.

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

2.4.1. Data Subject Requests. If Employ receives a request from any Data Subject made under Data Protection relating to Customer Data, Employ will provide a copy of that request to the Customer within two (2) business days of receipt. Employ 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, Employ will provide reasonable assistance to the Customer in responding to the request.



2.4.2. Supervisory Authority Requests. Employ 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. Employ 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, Employ will destroy the Customer Data to the Customer, unless legal obligations require storage of the Customer Data. Except as may be stated otherwise in the Agreement between the Parties, Customer is responsible for the retrieval of their data through available functionality or the purchase of the associated professional services.

2.4.4. Disclosure to Third Parties and Confidentiality. Employ will not disclose the Customer Data to third parties except as permitted by this DPA or the Agreement, unless Employ is required to disclose the Customer Data by applicable laws, in which case Employ shall (to the extent permitted by law) notify the Customer in writing and liaise with the Customer before complying with such disclosure request. Employ 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, Employ will provide assistance to Customer in complying with its obligations under applicable Data Protection Laws (which address obligations with regard to security, breach notifications, data protection impact assessments, and prior consultation). Upon request, Employ will provide Customer a list of processing operations.

2.4.6. and provide the features and functionality to allow Progressive to comply with its obligations

2.5. Deletion of Customer Data. Following termination or expiry of the Agreement, Employ, 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 Employ 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 Employ shall securely isolate and protect from any further processing until deletion in accordance with the Agreement, except to the extent required by law.

2.6. Third Party Certifications & Audit Obligations.

2.6.1. Employ 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, Employ 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 Employ that replace or otherwise



available by Employ), so that Customer can reasonably verify Employ's compliance with its obligations under this DPA

2.6.2. Employ's Audit Program. To the extent the reports provided in Section 2.7.1 do not verify Employ'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 Employ'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 Employ. Employ 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 Employ's confidential information and shall be protected by Auditor in accordance with the confidentiality provisions to be made between Employ 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. Employ 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 III.

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. Employ is not responsible for determining the requirements of laws applicable to Customer's business or that Employ's provision of the Services meet the requirements of such laws.

3.3. Security Incident Notification. Employ shall, to the extent permitted by law, promptly after becoming aware of any Security Incident. Employ'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.

3.4. Remediation. If Customer has reasonable cause to suspect that Employ is providing the platform



in a manner consistent with applicable Data Protection laws and may be allowing unauthorized use of personal information, Customer may (i) submit an inquiry to privacy@employinc.com, (ii) cease use of their license until they are able to confirm Employ's compliance, or (iii) with evidence of non-compliance of applicable Data Protection Laws terminate the Agreement between the parties.

3.5. Notice of Inability to Meet Obligations. Employ will provide notice if it believes it can no longer meet its obligations under this Data Protection Agreement, including applicable Data Protection Laws.

4. Subprocessor

4.1. SCC's. Pursuant to Clause 9 of the Standard Contractual Clauses, Customer acknowledges and expressly agrees Employ may engage new Sub-processors as described in Section 4 of this DPA.

4.2. General Consent. Customer agrees that Employ may engage third-party Sub-processors in connection with the provision of Services, subject to compliance with the requirements below. As a condition to permitting a Sub-processor to Process Customer Data, Employ will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor. Employ will provide copies of any Sub-processor agreements to Customer pursuant only upon reasonable request by Customer. To the extent necessary to protect business secrets or other confidential information, including personal data, Employ may redact the text of the agreement prior to sharing a copy.

4.3. Current Sub-processor List. Customer acknowledges and agrees that Employ may engage its current Sub-processors listed in Annex IV. Written Notice Via Mailing List. Employ will provide Customer with notice ("New Sub-processor Notice") of the addition of any new Sub-processor to the Sub-processor List at any time during the term of the Agreement. Employ will provide Customer with additional information about any Sub-processor on the Sub-processor List that Customer may reasonably request upon receipt of a New Sub-processor Notice

4.4. Customer Objection. If Customer has a reasonable basis to object to Employ's use of a new Sub-processor, Customer will notify Employ promptly in writing within 15 days after receipt of a New Sub-processor Notice. Employ 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 Employ is unable to make available such change within a reasonable period of time, which 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 Employ.

4.5. Responsibility. Employ will remain responsible for its compliance with the obligations of this DPA and for any acts and omissions of its Sub-processors that cause Employ to breach any of Employ's obligations under this DPA.

5. International Transfers of Data and GDPR Transfers



- 5.1. Customer is responsible to ensure that the transfer of personal data out of the jurisdiction it originated to Employ complies with Applicable Data Protection Law (“**Legal Basis for Transfer**”). The Parties agree that the Data Privacy Framework will apply to any Customer Data that is transferred outside the EEA, UK, or Swiss territories. Each Party agrees to comply with the principles of the Data Privacy Framework as may be further outlined in Exhibit A Annex 1. Should the Data Privacy Framework not apply or ever be invalidated, the Parties agree the Standard Contractual Clauses, as further outlined in Exhibit A (including Annexes I-IV), will apply to Customer Data that is transferred outside the EEA, UK, or Swiss territories, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described by the GDPR).

6. Miscellaneous.
 - 6.1. **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.

 - 6.2. **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 invalidating 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.

 - 6.3. **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 Employ 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 Employ and Customer.



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. and it’s Affiliates, 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 Standard 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.



ANNEX I

Transfer Mechanisms

1. Data Privacy Framework

1.1. Customer may confirm Employ or the applicable affiliate status under the Data Privacy Framework on the [active participant list](#).

1.2. Independent Recourse Mechanism: [JAMS](#)

2. STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS 2.1. Reference to the Standard Contractual Clauses. The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 2.

2.2. Docking clause. The option under clause 7 shall not apply.

2.3. Instructions. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to EMPLOY for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Customer to Process Personal Data are set out in section 2.3 of this DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.

2.4. Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by EMPLOY to Customer only upon Customer's written request.

2.5. Security of Processing. Security of Processing shall be provided as outlined in Annex III.

2.11. Supervision. Clause 13 shall apply as follows:

2.11.1. Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

2.11.2. Where Customer 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 shall act as competent supervisory authority.

2.11.3. Where Customer 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, Data Protection Commission of Ireland (DPC) shall act as competent supervisory authority.

2.11.4. Where Customer is established in the United Kingdom or falls within the territorial scope of application of the Data Protection Laws and Regulations of the United Kingdom ("UK Data Protection Laws and Regulations"), the Information Commissioner's Office ("ICO") shall act as competent supervisory authority.

2.11.5. Where Customer is established in Switzerland or falls within the territorial scope of application of the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws and



Regulations”), the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

2.12. Notification of Government Access Requests. For the purposes of clause 15(1)(a), EMPLOY shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

2.13. Governing Law. The governing law for the purposes of clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of Ireland; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of England and Wales..

2.14. Choice of Forum and Jurisdiction. The courts under clause 18 shall be those designated in the Venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) Ireland; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the courts of England and Wales shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

2.15. Appendix. The Appendix shall be completed as follows:

- The contents of section 1 of Schedule 2 shall form Annex I.A to the Standard Contractual Clauses
- The contents of sections 2 to 9 of Schedule 2 shall form Annex I.B to the Standard Contractual Clauses
- The contents of section 10 of Schedule 2 shall form Annex I.C to the Standard Contractual Clauses
- The contents of section 11 of Schedule 2 to this Exhibit shall form Annex II to the Standard Contractual Clauses.

2.16. Data Exports from the United Kingdom under the Standard Contractual Clauses. For data transfers governed by UK Data Protection Laws and Regulations, the Mandatory Clauses of the Approved Addendum, being the [template Addendum B.1.0](#) issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as revised under Section 18 of those Mandatory Clauses ("Approved Addendum") shall apply. The information required for Tables 1 to 3 of Part One of the Approved Addendum is set out in Schedule 2 of this DPA (as applicable). For the purposes of Table 4 of Part One of the Approved Addendum, neither party may end the Approved Addendum when it changes. Salesforce Data Processing Addendum Page 14 of 17 January 2023 online

2.17. Data Exports from Switzerland under the Standard Contractual Clauses. For data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity. In such circumstances, general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in Swiss Data Protection Laws (including the revised Federal Data Protection Act (revFADP)).

2.18. Conflict. The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.





ANNEX II

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: See signature in above Data Protection Addendum

Role (controller/processor): Controller

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.

Employ 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: See above signature in Data Protection Addendum

Role (controller/processor): **Processor**

...



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 Employ 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 Employ 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

Employ 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

Employ 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. Employ does not delete Customer data or configure retention policies for Customers.



Employ 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

Employ uses various sub-processors to deliver its 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.



ANNEX III

The technical and organizational measures adopted by Employ to ensure the security of data can be found at:

- For JazzHR: <https://www.jazzhr.com/security-exhibit/>
- For Jobvite, Talemetry, and Talentegy: <https://www.jobvite.com/security/>
- For Lever: <https://www.lever.co/security-exhibit/>



ANNEX IV

LIST OF SUB-PROCESSORS

The current list of Employ's subprocessors is available at:

- For JazzHR: www.JazzHR.com/subprocessors
- For Jobvite, Talentegy, & Talemtry: www.jobvite.com/terms-of-use/sub-processors/.
- For Lever: <https://www.lever.co/subprocessors/>

