DATA PROCESSING AGREEMENT

1. Scope and order of precedence

Ninahire, Inc ("**NinjaHire**") and **Customer or Partner** referred as ("**Customer**")have entered into an agreement for the provision of Services, including NINJAHIRE's Terms of Use and/or an applicable Master Services Agreement or API Partnership Agreement (as may be amended or entered into from time to time, individually or collectively, the "**Agreement**"). This Data Processing Agreement as updated from time to time (this "**DPA**") will apply to NINJAHIRE's Processing of Customer Personal Data. This DPA is hereby incorporated into and made a part of the Agreement. If there is any conflict between this DPA and the Agreement, this DPA shall control to the extent of such conflict. This DPA will be effective until such time as NINJAHIRE is no longer Processing Customer Personal Data in accordance with the Agreement. Capitalized terms in this DPA not defined herein shall have the definitions ascribed thereto in the Agreement.

2. Definitions

In this DPA, the following capitalized bold terms will have the following meanings:

"Authorized Purposes" means candidate relationship management.

"**CCPA**" means the California Consumer Privacy Act of 2018 found at California Civil Code Sec. 1798.100 et seq., and any amendments thereto, including the California Privacy Rights Act of 2020.

"**Controller**," "**Processor**," "**Data Subject**," "**Personal Data**," "**Personal Data Breach**," "**Processing**," "**Personal Information**," "**Business**," "**Service Provider**," or "**Consumer**" each has the meaning set forth in the applicable Data Protection Laws.

"**Customer**" means an individual acting in such an individual's own legal capacity, or an entity acting alone or with its affiliates, who ordered the Services by subscribing online or executing a Service Order with NINJAHIRE.

"**Customer Personal Data**" means Personal Data and/or Personal Information (as those terms are defined under the applicable Data Protection Laws) provided to NINJAHIRE by Customer or requested by Customer to be processed by NINJAHIRE in connection with the Services.

"**Data Protection Laws**" means applicable laws, standards and regulations governing the Processing of Personal Data and/or Personal Information under the Agreement, as may be amended or enacted from time to time, including, but not limited to the European Data Protection Laws, the UK Data Protection Laws, the CCPA, VCDPA, other United States' Data Protection Laws, and the data protection and privacy laws of other countries.

"**European Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 ("**GDPR**") and data protection laws of the European Economic Area ("**EEA**") and their member states and the FADP.

"**FADP**" means Switzerland's Federal Act on Data Protection of 19 June 1992, as revised.

"**Third Party Sub-processor**" means a third party subcontractor engaged by NINJAHIRE which, as part of the subcontractor's role of providing Services, will Process Customer Personal Data.

"**Services**" means the services to be provided by NINJAHIRE for the benefit of Customer that are specified in the Agreement.

"**UK Data Protection Laws**" means the UK Data Protection Act and/or the UK General Data Protection Regulation as amended from time to time.

"**United States' Data Protection Laws**" means the current and future enacted state and federal data protection laws and regulations that are applicable under the Agreement and the DPA with the Customer, including, without limitation to, CCPA, VCDPA, Colorado Privacy Act, Connecticut Data Privacy Act, Utah Consumer Privacy Act, Texas Data Privacy and Security Act, Montana Consumer Data Privacy Act, Iowa Consumer Data Protection Act, Tennessee Information Protection Act, and Indiana Consumer Data Protection Act, as amended.

"**Usage Data**" means NINJAHIRE's technical logs, data, and information about Customer's use of the Services and third-party integrations with the Services, including, but not limited to, the number of reports run, the frequency of User log-ins, location of User log-ins, and User behavioral data, such as the types of searches run and features heavily used), but excluding Customer Data.

"**VCDPA"** means the Virginia Consumer Data Protection Act, as amended from time to time.

3. NINJAHIRE's Processing of Customer Personal Data

3.1 Categories of Personal Data & Data Subjects

In order to perform the Services, Customer hereby authorizes and requests that NINJAHIRE Process Customer Personal Data as set forth on Schedule 1.

3.2 Customer's Instructions

This DPA, the Agreement, and Customer's use and configuration of features in the Services, are Customer's complete instructions to NINJAHIRE for the Processing of Customer Personal Data. Customer may provide additional instructions in writing to NINJAHIRE, but any such additional instructions must be agreed upon separately. The parties will negotiate in good faith with respect to any other change in the Services and/or fees resulting from any additional instructions.

3.3 Roles and Restrictions on Processing of Customer Personal Data

Customer will at all times (i) remain the Controller of Customer Personal Data pursuant to the Data Protection Laws; (ii) determine the purposes and means of its Processing of Customer Personal Data; (iii) comply with the obligations applicable to it pursuant to the Data Protection Laws regarding the Processing of Customer Personal Data, including, without limitation, establishing a legal basis for Processing of Customer Personal Data, as applicable, and with respect to the transfer and provision of Customer Personal Data to NINJAHIRE for Processing hereunder; and (iv) have sole responsibility for the accuracy, quality, and legality of any Customer Personal Data provided to NINJAHIRE and the means by which Customer acquired such data, as applicable.

NINJAHIRE is a Processor with respect to its Processing of Customer Personal Data hereunder. NINJAHIRE will Process Customer Personal Data solely for the provision of the Services and will not otherwise (i) Process Customer Personal Data for purposes other than those set forth in the Agreement or as instructed by Customer in accordance with Section 3.2, or (ii) disclose such Customer Personal Data to third parties other than Third Party Sub-processors as permitted or required by the Agreement, this DPA, or the Data Protection Laws. NINJAHIRE will comply with the obligations applicable to it pursuant to the Data Protection Laws regarding the Processing of Customer Personal Data.

3.4 Rights of Data Subjects

NINJAHIRE will follow Customer's detailed written instructions to meet its obligations pursuant to the Data Protection Laws to respond to Data Subject requests to access, delete, release, correct, or block access to Customer Personal Data held in NINJAHIRE's information technology environment. Customer agrees to pay NINJAHIRE's reasonable out-of-pocket costs and expenses and standard hourly fees that may be associated with NINJAHIRE's performance of any such request on behalf of Customer. NINJAHIRE will pass on to the Customer any Data Subject requests to access, delete, release, correct, or block Customer Personal Data. In doing so, NINJAHIRE will use the Customer's email contact information provided in the Service Order or the email address associated with Customer's NINJAHIRE account, at NINJAHIRE's discretion. NINJAHIRE will not be responsible for responding directly to the request, unless otherwise required by the Data Protection Laws.

3.5 Cross Border Transfers

Transfers of Customer Personal Data originating from the EEA to NINJAHIRE are subject to (i) the terms of the Controller to Processor Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses (Module Two)) ("**C2P SCC**"); or (ii) other appropriate transfer mechanisms pursuant to the Data Protection Laws. The terms of this DPA shall be read in conjunction with the C2P SCC or other appropriate transfer mechanisms, and the following shall apply: (A) NINJAHIRE will be the "data importer" and Customer will be the "data exporter"; (B) the optional Clause 7 docking clause will not apply; (C) Option 2 of Clause 9(a) shall apply, and the period shall be fourteen (14) days; (D) in Clause 11, the optional language will not apply; (E) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law for personal data transferred out of the European Economic Area or Swiss law for personal data transferred out of Switzerland; (F) in Clause 18(b), disputes will be resolved before the courts of Ireland for personal data transferred out of the European Economic Area or Switzerland for personal data transferred out of Switzerland; (G) Annex I will be deemed completed with the information set out in Schedule 1 of this DPA, with NINJAHIRE as the data importer and Customer as the data exporter; and (H) Annex II will be deemed completed with the information set out in Schedule 2 of this DPA.

For purposes of any transfers of personal data solely subject to the Swiss FADP, the C2P SCC shall apply with the following amendments: (A) References to "Regulation (EU) 2016/679" or "that Regulation" are to be interpreted as references to the Swiss FADP; (B) References to "Regulation (EU) 2018/1725" are removed; (C) References to "Union", "EU", and "EU Member State" shall be interpreted to mean Switzerland; (D) Clause 13 (a) and Part C of Annex I are not used and the competent supervisory authority is the Federal Data Protection and Information Commissioner (the "FDPIC"); (E) Clause 17 is replaced to state that "These Clauses are governed by the laws of Switzerland"; (F) Clause 18 is replaced to state: "Any dispute arising from these Clauses relating to the Swiss FADP shall be resolved by the courts of Switzerland. A data subject may bring legal

proceedings against the data exporter and/or data importer before the courts in the Canton of Zug. The parties agree to submit themselves to the jurisdiction of such courts."

For transfers of personal data from the UK, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner in force 21 March 2022 is agreed to and incorporated by reference, but, as permitted by clause 17 of such addendum, the parties agree to change the format of the information set out in Part 1 of the addendum such that:

- For the purposes of Table 1, NINJAHIRE shall be the "importer" and Customer shall be the "exporter," with the applicable details the same as identified in the Agreement.
- For the purposes of Table 2, (A) the EU SCCs shall apply, (B) Module 2 will apply to the personal data transferred to a third country; (C) in Clause 7, the optional docking clause will not apply; (D) in Clause 11, the optional language will not apply; (E) in Clause 17, Option 1 will apply, and, the EU SCCs will be governed by the laws of the UK for personal data transferred out of the UK; (F) in Clause 18(b), disputes will be resolved before the courts of the UK for personal data transferred out of the UK.
- For purposes of Table 3, Annex IA and Annex IB will be deemed completed with the information set forth in Schedule 1 of this DPA and Annex II will be deemed completed with the information set forth in Schedule 2 of this DPA.
- For purposes of Table 4, neither party may terminate this DPA when the Approved Addendum changes.

NINJAHIRE represents that it is self-certified under the EU-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework and complies with the Data Privacy Framework Principles when processing any such Personal Data. To the extent that Customer is (a) located in the United States of America and is self-certified under the Data Privacy Framework or (b) located in the EEA or UK, NINJAHIRE further agrees: (i) to provide at least the same level of protection to any Personal Data as required by the Data Privacy Principles; (ii) to notify Customer in writing, without undue delay, if its self-certification to the Data Privacy Framework is withdrawn, terminated, revoked, or otherwise invalidated (in which case, an alternative transfer mechanism will apply in accordance with applicable Data Protection Laws); and (iii) upon written notice, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized processing of personal data, if no alternative transfer mechanism exists.

3.6 Third Party Sub-processors

Some or all of NINJAHIRE's obligations under the Agreement may be performed by Third Party Sub-processors. NINJAHIRE maintains a list of Third Party Sub-processors that may Process Customer Personal Data at https://ninjahire.co/subprocessor, or Customer can subscribe to be notified by email whenever there is a newly added sub-processor, by emailing to privacy@ninjahire.co .

The Third Party Sub-processors shall abide by substantially the same obligations as NINJAHIRE under this DPA as applicable to their Processing of Customer Personal Data as determined by NINJAHIRE. NINJAHIRE remains responsible at all times for compliance with the terms of this Agreement by Third Party Sub- processors.

Customer consents to NINJAHIRE's use of Third Party Sub-processors in the performance of the Services in accordance with the terms of Sections 3.5 and 3.6 herein.

3.7 Technical and Organizational Measures

NINJAHIRE has implemented and will maintain appropriate technical and organizational security measures for the Processing of Customer Personal Data, including the measures specified in Schedule 2 to this DPA to the extent applicable to NINJAHIRE's Processing of Customer Personal Data. These measures are intended to protect Customer Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure, or access, and against all other unlawful forms of Processing. Additional measures, and information concerning such measures, including the specific security measures and practices for the particular Services ordered by Customer, may be specified in the Agreement and NINJAHIRE's security policies.

3.8 Audit Rights

NINJAHIRE will make all information reasonably necessary to demonstrate compliance with this DPA available to Customer and upon request, once per year, NINJAHIRE will provide to Customer the results of its most recent SOC 2 Type 2 and SOC 3 compliance audit provided by a certified, third-party audit firm ("**Report**"). The Report shall be considered NINJAHIRE confidential information pursuant to the Agreement. If NINJAHIRE does not provide a Report, Customer has the right to inspect NINJAHIRE's respective systems and facilities up to one (1) time every twelve (12) months, for the duration of not more than two (2) weeks, to ensure compliance with this DPA only to the extent required by the Data Protection Laws. Before the commencement of any such audit, Customer and NINJAHIRE shall mutually agree in good faith upon the scope, and duration of the audit if the audit will take more than two (2) weeks. The audit must be conducted during regular business hours at the applicable facility, subject to NINJAHIRE's policies, and may not unreasonably interfere with NINJAHIRE's business activities. Customer is entitled to conduct the audit through an authorized third-party agreed by the parties. Any such third-party auditor must comply with the confidentiality requirements under this DPA and the Agreement; the results of such audit will be deemed the confidential information of NINJAHIRE. Customer shall notify NINJAHIRE with information regarding any non-compliance discovered during the course of an audit. Any audits are at the Customer's expense, except where the audit finds material breach of this DPA, in which case NINJAHIRE shall be responsible for the cost. Any request for NINJAHIRE to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required for the provision of the Services. NINJAHIRE will seek the Customer's written approval and agreement to pay any related fees before performing such auditassistance.

3.9 Incident Management and Breach Notification

NINJAHIRE evaluates and responds to incidents that create suspicion of or indicate a Personal Data Breach. NINJAHIRE operations staff is instructed on responding to Personal Data Breach as required pursuant to the Data Protection Laws. NINJAHIRE will notify Customer as soon as reasonably practicable, and in any event within any notice period required pursuant to the Data Protection Laws, if NINJAHIRE has determined that a Personal Data Breach has occurred that involves Customer Personal Data. NINJAHIRE will promptly investigate the Personal Data Breach and take reasonable measures to identify its root cause(s) and prevent a recurrence. As information is collected or otherwise becomes available, unless prohibited by applicable law, NINJAHIRE will provide Customer with a description of the Personal Data Breach, the type of Personal Data that was the subject of the Personal Data Breach, and other information Customer may reasonably request concerning the affected Data Subjects. The parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects and/or notices to the relevant data protection authorities.

3.10 Return and Deletion of Personal Data upon End of Services

Following termination of the Services, at Customer's instruction, NINJAHIRE will return or otherwise make available for retrieval to Customer all Customer Personal Data then available in NINJAHIRE's information technology environment that holds Customer Personal Data, or if Customer provides no instructions, destroy the data in accordance with NINJAHIRE's then-current data retention policies and applicable law. Following return of such Customer Personal Data, NINJAHIRE will promptly delete or otherwise render inaccessible all copies of Customer Personal Data, except as may be required by applicable law.

3.11 Legally Required Disclosures

Except as otherwise required by applicable law, NINJAHIRE will promptly notify Customer of any subpoena, judicial, administrative, or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority ("**Demand**") that it receives and which relates to the Processing of Customer Personal Data. At Customer's request, NINJAHIRE will provide Customer with reasonable information in its possession that may be responsive to the Demand and any assistance reasonably required for Customer to respond to the Demand in a timely manner. Customer acknowledges that NINJAHIRE has no responsibility to interact directly with the entity making the Demand.

3.12 Service Analyses

NINJAHIRE may (i) compile statistical and other information related to the performance, operation, and use of the Services, and (ii) use data from the Services environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (collectively "**Service Analyses**"). NINJAHIRE may make Service Analyses publicly available. However, Service Analyses will not incorporate Customer Personal Data in a form that could identify or serve to identify Customer or any Data Subject. NINJAHIRE retains all intellectual property rights in and to such Service Analyses.

3.13 Compliance with United States' Data Protection Laws

For the purposes of this Section, "Sale", "Sell", "Sold", "Share" or other similar applicable terminology has the meanings provided in the CCPA, VCDPA and other United States' Data Protection Laws, NINJAHIRE shall constitute a "Service Provider", "Processor" or other role assigned by other similar applicable terminology as defined in the CCPA, VCDPA and other United States' Data Protection Laws, and "Services" shall mean the services specified in the Agreement.

In compliance with the United States' Data Protection Laws, NINJAHIRE shall (i) not Sell or Share any Customer Personal Data; (ii) not retain, use or disclose any Customer Personal Data outside of the direct business relationship between NINJAHIRE and Customer, or for any purpose (including a commercial purpose) other than for the specific purpose of providing the Services to Customer or as permitted by the United States' Data Protection Laws and implementing regulations; (iii) not collect, sell, or use the Customer Personal Data that is disclosed to it by Customer except as necessary to perform the Services; (iv) ensure that each person, employee, and/or contractor processing Customer Personal Data is subject to a duty of confidentiality with respect to such data; (v) without Customer's instruction not combine the Customer Personal Data with Personal Information NINJAHIRE receives from or on behalf of, another person or persons, or collects from its own interaction with a Consumer; (vi) notify the Customer if NINJAHIRE makes a determination that it can no longer meet

its obligations under any United States' Data Protection Laws, at which time the Services shall be deemed terminated for cause in accordance with the applicable terms of the Agreement, and Section 3.10 shall apply.

NINJAHIRE certifies that it understands and will comply with the requirements and restrictions set forth in this Section and with all applicable provisions of the United States' Data Protection Laws.

(End)

Schedule 1 – Details of Processing

A. LIST OF PARTIES

The Parties as identified in the Service Order and/or Customer's NINJAHIRE account.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Customer's employees and potential job candidates.

Categories of personal data transferred: the personal data Customer uploads or inputs to NINJAHIRE's Services including, but not limited to, names, email addresses, general location, social media profile links, telephone or mobile number, employment history information, education history information, job skills, projects, publications, communications, login credentials, and calendar events.

Sensitive data transferred: Not applicable, unless Customer elects to enable and use the Diversity Features in which case the following inferred sensitive data will be processed by NINJAHIRE on Customer's behalf and made available to Customer in the NinjaHire platform: gender, race/ethnicity.

The legal basis for the processing of sensitive data shall be found in the Agreement unless otherwise specified by the Customer as follows:_____.

The frequency of the transfer: As frequent as necessary to provide the Services.

Nature of the processing: Processing data for the Authorized Purposes as set out herein.

Purpose(s) of the data transfer and further processing: The Authorized Purposes as provided herein, namely candidate relationship management.

The period for which the personal data will be retained: For the duration of Customer's use of the Services.

For transfers to (sub-) processors: As necessary to provide the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identified competent supervisory authority in accordance with Clause 13: Irish supervisory authority for personal data transferred out of the European Economic Area, Swiss supervisory authority for

personal data transferred out of Switzerland, and UK supervisory authority for personal data transferred out of the UK.

Schedule 2 – Technical and Organizational Security Measures

NINJAHIRE has implemented and will maintain appropriate technical and organizational security measures, subject to NINJAHIRE's update from time to time, for the Processing of Customer Personal Data including the following:

Security Measures	Description
Measures for data center security and encrypted data at rest	NINJAHIRE's physical infrastructure is hosted and managed within Amazon's security data centers using Amazon Web Services (AWS) in the U.S., which is subject to Amazon's continuous risk management and recurring assessments to ensure compliance with industrial standards which can be found here: https://aws.amazon.com/security/ • Customer data is stored encrypted in AWS with snapshots backed by Amazon S3. All data at rest is encrypted using Advanced encryption Standard (AES) 256, a symmetric-key encryption standard using 256-bit encryption keys.
Measures for access controls	NINJAHIRE will ensure the following: • Limiting access to its information systems and the facilities in which they are housed to properly authorized persons; • Access is granted based on principles of the least privilege and need-to-know governed by role and individual user profile. • Access by NINJAHIRE personnel to Customer Data is removed upon termination of employment or a change in job status that results in the personnel no longer requiring access to Customer Data; and • System passwords conform to strong password standards (8 characters minimum) that include length, complexity and expiration. A maximum of six (6) password attempts can be made, after which access is blocked until the password is reset by authorized personnel. Password policies conform with NIST Special Publication 800-53. • Authorized NINJAHIRE personnel must pass two-factor authentication to have access to systems or applications. Access authentication supports SAML 2.0 and SSO integration. NINJAHIRE utilizes MFA, AWS SSO and Okta IdP to prevent unauthorized access to the systems and software application.

Security Measures	Description
Measures for data encryption in transit	All communications to Customers transmitted over the internet are encrypted. NINJAHIRE utilizes encryption on its own email servers to ensure point-to-point encryption via opportunistic TLS 1.2. All Customer Data storage and backups are encrypted with high-grade encryption. NINJAHIRE enables HTTPS for Customer facing web-services and internal services including database connections to protect sensitive data transmitted to and from applications.
Measures for penetration testing and vulnerability assessment	NINJAHIRE monitors its network and production systems and implements and maintains security controls and procedures designed to prevent, detect, and respond to identified threats and risks. Such monitoring and testing include, but is not limited to, the following: • Employing an industry standard network intrusion detection system to monitor and block suspicious network traffic; • Reviewing access logs on servers and security events and retaining network security logs for 180 days; • Reviewing all access to production systems; • Performing network vulnerability assessments on a regular basis. Scans will be performed using industry standard scanning tools that identify application and hosting environment vulnerabilities. NINJAHIRE shall maintain a vulnerability remediation program; and • Engaging third parties to perform network penetration testing on at least an annual basis.
Measures for end-point device control	• All endpoints run an anti-virus solution and apply timely signature updates; and • All critical, exploitable vulnerabilities are patched in a timely manner.
Measures for data backup and ensuring high availability	The database backup for the Services occurs on the following frequencies: backups are performed daily and retained for 30 days in AWS (U.S. West Region). All backup data is encrypted using AES-256 encryption. The Services use Kubernetes and Terraform which automates disaster recovery, web application and database restoration. The Services are designed to dynamically deploy the web-services within AWS cloud regions, actively monitor for service failures, and recover any failed platform components.
Measures for data retention and destruction	Customer Data is retained for up to a requested period by Customer. Customers can request to remove any Customer Data during the term of the underlying service agreement. If no instructions from Customer are provided,

Security Measures	Description
	Customer Data will not be retained for more than 3 years. Personal Data will not be retained for a longer period than necessary under the applicable data protection law. Upon the expiration of the data retention period, Customer Data will be destroyed, rendering the data unrecoverable. Decommissioning in AWS follows the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization").
Measure for secure development practices	NINJAHIRE is audited and governed through SOC and ISO27001 compliance and will actively monitor and apply development best practices to mitigate known vulnerability types such as those on the OWASP Top 10 Web Application Security Risks.
Measures for security management and governance	NINJAHIRE complies with its internal incident management and response policy, internal risk management policy, and change control and security patch policy to log and track all changes and incidents, monitor progress and approve resolutions.
Measures for security assurance	NINJAHIRE maintains controls over security systems through dedicated personnel and ensures such controls meet the high standard industrial certifications or assurance program.
Measures for data minimization, data portability, and data erasure	NINJAHIRE will only process Personal Data that is strictly necessary for the purposes for which they are collected. NINJAHIRE personnel will collect only the minimum required amount of data to fulfill one's responsibility. Customer Data can be exported in .csv format at any time. NINJAHIRE will follow Customer's instruction to delete or destruct Customer Data upon request in accordance with the decommissioning techniques of AWS as detailed in NIST 800-88.
Measures for data quality	NINJAHIRE has no responsibility for the accuracy of Customer Data; however, NINJAHIRE uses commercially reasonable efforts to monitor the quality of Personal Data collected by NINJAHIRE's data suppliers through the following: • Performing due diligence before onboarding a data supplier; • Ensuring data quality through testing and evaluation; • Requiring data suppliers to be contractually obligated to ensure data quality and accuracy; and • Refreshing data frequently.

Security Measures	Description
Measures for accountability	NINJAHIRE performs data protection impact assessments of the processing that it carries out to identify the measures to apply and ensure that Personal Data is processed in accordance with legal requirements. NINJAHIRE has policies in address: • Refreshing data frequently; • Appropriate organizational controls and policies; • Appropriate contractual safeguards with customers or vendors to process Personal Data; • Procedures to log, monitor and report any violations; • Procedures of handling data subject inquiries; and • Appropriate intervals to review and evaluate the foregoing.

DATA PROCESSING AGREEMENT

- Data Processing Addendum -

1. Scope and order of precedence

In the event that Customer receives Personal Data and/or Personal Information from NINJAHIRE, including but not limited to, via searching, accessing, filtering, etc. NINJAHIRE's Talent Database and/or receiving Rediscovery Data, this Data Processing Addendum is appended to and incorporated as part of the Data Processing Agreement (the "**DPA**"). This DPA Addendum will be effective until such time as Customer is no longer Processing NINJAHIRE Personal Data through NINJAHIRE's Services. Capitalized terms in this DPA Addendum not defined herein shall have the definitions ascribed thereto in NINJAHIRE's Terms of Use or an applicable Master Services Agreement (each an "**Agreement**") or DPA, as applicable.

2. Definitions

In this DPA Addendum, the following capitalized bold terms will have the following meanings:

"Authorized Purposes" means to identify candidates for possible recruitment and make initial contact with such candidates.

"Data Privacy Framework" means the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce.

"NINJAHIRE Personal Data" means Personal Data and/or Personal Information (as those terms are defined under the applicable Data Protection Laws) provided to Customer by NINJAHIRE in connection with the Services.

3. NINJAHIRE Personal Data

3.1 Customer's Responsibilities

Customer is the Controller (and/or Business, as applicable), pursuant to the Data Protection

Laws, with respect to any NINJAHIRE Personal Data it receives from NINJAHIRE and further processes on NINJAHIRE's systems or information technology environment (e.g. searching, sorting, outreach, feedback, etc.). Customer is also the Controller (and/or Business, as applicable), of any NINJAHIRE Personal Data that it transfers from NINJAHIRE's systems or information technology environment.

Customer shall abide by all obligations applicable to it under the Data Protection Laws and Data Privacy Framework with respect to its processing of NINJAHIRE Personal Data and shall provide the same level of privacy protection to NINJAHIRE Personal Data as required by such laws and Data Privacy Framework. NINJAHIRE has the right to take reasonable and appropriate steps to help ensure that Customer uses NINJAHIRE Personal Data in a manner consistent with the Customer's obligations under relevant Data Protection Laws and the Data Privacy Framework . Customer shall notify NINJAHIRE if it makes a determination that it can no longer meet its obligations under relevant Data Protection Laws and/or the Data Privacy Framework, and upon such notification, NINJAHIRE has the right to take reasonable and appropriate steps to stop and remediate unauthorized use of NINJAHIRE Personal Data.

Customer shall process NINJAHIRE Personal Data only as permitted by NINJAHIRE's Terms of Use and/or an applicable Master Services Agreement and for the Authorized Purposes set forth herein. Customer will treat NINJAHIRE Personal Data with strict confidence and take all reasonable steps to ensure that persons Customer employs and/or persons engaged at Customer's place(s) of business who will process NINJAHIRE Personal Data are aware of and comply with this DPA Addendum and are under a duty of confidentiality with respect to NINJAHIRE Personal Data no less restrictive than the duties set forth herein.

Customer will implement appropriate security (including both organizational and technical) measures to protect against, without limitation, the accidental, unlawful or unauthorized access to or use, transfer, destruction, loss, alteration, commingling, disclosure or processing of NINJAHIRE Personal Data and ensure a level of security appropriate to the nature of such data and the risks presented by Customer's processing of such data. These measures shall remain in place throughout the duration of Customer's processing of NINJAHIRE Personal Data.

Customer shall not transfer NINJAHIRE Personal Data to third parties except as permitted by NINJAHIRE's Terms of Use and/or an applicable Master Services Agreement, for the Authorized Purposes set forth herein, and under contracts that guarantee at least a level of data protection and information security as provided for herein.

3.2 NINJAHIRE's Responsibilities

NINJAHIRE has collected, and continues to collect, NINJAHIRE Personal Data in accordance with applicable law as an independent Controller and/or Business, as applicable, and shall provide such data to Customer in accordance with applicable law.

NINJAHIRE represents that it is certified to the Data Privacy Framework and complies with the Data Privacy Framework principles.

3.3 Data Subject Rights; Notice and Cooperation

Customer shall immediately notify NINJAHIRE of: (i) any breach of security or unauthorized access to NINJAHIRE Personal Data that Customer detects or becomes aware of, (ii) any Data Subject requests to access, delete, release, correct, or block access to NINJAHIRE Personal Data held in NINJAHIRE's systems or information technology environment; or (iii) any other complaint, inquiry, or request from a Data Subject or government or regulatory agency regarding NINJAHIRE Personal Data, unless such notice is prohibited by law. With respect to NINJAHIRE Personal Data residing on NINJAHIRE's systems or information technology environment, NINJAHIRE shall be responsible for responding to Data Subject requests to exercise their rights under the applicable Data Protection Laws. Customer will refrain from notifying or responding to any Data Subject, government or regulatory agency, or other third party, for or on behalf of NINJAHIRE, unless NINJAHIRE specifically requests in writing that Customer does so, except as and when otherwise required by an applicable Data Protection Law.

3.4 Cross Border Transfers

If NINJAHIRE Personal Data subject to the European Data Protection Laws is transferred outside of the European Economic Area, Switzerland or any European Commission approved country, then Customer hereby agrees to and hereby enters into the Controller to Controller Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses (Module One)) ("**C2C SCCs**") with NINJAHIRE, and the following terms shall apply: (A) NINJAHIRE will be the "data exporter" and Customer will be the "data importer"; (B) the optional Clause 7 docking clause will not apply; (C) in Clause 11, the optional language will not apply; (D) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law for personal data transferred out of the European Economic Area or Swiss law for personal data transferred out of Switzerland; (E) in Clause 18(b), disputes will be resolved before the courts of Ireland for personal data transferred out of the European Economic Area or Switzerland for personal data transferred out of Switzerland; (F) Annex I will be deemed completed with the information set out in Schedule 1 of this DPA Addendum, with NINJAHIRE as the data exporter and Customer as the data importer; and (G) Annex II will be deemed completed with the information set out in Schedule 2 of the DPA.

For purposes of any transfers of personal data also subject to the Swiss FADP, the C2C SCC shall apply with the following amendments:

(A) References to "Regulation (EU) 2016/679" or "that Regulation" are to be interpreted as references to the Swiss FADP; (B) References to "Regulation (EU) 2018/1725" are removed; (C) References to "Union", "EU", and "EU Member State" shall be interpreted to mean Switzerland; (D) Clause 13 (a) and Part C of Annex I are not used and the competent supervisory authority is the Federal Data Protection and Information Commissioner (the "FDPIC"); (E) Clause 17 is replaced to state that "These Clauses are governed by the laws of Switzerland"; (F) Clause 18 is replaced to state: "Any dispute arising from these Clauses relating to the Swiss FADP shall be resolved by the courts of Switzerland. A data subject may bring legal proceedings against the data exporter and/or data importer before the courts in the Canton of Zug. The parties agree to submit themselves to the jurisdiction of such courts."

If NINJAHIRE Personal Data subject to UK Data Protection Laws is transferred outside of the UK, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner in force 21 March 2022 is agreed to and incorporated by reference, but, as permitted by clause 17 of such addendum, the parties agree to change the format of the information set out in Part 1 of the addendum such that:

- For the purposes of Table 1, NINJAHIRE shall be the "exporter" and Customer shall be the "importer," with the applicable details the same as identified in the Agreement.
- For the purposes of Table 2, (A) the EU SCCs shall apply, (B) Module 1 will apply to the personal data transferred to a third country; (C) in Clause 7, the optional docking clause will not apply; (D) in Clause 11, the optional language will not apply; (E) in Clause 17, Option 1 will apply, and, the EU SCCs will be governed by the laws of the UK for personal data transferred out of the UK; (F) in Clause 18(b), disputes will be resolved before the courts of the UK for personal data transferred out of the UK.
- For purposes of Table 3, Annex IA and Annex IB will be deemed completed with the information set forth in Schedule 1 of this DPA Addendum, with NINJAHIRE as the data exporter and Customer as the data importer, and Annex II will be deemed completed with the information set forth in Schedule 2 of theDPA.
- For purposes of Table 4, neither party may terminate this DPA Addendum when the Approved DPA Addendum changes.

(End)

Schedule 1 – Details of Processing

A. LIST OF PARTIES

The Parties as identified in the Service Order and/or Customer's NINJAHIRE account.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Potential job candidates.

Categories of personal data transferred: The personal that NINJAHIRE collects and provides to Customer, or that Customer accesses and processes using NINJAHIRE's Services, including names, email addresses, general location, social media profile links, telephone or mobile number, employment history information, education history information, job skills, projects, and publications.

Sensitive data transferred: N/A

The frequency of the transfer: As frequent as necessary to provide the Services.

Nature of the processing: Processing data for the Authorized Purposes as provided in the DPA Addendum.

Purpose(s) of the data transfer and further processing: The Authorized Purposes as provided in the DPA Addendum, namely to identify candidates for possible recruitment and make initial contact with such candidates.

The period for which the personal data will be retained: For the duration of Customer's use of the Services.

For transfers to (sub-) processors: As necessary to provide the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identified competent supervisory authority in accordance with Clause 13: Irish supervisory authority for personal data transferred out of the European Economic Area, Swiss supervisory authority for personal data transferred out of Switzerland, and UK supervisory authority for personal data transferred out of the UK.