Instructions

To enter into this DPA, Customer must:

- Have an executed Order Form;
- Completed the signature page below by providing items identified and signing in appropriate space;
- Submit the completed and signed DPA to JazzHR as notified;
- This DPA will only be effective if executed and submitted to JazzHR accurately and countersigned by JazzHR

If you make any deletions or other revisions to this DPA, it will be null and void. This DPA will terminate automatically upon termination or expiration of JazzHR services.

Data Protection Addendum

This Data Protection Addendum ("*Addendum*") is entered into as of ______________________, (the **"Effective Date"**), by and between the customer specified in the table below ("***Client***") and Hireku, Inc. (d/b/a JazzHR), ("JazzHR"), Inc., on behalf of itself and its Affiliates (collectively, "***SUPPLIER***").

JazzHR Signature: _________________________ Name: _________________________ Title: _________________________	**Client** **Name** Signature: _________________________ Name: _________________________ Title: _________________________
Address: 610 Lincoln Street, #205 Waltham, MA 02451	Address: Client street address, City, State, zip
DPO/Contact for data protection enquiries: Name: Privacy Team Email: privacy@JazzHR.com	DPO/Contact for data protection enquiries Name/Role: _________________________ Email: _________________________ If applicable, Client's competent supervisory authority in the EU is: [INSERT AUTHORITY].

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. For the purposes of the California Consumer Privacy Act ("CCPA") personal data will mean "*Personal Information*", controller will mean "*Business*", processor will mean "*Supplier*", and data subject will mean "*Consumer*" as defined in the CCPA.

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 ("*General Data Protection Regulation*" or "*GDPR*").

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

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

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

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

1.1.9. "*UK Addendum*" means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner and laid before Parliament in accordance with S119A(1) Data Protection Act 2018 on 2 February 2022 but, as permitted by Section 17 of such Addendum, the format of the information set out in Part 1 of the Addendum shall be amended as set out in Section 5.3 of this DPA

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

2. **Processor Obligations (Client Data)**

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

2.2. Details of the processing.

2.2.1. Subject Matter: SUPPLIER's provision of the SUPPLIER Product to Client.

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

2.2.3. Categories of Data: Data relating to individuals provided to SUPPLIER via the SUPPLIER Product, by (or at the direction of) Client or Client's end users.

2.2.4. Categories of Data Subjects: Data subjects may include Client's job applicants, employees, suppliers, and end users about whom data is provided to SUPPLIER via the SUPPLIER Product by (or at the direction of) Client or by Client's end users.

2.2.5. Duration of the Processing: As between SUPPLIER and Client, the duration of the data processing of Client Data under this Addendum is necessarily determined by Client as provided for in the Agreement. The duration of the processing will include the retention of backups of Client Data for a period not to exceed 6 months from the expiration or termination of the Agreement.

2.2.6. Restriction: SUPPLIER shall not: (a) sell Client personal data; (b) retain, use, or disclose Client personal data for any purpose other than for the specific purpose of providing the SUPPLIER Product in accordance with the Agreement; (c) retain, use, or disclose personal data for a commercial purpose other than providing the SUPPLIER Product; or (d) retain, use, or disclose Client personal data outside of the direct business relationship between Client and SUPPLIER. SUPPLIER certifies that SUPPLIER 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. **Client Instructions.** Client appoints SUPPLIER as a processor to process Client Data on behalf of, and in accordance with, Client's instructions as set out in the Agreement and this Addendum, as otherwise necessary to provide the SUPPLIER 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 SUPPLIER Product may result in additional fees payable by Client to SUPPLIER for carrying out those instructions. Client shall ensure that its instructions comply with all laws, regulations and rules applicable to the Client Data and the related processing, and that SUPPLIER's processing of the Client Data in accordance with Client's instructions will not cause SUPPLIER to violate any applicable law, regulation or rule, including Applicable Data Protection Law. SUPPLIER agrees not to retain, use, or disclose Client Data, except to provide, operate, maintain or operate the SUPPLIER Product as provided for in the Agreement, or as necessary to comply with the law or other binding governmental order.

2.4. **Confidentiality of Client Data and Responding to Third Party Requests.** In the event that any request, correspondence, enquiry or complaint from a data subject, regulator, or third-party is made directly to SUPPLIER in connection with SUPPLIER's processing of Client Data, SUPPLIER shall promptly (but within 48 hours) inform Client providing details of the same, to the extent legally permitted. Unless legally obligated to do so, SUPPLIER shall not respond to any such request, inquiry or complaint without Client's prior consent except to confirm that the request relates to Client and to provide Client contact information, to which Client hereby agrees.

2.5. **Confidentiality Obligations of SUPPLIER Personnel.** SUPPLIER shall ensure that any person it authorizes to process the Client Data will protect the Client Data in accordance with SUPPLIER's confidentiality obligations under the Agreement which includes having a written confidentiality agreement in place.

2.6. **Subcontracting.** Client consents to SUPPLIER engaging third party sub-processors to process Client Data for Permitted Purposes provided that:

2.6.1. A current list of SUPPLIER's sub-processors can be found at www.JazzHR.com/terms-of-use/sub-processors/. SUPPLIER 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 SUPPLIER Product;

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

2.6.3. SUPPLIER 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.

2.7. **Objection to Sub-Processor**. Client may object to SUPPLIER's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds solely relating to data protection and compliance with Applicable Data Protection Law. In such event, the parties shall discuss commercially reasonable alternative solutions in good faith. If the parties cannot reach resolution, SUPPLIER shall either not appoint or replace the sub-processor or, if this is not commercially reasonable for SUPPLIER, Client may terminate the Agreement (without prejudice to any Fees incurred by Client prior to such termination) within 30 days following SUPPLIER's notice to Client that it will be appointing the sub-processor.

2.8. **Data Subject Rights.** As part of the SUPPLIER Product, SUPPLIER provides Client with a number of self-service features, including the ability to delete, retrieve, or restrict use of certain Client Data, which may be used by Client to assist in its obligations under Applicable Data Protection Law with respect to responding to requests from data subjects. In addition, SUPPLIER shall provide reasonable additional and timely assistance to the extent the self-service features of the SUPPLIER Product do not sufficiently enable Client to comply with its data protection obligations with respect to data subject rights under Applicable Data Protection Law.

2.9. **Impact Assessments and Consultations.** If SUPPLIER believes or becomes aware that its processing of Client Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, SUPPLIER shall inform Client and provide reasonable cooperation to Client (at Client's expense) in connection with any data protection impact assessment or consultations with supervisory authorities that may be required under Applicable Data Protection Law.

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

2.11. **Audit Obligations.**

2.11.1. **SUPPLIER's Audit Program.** The parties acknowledge that Client must be able to assess SUPPLIER's compliance with its obligations under Applicable Data Protection Law ("Security Audit"), insofar as SUPPLIER is acting as a processor on behalf of Client. Client may perform a Security Audit of SUPPLIER's security obligations under this Agreement up to once per year or more frequently if Client has such an obligation under Applicable Data Protection Law. If a third party is to be used by Client to conduct such audit, the third party must be mutually agreed to by Client and SUPPLIER and must execute a reasonable written confidentiality agreement with SUPPLIER before conducting the audit. The Security Audit must be conducted during regular business hours at the applicable SUPPLIER facility subject to SUPPLIER policies, and may not unreasonably interfere with SUPPLIER business activities.

2.11.2. **Audit Requests**. To request an audit, Client must submit a detailed audit plan to SUPPLIER at least 2 weeks in advance of the proposed audit date. The audit plan must describe the proposed scope, duration, and start date of the audit. SUPPLIER shall review the audit plan and provide Client with any concerns or questions. SUPPLIER and Client shall work cooperatively to agree on a final audit plan. If the requested audit scope is addressed in a SSAE 16 / ISAE3402 Type 2, ISO, NIST, PCI DSS, HIPAA or similar audit report performed by a qualified third-party auditor within the prior 12 months and there is confirmation there are no known material changes in the controls audited, Client agrees to accept those findings in lieu of requesting an audit of the controls covered by the report (including under Controller-Processors Clauses, as applicable). The third-party audit report and findings will be subject to reasonable confidentiality controls. If the Controller-Processors Clauses apply, nothing in this Section 2.11 (Audit Obligations) varies or modifies the Controller-Processors Clauses nor affects the supervisory authorities' or data subjects' rights under the Controller-Processors Clauses.

2.12. **Violations of Applicable Data Protection Law.** SUPPLIER shall inform Client if it becomes aware or reasonably believes that Client's data processing instructions violate Applicable Data Protection Law.

3. **Controller Obligations (Client Account Data and Usage Data)**

3.1. **Purpose Limitation.** SUPPLIER shall process Client Account Data and Client Usage Data in accordance with Applicable Data Protection Law and consistent with its privacy policies as posted on its publicly-available website and/or the Agreement.

3.2. **Cooperation and Data Subject Rights.** In the event that either party receives: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); or (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Client Account Data and Client Usage Data; (collectively, "*Correspondence*") then, where such Correspondence relates to processing conducted by the other party, it shall promptly inform the other party and the parties shall cooperate in good faith as necessary to respond to such Correspondence and fulfil their respective obligations under Applicable Data Protection Law.

4. **Security**

4.1. **Security Measures.** SUPPLIER has implemented and shall maintain appropriate technical and organizational measures (“*Security Standards*”) to protect Client Account Data, Client Usage Data, and Client 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 Exhibit 1.

4.2. **Determination of Security Requirements.** Client acknowledges that the SUPPLIER Product includes certain features and functionalities that Client may elect to use that impact the security of the data processed by Client’s use of the SUPPLIER Product, such as, but not limited to, Client’s choice of password requirements for Authorized Users on Client’s SUPPLIER Product account.

4.3. **Security Incident Notification.** SUPPLIER shall, to the extent permitted by law, promptly notify Client of any Security Incident of which SUPPLIER becomes aware. To the extent such Security Incident is caused by a violation of the requirements of this Addendum by SUPPLIER, SUPPLIER shall make reasonable efforts to identify and remediate the cause of such Security Incident. SUPPLIER shall provide reasonable assistance to Client in the event that Client is required under Applicable Data Protection Law to notify a supervisory authority or any data subjects of the Security Incident including such information about the Security Incident as SUPPLIER is reasonably able to disclose to Client.

4.4. **Communication.** Notification of Security Incidents, if any, will be delivered to one or more of Client’s administrators or designated contacts, by the means SUPPLIER reasonably selects. It is Client’s sole responsibility to ensure Client’s administrators or designated contacts maintain accurate contact information with SUPPLIER.

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

5.1. Client is responsible to ensure that the transfer of personal data out of the jurisdiction it originated to SUPPLIER complies with Applicable Data Protection Law (“**Legal Basis for Transfer**”). SUPPLIER shall ensure that any transfers it makes of Client Data, Client Account Data, or Client Usage Data has a Legal Basis for Transfer. Such measures may include (without limitation) for Client Data subject to the GDPR or the laws of Switzerland, transferring the Client Account Data, Client Data or Client Usage Data to a recipient in a country that the European Commission has decided provides adequate protection for personal data, to a recipient that has achieved binding corporate rules authorization in accordance with Applicable Data Protection Law, to a recipient that has certified under a recognized compliance standard for the lawful transfer of personal data (“Recognized Standard”), or to a recipient that has executed Controller-Processors Clauses adopted or approved by the European Commission.

5.2. **Standard Contractual Clauses.**

5.2.1. For the purposes of this Addendum, “Controller-Processors Clauses” shall mean the Standard Contractual Clauses, sections I – IV (as applicable).

5.2.2. For the purposes of the Controller-Processors Clauses, Client is the data exporter and SUPPLIER is the data importer.

5.2.3. The option under clause 7 shall not apply.

5.3. Transfers of UK Customer Personal Data by the Client to SUPPLIER where the SUPPLIER to this DPA is in a Third Country not deemed under UK Data Protection Law to provide an equivalent level of privacy protection to that in the UK, the Parties agree that the provisions of the UK Addendum shall apply to such transfers. In particular

5.3.1. the Client will be the data exporter, and SUPPLIER will be the data importer;

5.3.2. the start date for transfers in Table 1 of the UK Addendum shall be the Effective Date unless otherwise agreed between the Parties;

5.3.3. the details of the Parties and their key contacts in Table 1 of the UK Addendum shall be as set out at the commencement of this DPA, and with no requirement for additional signature;

5.3.4. for the purposes of Table 2, the UK Addendum shall be appended to the 2021 SCCs as incorporated by reference into this DPA (including the selection of modules as specified in Section 5.1 of this DPA and the selection and disapplication of optional clauses as set out in Sections 5.2.2 and 5.2.3 of this DPA);

5.3.5. the appendix information listed in Table 3 of the UK Addendum is set out at the commencement of this DPA (List of Parties), in Section 2 (Description of Transfer) and in Schedule 2 to this DPA (Technical and Organisational Measures); and

5.3.6. for the purposes of Table 4, neither Party may end the UK Addendum as set out in Section 19 thereof.

6. Miscellaneous

6.1. **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 JazzHR Services or may not be able to be made. For example, a data protection law in a country that would require Client 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 SUPPLIER and Client.

EXHIBIT 1

Security Standards

1. **Information Security Program.** SUPPLIER shall maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to satisfy the Security Objectives, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the JazzHR Services, and (c) minimize security risks, including through risk assessment and regular testing. SUPPLIER shall designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:
   1.1. **Be Based on an Industry Standard.** The information security program will be based upon a recognized industry standard such as ISO/IEC 27000:2018, ISO/IEC 27001:2013, and ISO/IEC 27002:2013.

   1.2. **Employee Security – General.** SUPPLIER shall ensure that all employees have executed an appropriate written confidentiality agreement and that they complete security and privacy education annually appropriate to their role.

   1.3. **Employee Security – Background Checks.** SUPPLIER shall conduct background checks on its employees, (and require its subcontractors to perform such background checks on their employees), who have access to Client Data.

   1.4. **Subcontractor Security.** SUPPLIER shall ensure that all subcontractors have written agreements in place with terms related to confidentiality and security appropriate for the function that they serve and the obligations in the Agreement. SUPPLIER shall review all subcontractors who have access to Client Data for their ability to comply with SUPPLIER's information security program, giving consideration to the nature of the data and processing that the subcontractor provides. Only subcontractors that are assessed as being able to provide an appropriate level of security will be utilized.

   1.5. **Application Development.** SUPPLIER shall develop the SUPPLIER Product using a defined system development lifecycle process that includes reviews related to security by design and privacy by design.

   1.5. Client acknowledges that, as of the Effective Date of this Addendum, SUPPLIER's primary processing facilities are in the United States, and SUPPLIER has support staff who may provide services that would be considered Processing in the United States, Canada, India, and the United Kingdom.

   1.6. **Application Security**. Supplier shall maintain measures for the Supplier Product to logically separate and prevent Client Data from being exposed to or accessed by unauthorized persons. Supplier shall maintain appropriate isolation of its production and non-production environments and not utilize Client Data in application development without the express written consent of Client. Client Data in transit and rest will be encrypted. All encryption algorithms and key lengths will be based upon commercially available methods.

1.7. **Restricted Access**. SUPPLIER shall limit access to Client Data to only those employees and subcontractors who require such access to perform the activities required to provide the SUPPLIER Product to Client. All access to Client Data will be individual, role-based, and subject to approval and regular review. Access will be revoked promptly upon the account holder's separation.

1.8. **Network Security.** The SUPPLIER Product will be electronically accessible to customers, employees, and subcontractors as necessary to provide the JazzHR Services. SUPPLIER shall maintain access controls and policies to manage what access is allowed to the SUPPLIER Product from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. SUPPLIER shall maintain corrective action and incident response plans to respond to potential security threats. SUPPLIER shall have a formal process for monitoring and installing operating system patches on systems that provide the SUPPLIER Product on a timetable related to the related risk severity.

1.9. **Vulnerability Assessments.** SUPPLIER shall conduct vulnerability assessments of the SUPPLIER Product on a regular basis but at least quarterly. Any identified issues shall be remediated in an appropriate timeframe in accordance with SUPPLIER policies.

1.10. **Disaster Recovery Plan.** SUPPLIER shall maintain a disaster recovery plan related to the JazzHR Software and a business interruption recovery plan related to its business. SUPPLIER shall test such plans at least annually.

1.11. **Incident Response Plan.** SUPPLIER shall maintain an incident response plan related to the identification of Security Incidents, limiting the impact of Security Incidents, investigation of Security Incidents, maintaining evidence of Security Incidents, and informing required parties of Security Incidents. Such plan shall be tested at least annually.

1.12. **Physical Security.** The SUPPLIER Product will be hosted with subcontractor providers of commercially reasonable hosting facilities. Such subcontractors are responsible for the physical security of the hosting facility.

1.12.1. **Physical Access Controls.** The physical components of the JazzHR Software are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors will be assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors will be required to sign-in with designated personnel, show appropriate identification, assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and continually escorted by authorized employees or contractors while visiting the Facilities.

1.12.2. **Limited Access.** The hosting subcontractor will only provide access to the Facilities to individuals with a legitimate business need for such access and will promptly revoke such access when the business need ends.

1.12.3. **Physical Security Protections.** All access points (other than main entry doors) will be maintained in a secured (locked) state. Access points to the Facilities will be monitored by video surveillance cameras designed to record all individuals accessing the Facilities. The hosting subcontractor will maintain electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors will be logged and routinely audited.

2. **Continued Evaluation**. SUPPLIER shall conduct periodic reviews of the security of the JazzHR Software and adequacy of its information security program as measured against industry security standards and its policies and procedures. SUPPLIER shall continually evaluate the security of the JazzHR Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

Controller to Processor Standard Contractual Clauses

This data transfer agreement is between

Client who has executed the Agreement into which the above Data Protection Addendum is incorporated, hereafter “data exporter”

And

JazzHR, 610 Lincoln Street, #205. Waltham, MA 02451 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 – Omitted.

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 (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 (14) 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. 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) 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.

(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;

(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.

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.

ANNEX I

A. LIST OF PARTIES

As set forth on the signature page of the DPA.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects include Customers of JazzHR and Visitors to JazzHR's website.
Data subjects can login to the system and change their profile details, resume, other documentation and can download their data in machine readable format.
The JazzHR Platform offers option to pseudonymize or delete applicant data records on-the-fly so your organization can respond to subject requests.

Categories of personal data transferred
The list below reflects the most commonly collected data across the JazzHR platform. Our customer ultimately decides what data is collected via the employment application process via the configuration of customer-specific applications and forms. JazzHR does not ultimately control what data will be collected in the process.
The types of Customer Personal Data to be Processed
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical home, and business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localization data

The categories of Data Subject to whom the Customer Personal Data Relates
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Employee's
- Potential employee's
- Candidates seeking employment

physical or mental health data race or ethnic origin political opinions

sex life

sexual orientation

actual or alleged criminal activity

religious or philosophical beliefs

genetic data

biometric data (where used for ID purposes)

trade union membership

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.

JazzHR collects, processes, and transfers the Sensitive Data listed directly above in subsection 2. This Sensitive Data is collected from potential employment candidates with the express consent of the candidates and is processed to carry out JazzHR's obligations with respect to employment and social security purposes, to the extent permitted by U.S. and EU Member State law.

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

JazzHR 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

JazzHR 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. JazzHR does not delete customer data or configure retention policies for customers.

JazzHR 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. Data contained in data backups are deleted over the course of the standard cycling of data backups so that such backup data will all be deleted by 200 days following contract termination. Upon request, JazzHR shall provide written certification to the Customer that it has fully complied with this form of request.

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

JazzHR 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 II Exhibit A, for a list of sub-processors. Data retention as defined above also applies for sub-processors when applicable.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority/ies in accordance with Clause 13 is Irish Data Protection Commission unless otherwise set forth in the signature page of the DPA.

ANNEX II

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

JazzHR, a provider of HR software and services that allow companies to post employment opportunities within and external to the software, collect and track information from applicants and candidates, coordinate the review of applicants and candidates amongst their internal or affiliated hiring teams, and manage the performance of current employees.

1. **Information Security Program** JazzHR maintains an information security program that protects JazzHR and its customers from risk, including the accidental or malicious disclosure of data. The information security program incorporates the following:
    - Monitoring the exposure of information assets to major threats.
    - Facilitating major initiatives to enhance information security.
    - Understanding the business impact of Information Security policies and standards.
    - Reviewing the effectiveness of the implementation of the information security policy.
    - Communication of security information and new technology.
    - Creating an escalation path for issues affecting the security of the business.
    - Ensuring appropriate corporate process for handling security threats.
    - Assessing security effectiveness and efficiency.
    - Ensuring that risk assessments are carried out.
2. **Information Security Standards** While JazzHR's Information Security program contains many policies, the core standards are summarized below.
    - **System and Network Security** With the exception of the web application's front end, all JazzHR systems, networks, and equipment are only accessible by employees onsite or remote via VPN. Contractors or other non-employees must be onsite in the JazzHR office. JazzHR maintains various controls and policies to ensure that role-based access principles are followed, which includes forbidding the use of shared credentials. JazzHR proactively monitors network activity and has policies and processes in place to respond to potential adverse events. All traffic is encrypted, including a full IPSec mesh VPN for inter-facility traffic.
    - **Physical Security** Systems containing customer data are protected by layered physical controls and monitored for intrusion. All doors are locked, require a key fob for entry, and are protected by an alarm system that includes contact and vibration sensors. Entrances to the building and our suite are monitored by continuously recording surveillance cameras.
3. **Continual Evaluation** JazzHR performs reviews of information security-related policies on a scheduled basis. Based on importance and criticality, these reviews occur quarterly, biannually, or yearly. Additionally, policies are reviewed in response to any emerging threats, incidents, or concerns.

ANNEX II EXHIBIT A

LIST OF SUB-PROCESSORS

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

https://www.jazzhr.com/subprocessor-list

Client consents to JazzHR engaging third party sub-processors to process data. JazzHR 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 JazzHR Product.

EXHIBIT B
COMPLIANCE WITH CALIFORNIA CONSUMER PRIVACY ACT AND CALIFORNIA PRIVACY RIGHTS ACT

In connection with JazzHR's ("Supplier") continued delivery and continued receipt of products or services under the applicable Data Privacy Agreement with Customer in effect between the Parties that involve the access, sharing, or use of personal information as defined in the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) (together, the "Data Laws") and for valuable consideration the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree, at no additional charge to either Party, to abide by each of the following terms.

1. <u>General Terms</u>

Effective as of January 1, 2020 (the "Effective Date") and continuing through for the duration of each of the Agreement, the following additional terms apply to the Agreement and govern over any conflicting terms in the Agreement:

a. Each of the Parties will comply with the Data Laws;
b. Each of the Parties will, upon the request of the other Party, comply with the other Party's request to enter into any further amendments to the Agreement to the extent reasonably necessary to comply with the Data Laws;
c. Supplier shall provide the same level of privacy protection around personal information (as defined in the Data Laws) as is required by the Data Laws and the Agreement. Should Supplier use a subcontractor or subprocessor in order to fulfill the Services as described in the Agreement, Supplier shall ensure that the subcontractor or subprocessor is bound by privacy protections at least as restrictive as those provided for by this Agreement.

<u>2. Supplier Obligations.</u>

To the extent that Supplier receives from Customer any personal information of any "consumer" (as defined in the Data Laws) for processing (as defined in the Data Laws) on behalf of Customer pursuant to one of more of the Agreement, Supplier shall:

a. be a "contractor" and/or a "service provider" to Customer under the Data Laws (for purposes of the CPDA, Company is the "data controller" and Service Provider is the "data processor");
b. comply with any and all Customer instructions to Supplier regarding the processing of personal information, including the nature and purpose of processing, the type of of information subject to processing, the duration of processing, and the rights and obligations of both parties;
c. ensure that any Supplier personnel (including any subcontractors or subprocessors) is subject to a duty of confidentiality with respect to personal information, either by a written agreement or by a statutory duty of confidentiality;
d. not "sell" or "share" (as defined by the Data Laws) Customer personal information;
e. not retain, use, or disclose the personal information outside of the direct business relationship between Customer and Supplier or for any purpose other than for the limited and specific "business purpose" (as defined in the Data Laws) of performing services under such Agreement or as otherwise permitted by the Data Laws, including for any "business purpose" except:

(1) To perform the services and fulfill the limited and specific business purposes specified in the written contract with Customer;
(2) To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the Data Laws and these regulations and provided that Customer has granted Service Provider written approval of such subcontractor;
(3) To detect data security incidents, or protect against fraudulent or illegal activity; or
(4) For the purposes enumerated in Civil Code section 1798.145, subsections (a)(1) through (a)(4).

f. make available, upon Customer's reasonable request, all information in Supplier's possession necessary to demonstrate compliance with the Data Laws;
g. not combine Customer's personal information with personal information acquired from another source;
h. delete or return all personal information to Customer as requested at the end of the provision of Services by Supplier, unless further retention is required by law;
i. upon timely and adequate notice to Customer, take reasonable steps to stop or remediate the unauthorized use of personal information;
j. take reasonable and appropriate steps to ensure Supplier's retention, use, and/or disclosure of personal information is consistent with the Services identified in the Agreement;
k. promptly notify Customer if it determines it can no longer meet its obligations under the Data Laws or this Agreement; and
l. not retain, use, and/or disclose sensitive personal information (as defined in the Data Laws) after it has received instructions from Customer and to the extent it has actual knowledge that the personal information is sensitive information for any other purpose than as expressly provided for in the Agreement.

Supplier certifies that it understands and shall comply with the restrictions on retention, use, and/or disclosure of personal information as described above.

3. Data Subject Requests.

Supplier will promptly (and, in any case within three (3) days of receipt) comply with Customer's written instructions associated with responding to an individual's request to exercise their privacy rights with respect to their personal information as provided for by the Data Laws, and will provide reasonable assistance to Customer in responding to an individual's request.

4. Sub-Processors.

Customer must authorize any subcontractor, service provider or third party ("Sub-processor") to process Customer's personal information. Supplier shall enter into contractual provisions so that such Sub-processor is a "service provider" as defined in the Data Laws, and such contractual provisions must require the Sub-processor to be bound by obligations that are at least as restrictive as this Agreement.

5. Miscellaneous.

Supplier must notify Customer in writing if Supplier objects to or does not agree to be bound by the terms above, with such notice to include the specific reasons for Supplier's concerns. If Supplier fails to object to the terms as set forth above, then Supplier is hereby deemed to have accepted and agreed to be bound by the terms without limitation as of the Effective Date.