# JAZZHR DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**Addendum**") is made and entered into by and between Hireku, Inc. d/b/a JazzHR ("**JazzHR**") and the customer specified in the table below (the "**Customer**"), and shall be annexed to, and incorporated into, the Terms of Service between JazzHR and Customer, dated as of May 15th, 2018 ("**Agreement**") to reflect the parties' agreement about certain data processing and transfer obligations of the parties. In the event of any inconsistency between this Addendum and the Agreement, this Addendum shall control.

By signing below, each party agrees to be bound by the terms of this Addendum.

| | |
|---|---|
| Hireku, Inc. (d/b/a JazzHR)<br><br>J. Britton Hutchins<br>(signature) | Customer Name:<br><br>(signature) |
| Name: J. Britton Hutchins<br><br>Title: CFO<br><br>Date: May 15, 2018 | Name:<br><br>Title:<br><br>Date: |

## 1. INSTRUCTIONS

1.1 To enter into this Addendum, an individual with authorization to execute contracts on behalf of Customer must send an email to compliance@jazzhr.com that includes the following information:

(a) Customer's legal company or entity name and its registered business address; and
(b) Customer's email address, telephone number, and, if available, fax number.

1.2 Once the email is received, JazzHR will prepare the Agreement and contact Customer with further instructions for electronic signing and final execution.

## 2. DEFINITIONS

2.1 The terms "**Data Controller**", "**Data Processor**", "**Data Subject**", "**Personal Data**" and "**Processing**" shall have the meaning given to those terms in the GDPR, and "**Process**" and "**Processed**" shall be construed accordingly;

2.2 "**Customer Data**" means the Personal Data that is uploaded by the Customer to the Services in connection with the Agreement comprised of Customer's end-users, which are Customer's designated users of the Services, as well as any job applicants who are applying to a role posted by a Customer through the Services or that are imported by Customer into the Service;

2.3 "**Data Protection Laws and Regulations**" means laws and regulations applicable to the Processing of Personal Data under the Agreement, including applicable laws and regulations of the European Union, the European Economic Area and their member

states, Switzerland, and the United Kingdom, including without limitation 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" or "GDPR") and EU Directive 2002/58/EC on Privacy and Electronic Communications ("e-Privacy Directive") or, the superseding Regulation on Privacy and Electronic Communications ("e-Privacy Regulation"), once effective;

2.4 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

2.5 "**Services**" means the services provided to Customer by JazzHR under the Agreement;

2.6 "**Subprocessor**" means any Processor engaged by JazzHR in the provision of the Services to Customer, as further described in Section 3.4 of this DPA.

## 3. PROTECTION OF PERSONAL DATA

3.1 Relationship of Parties: For the purposes of this Addendum, Customer is the Controller and appoints JazzHR as a Processor to Process Customer Data on behalf of Customer in connection with Company's use of the Services pursuant to the Agreement. The Processor and Controller shall each comply with their respective obligations applicable to it under the Data Protection Laws and Regulations and this Addendum.

3.2 Purpose Limitation: JazzHR shall Process Customer Data in order to perform JazzHR's obligations, or as otherwise permitted, under the Agreement as a Processor, in compliance with the applicable Data Protection Laws and Regulations. The purposes of Processing are as described in the Agreement, including Schedule A to this Addendum, and any other exhibits, statements of work or addenda attached to or otherwise incorporated into the Agreement (the "Permitted Purpose").

3.3 Cross-Border Transfers: With respect to Customer Data that is transferred under the Agreement from the European Economic Area or Switzerland by Customer as Controller to JazzHR as Processor, or otherwise by JazzHR as Processor, to a jurisdiction which the European Commission or, where relevant, the Swiss Federal Data Protection and Information Commissioner, has determined does not ensure an adequate level of protection of Personal Data, JazzHR has self-certified to the EU-U.S. Privacy Shield Framework as an appropriate legal instrument for such transfer .

3.4 Subprocessing:

(a) Customer acknowledges and agrees that JazzHR may engage Subprocessors in connection with the provision of the Services. A list of approved Subprocessors

as of the Effective Date of this Addendum is located at https://www.jazzhr.com/subprocessor-list (the "Subprocessor List"). Customer may subscribe to receive update alerts when changes are made to the Subprocessor List.

(b) JazzHR will enter into a written agreement with each Subprocessor containing data protection obligations, to the extent practicable, no less protective than those in this Addendum or as may otherwise be required by applicable Data Protection Laws and Regulations. JazzHR agrees to be responsible for the acts or omissions of each such Subprocessor to the same extent as JazzHR would be liable if performing the services of such Sub-processor under the terms of the Agreement.

(c) JazzHR will inform Customer of any new Subprocessor engaged during the term of the Agreement by updating the Subprocessor List. If Customer reasonably believes that the appointment of a new Subprocessor will have a material adverse effect on JazzHR's ability to comply with applicable Data Protection Laws and Regulations as a Processor, then Customer must notify JazzHR in writing, within 30 days following the update to the Subprocessor List, of its reasonable basis for such belief. Upon receipt of Customer's written notice, Customer and JazzHR will work together without unreasonable delay on an alternative arrangement. If a mutually-agreed alternative arrangement is not found, and Customer has a termination right under applicable Data Protection Laws and Regulations, then those Services that cannot be provided without the use of the new Subprocessor may be terminated by Customer without penalty.

(d) Notices and Consents:

(i) General: Customer shall comply with all applicable Data Protection Laws and Regulations, including: (a) providing all required notices and appropriate disclosures to all Data Subjects regarding Customer's, and JazzHR's, Processing and transfer of Personal Data; and (b) obtaining all necessary rights and valid consents from Data Subjects to permit Processing by JazzHR for the purposes of fulfilling JazzHR's obligations, or as otherwise permitted, under the Agreement.

(ii) Sensitive Data: Customer's use of the Services in connection with the distribution of Customer Data and/or Processing of sensitive Customer Data of a Data Subject (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or an individual's genetic data, biometric data, health data, or data regarding sex life or sexual orientation) must be in compliance with all applicable Data Protection Laws and Regulations, including obtaining express consent from Data Subjects whose Personal Data is provided to JazzHR for Processing.

## 4. COOPERATION AND DATA SUBJECTS' RIGHTS

(a) JazzHR will provide reasonable and timely assistance, at Customer's request, to enable Customer to respond to: (a) a request from a Data Subject to exercise any rights under applicable Data Protection Laws and Regulations (including rights of access, correction, objection, erasure and data portability, as applicable); and (b) any other correspondence, inquiry or complaint received from a Data Subject, regulator or other third party in connection with Processing of Customer Data. If a Data Subject contacts JazzHR directly to request access to, or correction or deletion of, Personal Data in connection with services provided to Customer by JazzHR, JazzHR will promptly notify Customer of the request.

## 5. Investigations and Audits

(a) Regulatory Audit. JazzHR shall reasonably assist and support Customer in the event of an investigation by a data protection regulator or similar authority, if and to the extent that such investigation relates to JazzHR's Processing of Customer Data.

(b) Customer Audit. Upon at least 30 days' advance written request by Customer, at mutually agreed times and subject to JazzHR's reasonable audit guidelines, JazzHR shall provide to Customer, its authorized representatives and/or independent inspection body designated by Customer: (a) reasonable access to records of JazzHR's Processing of Customer Data; (b) reasonable assistance and cooperation of JazzHR's relevant staff for the purpose of auditing JazzHR's compliance with its obligations under this Addendum and (c) in the case of an audit requiring a security scan, penetration test, or other similar automated or manual information security activities, an alternate environment in which to conduct the test. JazzHR reserves the right to restrict access to its proprietary information, including but not limited to its network architecture, internal and external test procedures, test results and remediation plans. Customer will not cause any damage, injury or disruption to JazzHR Services and JazzHR's premises, equipment, personnel and business operations. Customer further agrees that: (i) Customer will not perform security scans, penetration tests, or other similar automated or manual information security activities without the express written permission of JazzHR in each case; (ii) personnel (or designated third parties) performing said audits will be bound by the confidentiality obligations set forth in the Agreement; (iii) all findings will be deemed JazzHR's Confidential Information (as defined in the Agreement); (iv) Customer will share all findings with JazzHR; and (v) JazzHR will classify and remediate all findings in accordance with JazzHR's risk management program.

(c) JazzHR will not give access to its premises for the purposes of such an audit or inspection: (i) to any individual unless he or she produces reasonable evidence of identity and authority and (ii) outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer has given notice to JazzHR that this is the case before attendance outside those hours begins.

(d) Customer is limited to one audit in any 12-month period, except (i) if and as required by a competent data protection authority; or (ii) Customer believes a further audit is necessary as a result of a Personal Data Breach relating to the Services.

(e) Data Protection Impact Assessment. JazzHR shall, upon Customer's written request, provide Customer with reasonable cooperation and assistance to fulfill Customer's obligations under applicable Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the Services and, if necessary, consult with Customer's relevant Supervisory Authority.

## 6. NOTICE OF NON-COMPLIANCE

(a) If required by applicable Data Protection Laws and Regulations, in the event that JazzHR is unable to comply with its obligations in this Addendum, JazzHR shall promptly notify Customer, and if JazzHR is unable to take reasonable and appropriate steps to remediate the non-compliance within a mutually-agreed upon timeframe, Customer may take any one or more of the following actions: (a) suspend the transfer of Customer Data to JazzHR; (b) require JazzHR to cease Processing Customer Data to the extent technically possible; (c) demand the return or destruction of Customer Data; and/or (d) terminate this Addendum in accordance with the Agreement.

## 7. INSTRUCTIONS ON DATA PROCESSING

(a) JazzHR will process Customer Data in accordance with Customer's instructions. The parties agree that this Addendum sets out Customer's complete and final instructions to JazzHR in relation to the processing of Customer Data.

(b) JazzHR will not access or use Customer Data, except as necessary to provide and support the Services.

## 8. CUSTOMER CONTROLS

(a) The Services provide Customer with controls to enable Customer to (a) add, retrieve, correct, or delete Customer Data, (b) create user accounts with access to Customer Data, and (c) manage user account permissions. Customer is responsible for properly (a) using the Services in accordance with applicable Data Protection Laws and Regulations, (b) creating, modifying, and disabling user accounts, and (c) taking such steps as Customer considers adequate to maintain appropriate security and protection of Customer Data. JazzHR has no knowledge of, or control over, the Personal Data that Customer provides for Processing. Customer is solely responsible (i) for the accuracy, quality, and legality of the Customer Data and the means by which it acquired the Customer Data and (ii) ensuring that its submission of Personal Data to JazzHR and

instructions for the Processing of Personal Data will comply with applicable Data Protection Laws and Regulations.

## 9. TERM AND TERMINATION; DELETION OR DESTRUCTION OF CUSTOMER DATA

(a) This Addendum will be effective as of the day JazzHR receives a complete and executed Addendum from Customer in accordance with the instructions set out in Section 1 of this Addendum.

(b) This Addendum will terminate automatically upon termination or expiration of the Agreement without further action required by either party. Provisions of this Addendum that, by their nature should survive, will survive any such termination or expiration.

(c) Upon termination or expiration of the Agreement or at any time at Customer's written request, JazzHR shall return to Customer or destroy all Customer Data, except as otherwise permitted by applicable Data Protection Laws and Regulations.

## 10. DISCLOSURE

10.1 JazzHR will not disclose Customer Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as subpoena or court order).

## 11. DATA SECURITY

(a) JazzHR will ensure that all individuals with access to Customer Data are subject to written obligations of confidentiality and that Customer Data is Processed only for the Permitted Purpose.

(b) Security Measures. JazzHR's technical and organizational security measures to protect Customer Data shall be as set forth in the Agreement, this Addendum, and/or in any orders or statements of work issued pursuant to the Agreement. Such measures shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. At a minimum, JazzHR shall comply with the technical and organizational measures set out in Schedule B to this Addendum.

(c) Breach Notification. If JazzHR becomes aware of a Personal Data Breach involving the Services, JazzHR shall: (a) promptly, and without undue delay, but in no event later than 3 business days, following JazzHR's discovery thereof, notify Customer of such Personal Data Breach; (b) investigate, remediate and mitigate the effects of the Personal Data Breach; (c) reasonably cooperate with Customer's investigation of the Personal Data Breach to the extent that such cooperation does not compromise JazzHR's security; (d) take any additional actions and provide any additional cooperation to Customer as may reasonably be required under applicable Data Protection Laws and

Regulations; and (e) upon resolution, provide Customer with a written incident report describing the breach, actions taken during the response and plans for future actions to prevent a similar breach from occurring in the future.

## 12. SERVICE ANALYSES

12.1 JazzHR may compile statistical and other information related to the performance, operation and use of the Services, and use data from the Services in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes. JazzHR may make the results of Analyses publicly available; however, they will not incorporate Customer Data in a form that could identify or serve to identify Customer or any data subject. Such analyses do not constitute Personal Data.

## 13. GOVERNING LAW

(a) This Addendum shall be governed by and construed in accordance with the governing law set forth in the Agreement, except where otherwise required by applicable Data Protection Laws and Regulations.

.

## SCHEDULE A

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.

## SCHEDULE B

**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:

(a) Monitoring the exposure of information assets to major threats.
(b) Facilitating major initiatives to enhance information security.
(c) Understanding the business impact of Information Security policies and standards.
(d) Reviewing the effectiveness of the implementation of the information security policy.
(e) Communication of security information and new technology.
(f) Creating an escalation path for issues affecting the security of the business.
(g) Ensuring appropriate corporate process for handling security threats.
(h) Assessing security effectiveness and efficiency.
(i) 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.

**2.1 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.

**2.2 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.

HELLOSIGN

# Audit Trail

| | |
|---|---|
| **TITLE** | DPA Agreement |
| **FILE NAME** | JazzHR Data Proce...(executable).docx |
| **DOCUMENT ID** | 347965ba3ffbc55929ea27069b626238a9b8926d |
| **STATUS** | Completed |

## Document History

| | | |
|---|---|---|
| SENT | **05/18/2018** 16:47:25 UTC-5 | Sent for signature to J. Britton Hutchins (brit.hutchins+hr@jazzhr.com) from corey.berkey@jazzhr.com IP: 164.52.232.82 |
| VIEWED | **05/18/2018** 16:54:18 UTC-5 | Viewed by J. Britton Hutchins (brit.hutchins+hr@jazzhr.com) IP: 50.227.240.190 |
| SIGNED | **05/18/2018** 16:54:53 UTC-5 | Signed by J. Britton Hutchins (brit.hutchins+hr@jazzhr.com) IP: 50.227.240.190 |
| COMPLETED | **05/18/2018** 16:54:53 UTC-5 | The document has been completed. |