DATA PROCESSING ADDENDUM

This Data Processing Addendum ("Addendum") details the parties' obligations regarding the protection of personal data associated with the processing by gr8 People, Inc. ("Vendor") of personal data on behalf of its customers who execute an Agreement that references this Addendum (each a "Customer"). This Addendum applies to any and all activities associated with the Agreement, in whose scope Vendor or Vendor's subcontractors or agents process personal data on behalf of Customer, but only to the extent (i) such personal data pertain to data subjects in the European Economic Area and/or (ii) Vendor is otherwise subject to the Data Protection Laws.

1. ROLES. The parties acknowledge and agree that with regard to the processing of personal data, Customer is either a controller or a processor and Vendor is a processor or sub-processor.

2. COMPLIANCE. Each party will comply with the Data Protection Laws.

3. PERSONAL DATA PROCESSING DETAILS. The personal data processing details are set forth in Schedule 1.

4. INSTRUCTIONS. Vendor agrees that it will process personal data in accordance with Customer's documented instructions. Customer instructs Vendor to process personal data to provide Vendor's products and services in accordance with the Agreement and this Addendum. Customer may provide additional instructions to Vendor to process personal data; however, Vendor will be obligated to perform such additional instructions only if they are consistent with the terms and scope of the Agreement and this Addendum. If Vendor is required to process personal data pursuant to applicable law, Vendor will notify Customer of any such requirement before processing the personal data (unless that law prohibits such information on important grounds of public interest). Vendor will promptly inform Customer if, in Vendor's reasonable opinion, a Customer instruction would infringe the Data Protection Laws.

5. TECHNICAL AND ORGANIZATIONAL MEASURES. Vendor has implemented and maintains appropriate technical and organisational measures to ensure a level of security commiserate to the risk to the personal data. Such measures include taking appropriate administrative, physical, organizational, and technical safeguards to prevent and guard against the unauthorized or accidental access, disclosure, destruction, loss, processing, damage, or alteration of personal data.

6. SUB-PROCESSORS.

6.1. **Use of Sub-Processors.** Customer authorizes Vendor to appoint Sub-Processors to process personal data, so long as Vendor provides Customer an up-to-date list of all Sub-Processors used to process personal data prior to allowing any Sub-Processor to process personal data. Such list will be provided in the form of Schedule 2 attached hereto. Vendor will make available to Customer upon Customer's written request a list of Sub-Processors authorized to process personal data.

6.2. **Notification of New Sub-Processors.** Vendor will provide notice to Customer at least 30 days prior to authorizing any new Sub-Processor to process personal data.

6.3. **Objection to New Sub-Processor.** If Customer objects to Vendor's use of a new Sub-Processor, Customer must notify Vendor in writing within 10 days following Vendor's notification pursuant to Section 6.2 above. Vendor will have the right to cure the objection by: (i) cancelling its plans to use the Sub-Processor with regard to Customer's personal data or offering an alternative to provide the services without such Sub-Processor; (ii) taking the corrective steps requested by Customer in its objection and proceed to use the Sub-Processor with regard to Customer's personal data; (iii) not providing, or Customer may agree to not use, the particular aspect of the service that would involve the use of such Sub-Processor with regard to Customer's personal data; or (iv) if none of the above options are reasonably available and Vendor has not addressed Customer's reasonable concerns about the Sub-

Processor within 30 days from Customer's initial objection, Customer may terminate the affected service on written notice without penalty to Customer.

6.4. **Sub-Processor Contracts.** Vendor will ensure that Sub-Processors appointed in accordance with this Section 6 are appointed under a binding written contract that meets the requirements of the Data Protection Laws ("**Sub-Processor Contract**"). Customer may request a copy of the Sub-Processor Contract, provided that Vendor may redact portions of the Sub-Processor Contract that are confidential or not relevant to the services provided to Customer. The appointment of a Sub-Processor will not in any way limit the obligations of Vendor to Customer under the Agreement. Vendor will remain liable for any breach of this Addendum that is caused by an act, error, or omission of its Sub-Processor.

7. VENDOR'S PERSONNEL. Vendor will ensure that its personnel engaged in the processing of personal data are informed of the confidential nature of the personal data and have executed written contracts to maintain the confidentiality of personal data. Vendor will take all reasonable steps to ensure the reliability of Vendor personnel processing personal data and that Vendor personnel processing personal data receive adequate training on compliance with this Addendum and the Data Protection Laws applicable to the processing.

8. DATA SUBJECT RIGHTS. Vendor will, without undue delay, notify, then record, and then refer to Customer full details of all: (i) Data Subject Requests; and (ii) complaints or other requests relating to a party's obligations under Data Protection Laws, or relating to personal data or a data subject ("Complaint"). To the extent Customer is unable to respond to a Data Subject Request or a Complaint using information available through Vendor's products or services, Vendor will provide reasonable assistance to Customer (and procure that any relevant Sub-Processor does the same) in responding to a Data Subject Request or Complaint. Vendor will not respond to a Data Subject Request or Complaint absent Customer's explicit instruction.

9. ASSISTANCE. Vendor will provide assistance as Customer reasonably requires (taking into account the nature of processing and the information available to Customer) as mandated by the Data Protection Laws with respect to: (i) DPIAs, by providing such information and cooperation as Customer may reasonably require for the purpose of assisting Customer in carrying out a DPIA; and (ii) prior consultation with a Supervisory Authority regarding high risk processing in consultation with Customer.

10. RECORDS. If required under Data Protection Laws, Vendor will maintain complete, accurate, and up to date written records of all categories of processing activities carried out on behalf of Customer as required by the Data Protection Laws, including: (i) the name and contact details of each of its Sub-Processors carrying out specific processing activities on behalf of Customer; (ii) the categories of processing carried out on behalf of Customer; (iii) where applicable, transfers of data to an international recipient; and (iv) a general description of its technical and organizational security measures as required by the Data Protection Laws.

11. INSPECTIONS. Customer may request once per calendar year (unless otherwise required by Data Protection Laws) to carry out an audit and/or on-site inspection of the technical and organisational measures, systems, and facilities relevant to the processing of personal data and protection of such personal data in order to verify compliance with this Agreement and Data Protection Laws. If Customer wishes to conduct an on-site audit using a third party auditor, Vendor may object to Customer's choice of third party auditor on reasonable grounds and in such event, Customer will select a different auditor. Customer will reimburse Vendor for any time expended in relation to such on-site inspection at Vendor's then-current professional services rate. Customer and Vendor will mutually agree upon the scope and timing of an audit or inspection prior to any such audit or on-site inspection. An audit or inspection performed pursuant to this Section 11 will not exceed one business day and will not unreasonably interfere with the normal conduct of Vendor's business. Customer (or Customer's third party auditor) will at all times comply with the use, security, and access policies at and for such location as may be in effect from time to time, including Vendor's health, safety, and environmental requirements. Customer is

responsible, and is fully liable, for the actions and omissions of its personnel and third party auditors while on Vendor's premises and/or inspecting Vendor's systems and facilities, and Customer will require its personnel and third party auditors to follow Vendor's safety and security rules as well as Vendor's guidelines, policies, and instructions. Customer will promptly notify Vendor with any information regarding any non-compliance discovered during the course of an audit or inspection. Any audit or inspection performed pursuant to this Section 11 will be conducted under a non-disclosure agreement and any information or report derived from such inspection will be deemed Vendor's confidential information.

12. SUSPENSION. Customer may suspend the transfer of personal data to Vendor, Vendor's processing of personal data, or terminate the affected Agreement without penalty to Customer if: (i) Vendor or a Vendor Sub-Processor is in breach of its obligations under this Addendum and does not cure such breach within 30 days of Customer's notification to Vendor of such breach; or (ii) if Vendor notifies Customer that it cannot comply with the obligations set forth in this Addendum or the Data Protection Laws.

13. PERSONAL DATA BREACH.

13.1. **Personal Data Breach Notification.** In respect of any personal data breach related to the Agreement or this Addendum involving Vendor (or a Sub-Processor), Vendor will, without undue delay of Vendor becoming aware of such personal data breach:

13.1.1. notify Customer of the personal data breach; and

13.1.2. provide Customer with such details as Customer reasonably requires regarding:

(a) the nature of the personal data breach, including the categories and approximate numbers of data subjects and personal data records concerned;

(b) any investigations into such personal data breach;

(c) the likely consequences of the personal data breach; and

(d) any measures taken, or that Vendor recommends, to address the personal data breach, including to mitigate its possible adverse effects and prevent the re-occurrence of the personal data breach or a similar breach.

13.2. **Ongoing Updates.** Vendor may give Customer phased updates as additional information regarding the personal data breach becomes available to Vendor; and provide reasonable cooperation and assistance to Customer in relation to any remedial action to be taken in response to a personal data breach, but will not notify any data subjects of the personal data breach, absent Customer's explicit instruction or as required by any law, rule, regulation, or binding court order to which Vendor is subject.

13.3. **Notification Sharing.** Customer may share any notification and details provided by Vendor under this Section 13 with the appropriate Supervisory Authority if required to do so under the Data Protection Laws.

14. DELETION OR RETURN OF PERSONAL DATA. Vendor will promptly, but without undue delay, return to Customer, or destroy, to the extent permitted by law, personal data upon Customer's written request or the termination or expiration of the Agreement. Vendor may retain personal data to the extent required by the laws, rules, and regulations to which Vendor is subject, or if personal data resides in backup archives. Vendor will continue to protect the security and confidentiality of such retained personal data in accordance with the Agreement and this Addendum. Vendor has implemented retention rules so that personal data in backup archives is retained for as short a time as necessary before being automatically deleted.

15. CLIENT DATA DISCLOSURES. To the extent legally permissible, Vendor will promptly notify Customer of any legally binding request for disclosure or seizure of personal data by a government agency or law enforcement authority.

16. DATA TRANSFER.

16.1. **Cross Border Transfer Mechanisms.** Vendor will not, other than in accordance with Customer's instructions, transfer any personal data to any country or territory outside the European Economic Area unless that country or territory has been declared to provide an adequate level of protection for personal data by the European Commission. Where Customer does consent or has consented to the transfer or processing of personal data outside of the European Economic Area, the parties shall comply with the applicable provisions of the Data Protection Laws relating to the transfer of personal data outside of the European Economic Area and undertake to take steps necessary to comply with those provisions or to provide and make use of Vendor's services without making such transfers.

16.2. **Alternate Mechanisms.** To the extent that the parties are relying on a specific statutory mechanism to normalize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the parties agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

17. TERM. The term of this Addendum will end simultaneously and automatically at the later of (i) the termination of the Agreement; or (ii) when all personal data is deleted from Vendor's systems.

18. DEFINITIONS AND INTERPRETATION.

18.1. **Definitions.**

The terms "processor", "controller", "data subject", "personal data", "processing", "process", and "personal data breach" all have the meanings given to those terms in the Data Protection Laws.

"Data Subject Request" means a request made by a data subject to exercise any data subject rights granted by Data Protection Laws.

"DPIA" means a data protection impact assessment or privacy impact assessment (as defined or used in the Data Protection Laws, including relevant guidance from Supervisory Authorities).

"Data Protection Laws" means:

(a) the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR");
(b) all relevant European Union member state laws or regulations giving effect or corresponding with the GDPR;
(c) the laws, regulations, or other binding obligations (including any and all legislative and/or regulatory amendments or successors thereto) of the European Union, European Economic Area, Switzerland, and the United Kingdom that govern or apply to personal data; and
(d) any judicial or administrative interpretation of any of the above, any guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority and binding under applicable law,

in each case, as in force and applicable, and as may be amended, supplemented, or replaced from time to time.

"Sub-Processor" means another processor engaged by Vendor for carrying out processing activities in respect of the personal data on behalf of Customer and authorised by Customer in accordance with Section 6.

"Supervisory Authority" means any local, national, or multinational agency, department, official, parliament, public, or statutory person or any government or professional body, regulatory, or supervisory authority, board, or other body responsible for administering Data Protection Laws.

18.2. **Interpretation and Applicability.** This Addendum relates to the processing of personal data that is subject to Data Protection Laws.

SCHEDULE 1

DATA PROCESSING DETAILS

NATURE AND PURPOSE OF THE PROCESSING:

Processing of candidate data for support of Customer's recruiting process.

DURATION OF THE PROCESSING:

The duration of processing will be for the duration of the Agreement.

TYPE OF PERSONAL DATA:

Recruiting related information, including name, email, telephone, address, resume (CV) and data which may be included on the same, employment history, email communication between Customer and Data Subject, offer letter and details of employment.

CATEGORIES OF DATA SUBJECTS:

Jobseekers/candidates

SCHEDULE 2

SUB-PROCESSORS

Sub-Processor: Amazon

Personal Data Processed: n/a

Type of Processing:Hosting

Sub-Processor: Daxtra

Personal Data Processed: Pass personal data to GR8 People; GR8 People initiates opt-in

Type of Processing:Job Board Search

Sub-Processor: GoodData

Personal Data Processed: Person Name

Type of Processing: Aggregate reporting

Sub-Processor: Rchilli

Personal Data Processed: n/a

Type of Processing: Resume Parsing/Parsing of uploaded resume; no storage of data by Rchilli