Data Processing Addendum

This Data Processing Addendum (the "Addendum") is in addition to the Software as a Service agreement entered into between EnterpriseJungle, Inc., ("Service Provider") and you ("Subscriber") that incorporates this Addendum by reference (the "Agreement"), and governs the Processing of Personal Data by EnterpriseJungle, Inc. in providing its EnterpriseAlumni service pursuant to the Agreement.

If you would like to complete a countersigned copy of this Addendum for your records, the following are the instructions for completing such a copy:

1. This Addendum has been pre-signed on behalf of EnterpriseJungle. The Clauses have been pre-signed by EnterpriseJungle as the data importer and processer.
2. To complete a countersigned copy of this Addendum, you must:
   (a) Complete the information in the signature box and sign this Addendum below.
   (b) Send the completed and signed Addendum by email to infosec@enterprisealumni.com

1. Definitions

"**Authorized Person**" means any person the Supplier authorizes to process Subscriber Data, which may include the Supplier's staff, agents and subcontractors;

"**Data Protection and Security Schedule**" means this Schedule;

"**Data Protection Laws**" means all applicable laws and regulations relating to the processing of personal data (including where applicable the guidance and codes of practice issued by a regulator), and in particular:

(a) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data; and

(b) on and after 25 May 2018, the GDPR,

including the equivalent of any of the foregoing in any relevant jurisdiction and any implementing and supplemental legislation;

"**GDPR**" means 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;

"**HIPAA**" means the US Health Insurance Portability and Accountability Act of 1996;

"**PCI DSS**" means the Payment Card Industry Data Security Standard, as updated and maintained by the PCI Security Standards Council from time to time;

"**Subscriber Data**" means Subscriber's Confidential Information, Subscriber Materials and Subscriber Personal Information;

"**Subscriber Materials**" means all text, images, literary and artistic works, photographic works, films, animations, videos, software, databases, instructions, documents, layout, design, trademarks and logos or similar materials which may be supplied by or on behalf of Subscriber to the Supplier or be created by Supplier or on behalf of Supplier;

"**Subscriber Personal Information**" means personal data processed by the Supplier as a processor or sub-processor for and on behalf of Subscriber or its customers;

"**personal data**" means personal data, personal information, personally identifiable information or covered information related to an identifiable individual as applicable and defined under applicable Data Protection Laws;

"**controller**" has the meaning given to it under applicable Data Protection Laws, provided, however, that to the extent the applicable Data Protection Laws do not provide such definition or meaning, "controller" means and refers to the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

"**process**" has the meaning given to it under applicable Data Protection Laws, and "**processing**" and "**processed**" shall have the corresponding meaning; provided, however, that to the extent the applicable Data Protection Laws do not provide such definition or meaning, "process," "processing" and "processed" mean and refer to any operation or set of operations performed on personal data, whether or not by automated means, including, without limitation, collection, recording, organization, structuring, storage, adaptation, alteration, accessing, retrieval, consultation, use, disclosure by transmission, dissemination, distribution or making available by other means, alignment, combination, restriction, erasure, deletion or destruction;

"**processor**" has the meaning given to it under applicable Data Protection Laws, provided, however, that to the extent the applicable Data Protection Laws do not provide such definition and meaning, "processor" means and refers to a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"**Security Incident**" means the loss of, or attempted or successful unauthorised access, use, disclosure, modification, or destruction of, any Subscriber Data, other Subscriber materials, or any information system that hosts or otherwise processes Subscriber Data.

2. Scope and conflicts

2.1 The Parties acknowledge and agree that, for the purposes of this Agreement:

(a) Subscriber is, or shall be regarded as, a controller of Subscriber Personal Information and the Supplier is, or shall be regarded as, a processor of Subscriber Personal Information; or

(b) Subscriber is, or shall be regarded as, a processor of Subscriber Personal Information (acting on behalf of its customers) and the Supplier is, or shall be regarded as, a sub-processor of Subscriber Personal Information.

2.2 To the extent that any term of this Data Protection and Security Schedule conflicts with the terms of the rest of this Agreement then the terms of this Data Protection and Security Schedule shall prevail.

3. Processing instructions

3.1 The Supplier shall:

(a) only process Subscriber Personal Information as required to perform its obligations under this Agreement;

(b) not disclose, publicize, share, copy, amend, delete, interfere, or otherwise process Subscriber Personal Information, except as otherwise permitted by this Agreement; and

(c) comply with any reasonable, lawful and written instructions from Subscriber in relation to the Supplier's processing of Subscriber Personal Information,

except where otherwise required by any Data Protection Laws applicable to the relevant Subscriber Personal Information.

3.2 In no event shall the Supplier process Subscriber Data for its own purposes or the purposes of any third party.

3.3 The Supplier shall comply with all applicable laws, including, without limitation, all applicable Data Protection Laws in respect of its processing of Subscriber Personal Information.

4. Confidentiality of processing

4.1 The Supplier shall ensure that all Authorized Persons:

(a) are and shall continue to be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process Subscriber Data who is not under such a duty of confidentiality; and

(b) process Subscriber Data only as necessary for the Supplier to perform its obligations under this Agreement.

4.2 The Supplier shall ensure that access, retrieval and other processing of Subscriber Data by Authorized Persons is restricted to those who have a legitimate and necessary reason to so access, retrieve and otherwise process such Subscriber Data for purposes of performing this Agreement.

5. Data Subject rights

5.1 The Supplier shall provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to Subscriber (at its own expense) to enable Subscriber or, if applicable, a controller for whom Subscriber is a processor, to respond to:

(a) any request relating to Subscriber Personal Information from a data subject to exercise any of its rights under any Data Protection Laws (including its rights of access, correction, objection, erasure and data portability, as applicable);

(b) any request relating to Subscriber Personal Information from a controller for access, correction, erasure, deletion and data portability, where Subscriber is a processor of the Subscriber Personal Information for such controller; and

(c) any other correspondence, enquiry or complaint received from a data subject, controller, regulator or other third party in connection with the processing of Subscriber Data.

5.2 In the event that any such request, correspondence, enquiry or complaint is made directly to the Supplier, the Supplier shall promptly inform Subscriber and provide full details of the same.

5.3 The Supplier shall not disclose any Subscriber Data in response to a request for access or disclosure from any third party without Subscriber's prior written consent, save where compelled to do so in accordance with applicable law.

6. Data protection impact assessments

If the Supplier believes or becomes aware that its processing of any Subscriber Personal Information is likely to result in a high risk to the data protection rights and freedoms of data subjects, the Supplier shall promptly inform Subscriber. In this circumstance and upon any other request by Subscriber, the Supplier shall provide Subscriber with all such reasonable and timely assistance as Subscriber may require in order for Subscriber to (or for Subscriber to assist its customers to) conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

7. Records

The Supplier shall maintain records regarding the Supplier's processing of Subscriber Personal Information, including data flow diagrams and the Supplier's processes for handling Security Incidents, for a period of two years following the completion of the Supplier's processing activities.

8. Security

8.1 The Supplier shall put in place and maintain a comprehensive information security program reasonably appropriate for the Subscriber Data, which shall include implementing and maintaining all appropriate technical, security and organizational measures to protect Subscriber Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access and against all other unlawful forms of processing.

8.2 The technical, security and organizational measures referred to under paragraph 8.1 shall at minimum meet the security requirements set out in Exhibit D-2 to this Data Protection and Security Schedule.

8.3 Where the Supplier processes, transmits, and/or stores cardholder data and/or sensitive authentication data (as defined in PCI DSS) in the performance of services provided to Subscriber, the Supplier shall comply with the provisions set out in Exhibit D-3.

8.4 Where the Supplier accesses, stores or otherwise processes personal health information subject to HIPAA in the performance of its services provided to Subscriber, the Supplier shall ensure that it executes and complies with a HIPAA Business Associate Agreement in the form set out in Exhibit D-4.

9. Security Incidents

9.1 The Supplier shall notify Subscriber immediately, and in any event no later than 24 hours, after becoming aware (or after the Supplier should have reasonably become aware) of any Security Incident or any other breach of this Data Protection and Security Schedule, including details regarding the measures the Supplier has taken to promptly remedy such Security Incident or other breach and any further information and support that Subscriber may reasonably require. All such notifications should be made to the Subscriber Security Operations Center (email: soc@Subscriber.com) in addition to any Subscriber representative the Supplier regularly liaises with.

9.2 The Supplier shall take all such measures and actions as are necessary to remedy or mitigate the effects of Security Incidents and shall keep Subscriber up-to-date about all developments in connection with Security Incidents.

9.3 After a notification to Subscriber made under paragraph 9.1, the Supplier shall promptly provide a report summarizing the Security Incident with sufficient detail to enable Subscriber to comply with any and laws and regulations, which shall include at least the following information (if known):

(a) the date, time, and description (including root cause) of the Security Incident;

(b) how the Security Incident was detected;

(c) the systems and data affected;

(d) whether the Security Incident included Subscriber Personal Information;

(e) a list of all Subscriber Data disclosed as a result of the Security Incident;

(f) any corrective action taken; and

(g) any additional planned or required corrective actions.

9.4 The Supplier shall promptly, and at mutually agreed intervals or times for the duration of the Security Incident, provide Subscriber such additional documentation concerning the Security Incident, which may include the results of any audit, assessments or analyses related to the Security Incident, remediation plans with milestones and dates and progress reports.

9.5 Within five (5) days of the closure of the Security Incident, the Supplier will provide Subscriber with a written report describing the Security Incident, the actions taken by the Supplier during its response and the Supplier's plans for future actions to prevent a similar incident from occurring.

9.6 At no additional charge to Subscriber, the Supplier shall provide full and timely cooperation, assistance and information to Subscriber:

(a) in the investigation of any actual or potential Security Incident; and

(b) in relation to any notifications of a Security Incident Subscriber makes to a regulator.

9.7 If so requested by Subscriber, in the event of a Security Incident which results in the processing of any Subscriber Personal Information, the Supplier shall prepare and provide notification of the Security Incident in a form approved by Subscriber, and paid for by the Supplier, to each data subject that may be affected by such Security Incident.

9.8 At its expense, the Supplier agrees to such other commercially reasonable actions as reasonably requested by Subscriber in response to a Security Incident.

9.9 The Supplier shall not make any public statements about, or notify a regulator of, a Security Incident without Subscriber's prior written consent.

10. Sub-processors

10.1 Subject to paragraph 10.2, the Supplier shall not provide access to or disclose any of the Subscriber Data to a subcontractor or other third party without Subscriber's express, prior, written authorization and subject to terms no less onerous than those imposed upon the Supplier under this Data Protection and Security Schedule.

10.2 Notwithstanding paragraph 10.1, Subscriber consents to the Supplier engaging third party subcontractors to process Subscriber Data provided that the Supplier:

(a) provides Subscriber at least 60 days' prior notice of the addition of any subcontractor (including details of the processing it performs or will perform in relation to Subscriber Data) and Subscriber has not objected to the addition of sub-contractor (and, in the event that Subscriber objects to the addition of such sub-contractor then either the Supplier shall not appoint the subcontractor or Subscriber may elect to suspend or terminate this Agreement without penalty);

(b) imposes data protection terms on any subcontractor it appoints that protect the Subscriber Data to the same standard provided for under this Data Protection and Security Schedule;

10.3 A list of subcontractors approved by Subscriber to process Subscriber Data as at the date of this Agreement is attached at Exhibit D-1 to this Data Protection and Security Schedule, and the Supplier shall maintain and provide updated copies of this list to Subscriber upon request.

10.4 The Supplier shall remain fully liable for any breach of this Agreement that is caused by an act, error or omission of any of its subcontractors who are processing Subscriber Data.

11. Audit and records retention

11.1 No more than once annually the Supplier shall complete and return to Subscriber a Subscriber audit survey within 30 days of receipt of such audit survey from Subscriber.

11.2 Any findings made as a result of the audit survey completed by Supplier under this paragraph 11 will be addressed in a mutually agreed upon remediation plan and the Supplier shall complete and comply with such remediation plan within a mutually agreeable timeframe set forth therein. Failure to correct or remediate findings shall be considered a material breach of this Agreement.

11.3 If Subscriber elects to exercise any of its audit and inspection rights it holds in relation to the records and practices of such sub-processors, the Supplier shall cooperate with Subscriber in procuring the compliance of its sub-processors, including procuring that its sub-processors complete a Subscriber audit survey.

11.4 At least annually, the Supplier shall perform a risk analysis regarding the Supplier’s systems which contain any Subscriber Data. The Supplier shall generate an audit report containing this risk analysis and send it to Subscriber for review.

11.5 The Supplier shall complete an annual attestation to certify all Subscriber Data and its licensee customers, end users, and authorized participants, is appropriately protected from improper disclosure or from unwanted intrusion and otherwise reflect its commitment and adherence to the provisions of this Data Protection and Security Schedule.

11.6 As soon as it is reasonably available, but no less frequently than once each year and from time to time upon Subscriber's request, the Supplier shall provide Subscriber a copy of its hosting and other sub-processors' most recent certified report, which for the avoidance of doubt include an ISAE3402 (SOC1) report, AIT 101 SOC 2 report or equivalently certified third party audit report which include trust principles of privacy, security, confidentiality and availability. The report shall address the internal control environment with respect to any services performed by the Supplier for Subscriber and the Supplier's processing of Subscriber Data. The Supplier shall update this report at least once each year.

11.7 Within thirty (30) days of Subscriber's receipt of an assessment or audit report, the Supplier shall provide Subscriber with a written report outlining the corrective actions that the Supplier has implemented or proposes to implement with the schedule and status of each corrective action.

11.8 The Supplier shall maintain accurate and detailed records relating to its compliance with this Data Protection and Security Schedule for a period of two (2) years after the termination or expiration of this Agreement in a format that will permit assessment or audit.

12. International data transfers

12.1 Where the Supplier processes Subscriber Data which is subject to any laws (including Data Protection Laws) of a country that prevent or impose restrictions on processing such Subscriber Data outside of such country, then the Supplier may only process (or permit the processing of) such Subscriber Data outside of such country where:

(a) it first obtains Subscriber's prior written consent; and

(b) the Supplier takes all such measures as are necessary to ensure that any processing of such Subscriber Data is in compliance with such consent, applicable laws and all other applicable terms of this Agreement.

13. Indemnity

13.1 The Supplier shall indemnify and defend Subscriber from and against any and all claims, actions, loss, cost, harm, expense (including court costs and reasonable legal fees), liabilities or damage ("Damage") suffered or incurred by Subscriber or made by any third party as a result of or in connection with the failure of the Supplier or any Supplier subcontractor to comply with any of the Supplier's obligations under this Data Protection and Security Schedule, provided that Subscriber:

(a) gives the Supplier prompt notice of any circumstances of which it is aware that give rise to an indemnity claim under this paragraph; and

(b) takes reasonable steps and actions to mitigate any ongoing Damage it may suffer as a consequence of the Supplier's failure to comply with any of its obligations under this Data Protection and Security Schedule.

14. Intellectual property

All rights in and to any Subscriber Data processed pursuant to this Agreement (including any Intellectual Property Rights) will be and remain the property of Subscriber or other applicable owner of the same. Subscriber hereby grants to the Supplier a non-exclusive license for the duration of this Agreement to use such Subscriber Data solely for the purposes of performing its

obligations under this Agreement. Save in respect of disclosure of Subscriber Data to sub-processors approved under paragraph 10, the Supplier may not disclose or sub-license the use of such Subscriber Data without Subscriber's prior written consent.

15. Effects of termination

15.1 Upon termination or expiry of this Agreement, the Supplier shall immediately cease processing the Subscriber Data.

15.2 Subject to paragraph 15.3, upon expiry or termination of this Agreement the Supplier shall (at Subscriber's election) destroy or return to Subscriber all Subscriber Data (including all copies of Subscriber Data) in its possession or control (including any Subscriber Data subcontracted to a third party for processing).

15.3 Paragraph 15.2 shall not apply to the extent that the Supplier is required by any European Union (or any European Union Member State) law or other applicable law to retain some or all of the Subscriber Data, in which case Supplier shall isolate and protect such Subscriber Data from any further processing except to the extent required by such law.

EXHIBIT 1 - LIST OF APPROVED SUB-PROCESSORS

EnterpriseJungle uses certain sub-processors, subcontractors, and content delivery networks to assist in providing the Services as described in the Agreement. More information can be found here:

https://enterprisealumni.com/infosec-compliance/enterprisealumni-sub-processors

EXHIBIT 2 – SECURITY EXHIBIT

SUBSCRIBER GLOBAL SECURITY COMPLIANCE REQUIREMENTS FOR SUPPLIERS AND PARTNERS

Part A: Introduction

1. **Overview**. This security exhibit (the "**Exhibit**") sets out Subscriber's minimum security requirements (the "**Requirements**").

2. **Definitions**. Words and expressions not defined elsewhere in this Agreement shall have the meanings set out in Annex A to this Exhibit.

3. **Relationship with rest of Agreement**. The provisions in this Exhibit are without prejudice to the provisions in the remainder of this Data Protection and Security Schedule. However, if any term in this Exhibit directly conflicts with a term of this Data Protection and Security Schedule, then the term of this Data Protection and Security Schedule shall prevail.

4. **Updates**. Subscriber reserves the right to update or otherwise modify its requirements in this Exhibit from time to time. Upon notice by Subscriber to the Supplier that the Requirements have been updated or modified, the revised version of the Requirements shall apply.

Part B: General Supplier Obligations

5. The Supplier shall implement and maintain a policy that prohibits the use of any devices that are not administered and/or managed by Supplier, Supplier's approved sub-processors or Subscriber to access and/or store Subscriber Data.

Part C: Information Security Requirements

6. **General Security Requirements**. The Supplier shall:

6.1 Be compliant with **applicable** government and industry mandated information security standards (**examples** of such standards include, **but are not limited to**, ISO/IEC 27001, the Payment Card Industry-Data Security Standards (PCI-DSS), Electronic Data Interchange (EDI) standards, and the information security requirements documented within laws, such as the Health Insurance Portability and Accountability Act - HIPAA.)

6.2 Establish and maintain a formal and comprehensive security program in accordance with Industry Best Practice with reasonable and appropriate administrative, organizational, technical, and physical safeguards, including those set out in this Part C (the "**Information Security Requirements**"), designed to ensure the security, confidentiality, integrity, and availability of Subscriber Data (including, without limitation, the privacy of Subscriber Data) and to guard against Security Incidents. Such data safeguards will include, but are not limited to, the following:

(a) Supplier shall maintain an inventory of systems used by Supplier to store or process Subscriber Data;

(b) Supplier shall have a media and non-volatile storage sanitization and destruction policy and procedure, which:

(i) requires onsite destruction or sanitization;

(ii) meets at a minimum, NIST SP 800-88 Purge and Destruction requirements; and

(iii) includes the issuance of a certificate of destruction or sanitization to Subscriber that Subscriber Data is properly wiped or destroyed,

so as not to allow for any type of data recovery at any time during or at the end of the term of this Agreement or as requested by Subscriber;

(c) Any hard copy materials containing Subscriber Data or related application support shall be secured in locked containers when not in use, and destroyed by secure shredding at any time during or at the end of the term of this Agreement or as requested by Subscriber. Certificate(s) of Destruction may be requested by Subscriber;

(d) Isolate Subscriber's applications and Subscriber Data from any other customer's or Supplier's own applications and information by using physically separate servers or (where physical separation of servers is not a condition of any agreement with the Supplier) by using logical access controls.

(e) Have documented procedures for the secure backup and recovery of Subscriber Data, which shall include, at a minimum, Strong Encryption, secure procedures for the transport, storage, and disposal of the backup copies of Subscriber Data, with documented chain of custody.

(f) Use Strong Encryption to protect Personal Information when transmitted and stored.

7. **Personnel or Staff Terms**. The Supplier shall:

7.1 where legally permissible, complete a comprehensive background investigation (in line with British Standard 7858) on all employees before providing access to Subscriber Data including verification of the identity, address, employment history/eligibility, professional qualifications of any member of Supplier's team and performing additional checks such as drug screening or criminal records (where available);

7.2 Ensure that all its employees and permitted subcontractors who handle Subscriber Data:

(a) Are informed of the confidential nature of Subscriber Data;

(b) Have undertaken training regarding:

(i) Applicable laws and regulations;

(ii) potential security incident or breach reporting, and

(iii) acceptable use of personal data and proper procedures for storing and transmission of such personal data, and

(c) Are aware of both the Supplier's and their own duties and obligations under applicable Data Protection Laws and this Agreement.

7.3 Ensure that its information security staff has reasonable and necessary experience and training in information and network protective security.

7.4 Maintain records of the training provided by the Supplier to its employees and permitted subcontractors as required herein and will make such records available to Subscriber upon request.

7.5 Have a formal policy on conditions and timelines for access to Subscriber or supplier systems to be given to individuals joining, changed for individuals moving to different roles, and removed for those individuals leaving for any reason.

8. **System Security**. The Supplier shall:

8.1 Actively monitor industry resources (e.g., www.cert.org, https://cve.mitre.org, pertinent software vendor mailing lists, and websites) for timely notification of all applicable security alerts pertaining to the Supplier's Information Resources.

8.2 Deploy one or more Intrusion Prevention Systems (IPS) or Intrusion Detection and Prevention Systems (IDPS) in an active mode of operation that monitors all traffic entering and leaving Information Resources and issues active alerts on potential threats, in environments where such technology is commercially available and to the extent practicable.

8.3 Have and use a documented process to remediate security vulnerabilities in its Information Resources including those discovered through industry publications, risk assessments, audits, vulnerability scanning, virus scanning, and the review of security logs, and apply appropriate security patches promptly with respect to the probability that such vulnerability can be or is in the process of being exploited.

8.4 Ensure that all of the Supplier's Information Resources are and remain 'hardened' including removing or disabling unused network and other services (e.g., finger, rlogin, ftp, and simple Transmission Control Protocol/Internet Protocol (TCP/IP) services) and installing a system firewall, Transmission Control Protocol (TCP) wrappers or similar technology.

8.5 Change all default account names and/or default passwords prior to deployment.

8.6 Limit system privileged (also known as root, admin, DBA, or super user) access to operating systems and applications intended for use by multiple users only to individuals requiring such high-level access in the performance of their jobs. System administrator, root, privileged, and/or super user access must not be used for day-to-day work and all activity must be logged to a unique identifier with active alerting or regular log reviews. The Supplier shall keep accurate and detailed records of all members of the Supplier's team who have root access and privileged access to Subscriber Data (including the level of access supplied).

8.7 Require application, database, network, and system administrators to restrict access by users to only the commands, data and Information Resources necessary for them to perform authorized functions.

9. **Physical Security**. The Supplier shall:

9.1 Ensure that all systems used to process and store Subscriber Data will be in secure, monitored and access-controlled premises;

9.2 Locate all Information Resources in secure physical facilities with access limited and restricted to authorized individuals only;

9.3 Locate all Information Resources in geographies that provide an adequate legal framework to ensure compliance with the terms and conditions of this Agreement;

9.4 Monitor and record, for audit purposes, access to the physical facilities containing Information Resources intended for use by multiple users, including the name of the employee, time and date of entry and exit, and where feasible, monitor the room by camera.

10. **Network Security**. The Supplier shall:

10.1 Always use Strong Encryption (e.g. FIPS 197) to protect Subscriber Data when transmitted over any Subscriber-controlled or Supplier-controlled network. This also applies to Subscriber Data contained in an email, or the attachments embedded within the email. For example, where the text in an email does not contain Subscriber Data, but the embedded attachments within that email do contain Subscriber Data, then the embedded attachments, but not the email, must be encrypted.

10.2 Use Strong Encryption for the transfer of Subscriber Data outside of Subscriber-controlled or Supplier-controlled networks or when transmitting Subscriber Data over any untrusted network (in-transit).

10.3 Only remove Subscriber Data from its premises if authorized in writing by Subscriber. If so authorized (e.g., in connection with offsite storage of data backups), such Subscriber Data may only be transported on devices configured with full disk encryption to protect the data from loss or theft.

10.4 Require Strong Authentication for any remote access use of non-public Information Resources.

10.5 Not store Subscriber Data on removable media (e.g., USB flash drives, thumb drives, memory sticks, tapes, CDs, or external hard drives) except: (a) for backup, business continuity, disaster recovery, and data interchange purposes as allowed and required under this Agreement, and (b) in all cases using Strong Encryption.

10.6 When providing Internet-based services to Subscriber, the Supplier shall protect Subscriber Data by ensuring that internal and external network segments are separated by security groups or similar cloud-based access control technology a) Supplier shall ensure that Network Access Control Lists (ACLs) restrict direct access to the Supplier infrastructure. b) Supplier shall ensure that there will be no direct access to application or data tier servers outside of the specific hosts or networks used by Supplier Hosting technical staff.

10.7 Ensure that inbound packets from an untrusted external network terminate within the DMZ and must not be allowed to flow directly through to the trusted internal network. All inbound packets, which flow to the trusted internal network, must only originate within the DMZ. Supplier shall also ensure security groups, access control lists, and other such technologies are configured to log and alert on malicious activities, unauthorized intrusion attempts, and policy violations.

10.8 Ensure that only the following are located within the trusted internal network:

(a) The official record copy of information to be accessed from requests originating from the untrusted external network,

(b) The official record copy of information to be modified as the result of requests originating from the untrusted external network,

(c) Database servers,

(d) All exported logs, and

(e) Development environments and source code.

10.9 Ensure that authentication credentials not protected by the use of Strong Encryption are not located within the DMZ.

11. **Identification and Authentication**.

11.1 In relation to access to Subscriber Data, either in electronic or hard copy, by the Supplier's team, the Supplier shall:

(a) Ensure such access is limited to a minimal set of authorized users.

(b) Assign unique User IDs to individual users.

(c) Have and use a documented User ID lifecycle management process including procedures for approved account creation, account removal immediately on termination or within 24 hours on role change, and account modification (e.g., changes to privileges, span of access, functions/roles) for all Information Resources and across all environments (e.g., production, test, development, etc.). Such process shall include review of access privileges and account validity to be performed at least quarterly.

(d) Enforce the rule of least privilege (i.e., limiting access to only the commands and Information Resources necessary to perform authorized functions according to one's job function).

(e) Limit failed login attempts to no more than five (5) successive attempts and lock the user account upon reaching that limit. Access to the user account can be reactivated subsequently through a manual process requiring verification of the user's identity or, where such capability exists.

(f) Terminate interactive sessions, or activate a secure, locking screensaver requiring authentication, after a period of inactivity not to exceed fifteen (15) minutes.

(g) Require password expiration at regular intervals not to exceed sixty (60) days.

(h) Use an authentication method based on the sensitivity of Subscriber Data.

(i) Whenever authentication credentials are stored, protect them using Strong Encryption.

(j) When passwords are used, ensure they are complex and at least meet the following password construction requirements:

(i) Be a minimum of eight (8) characters in length.

(ii) Contain characters from at least three (3) of these groupings: uppercase letter, lower case letter, numeric, and special characters.

(iii) Not be the same as the User ID with which they are associated.

(iv) Not contain repeating or sequential characters or numbers.

(k) Use a secure method for the conveyance of authentication credentials (e.g., passwords) and authentication mechanisms (e.g., tokens or smart cards).

11.2 Applications housing sensitive copies of Subscriber Data may require an authentication mechanism stronger than passwords. In such case, the authentication mechanism shall be mutually agreed to by the Parties in advance in writing. Examples of stronger authentication methods include tokens, one-time passwords and biometrics.

12. **Software and Data Integrity**. The Supplier shall:

12.1 Have current antivirus and personal firewall software installed and running to scan for and promptly remove or quarantine viruses and other malware. For the avoidance of doubt, this requirement also applies to Mobile and Portable Devices where antivirus software is commercially available. Updates to signatures on anti-virus servers and on individual systems must occur at a minimum, once every 24 hours.

12.2 Separate non-production Information Resources from production Information Resources.

12.3 Use only synthetic or de-identified data in development and test environments. If this is not possible, the Supplier must obtain Subscriber's written approval to use Subscriber Data and the Supplier warrants and undertakes that such environments have access controls as rigorous as those used in production.

12.4 Have a documented change control process including security impact review and back-out procedures for all production environments.

12.5 For applications which utilize a database that allows modifications to Subscriber Data, the Supplier shall have database transaction logging features enabled and retain database transaction logs for a minimum of twelve (12) months.

12.6 Review such software to find and remediate security vulnerabilities (static code analysis) prior to initial implementation and upon any modifications and updates for all software developed under an agreement with the Supplier.

12.7 Review such software to find and remediate security vulnerabilities (dynamic code analysis) prior to initial implementation and upon any modifications and updates, for all software used, furnished and/or supported under an agreement with the Supplier, where technically feasible.

12.8 Perform quality assurance testing for the security components (e.g., testing of identification, authentication and authorization functions), as well as any other activity designed to validate the security architecture, during initial implementation and upon any modifications and updates.

12.9 if the Supplier is developing an application for Subscriber, ensure that any solution it uses to process Subscriber Data is free of common web application security vulnerabilities as defined by, but not limited to, the OWASP top 10.

13. **Mobile and Portable Devices**. The Supplier shall:

13.1 Not use network aware Mobile and Portable Devices that are not laptop computers ("network aware devices") to access and/or store Subscriber Data, without Subscriber's express prior written approval.

13.2 Review, at least annually, the use of, and controls for, all Supplier-administered or -managed Mobile and Portable Devices to ensure that the Mobile and Portable Devices can meet the applicable Information Security Requirements.

14. **Security Gateways**. The Supplier shall:

14.1 Require Strong Authentication for administrative and/or management access to Security Gateways, including any access for the purpose of reviewing log files.

14.2 Have and use documented controls, policies, processes and procedures to ensure that unauthorized users do not have administrative and/or management access to Security Gateways, and that user authorization levels to administer and manage Security Gateways are appropriate.

14.3 At least once every six (6) months, ensure that Security Gateway configurations are hardened by selecting a sample of Security Gateways and verifying that each default rule set and set of configuration parameters are implemented, including:

(a) Internet Protocol (IP) source routing is disabled;

(b) The loopback address is prohibited from entering the internal network;

(c) Anti-spoofing filters are implemented;

(d) Broadcast packets are disallowed from entering the network;

(e) Internet Control Message Protocol (ICMP) redirects are disabled;

(f) All rule sets end with a "DENY ALL" statement; and

(g) Each rule is traceable to a specific business request.

14.4 Use monitoring tools to validate that all aspects of Security Gateways (e.g., hardware, firmware, and software) are continuously operational.

14.5 Configure and implement all Security Gateways such that all non-operational Security Gateways shall deny all access.

14.6 Configure real-time alerting for changes to the Security Gateway configuration and/or rule base.

15. **Connectivity Requirements**. In the event that Supplier has, or will be provided, connectivity to Subscriber's or Subscriber's customers' Nonpublic Information Resources, it shall:

15.1 Use only the mutually agreed upon facilities and connection methodologies to interconnect Subscriber's and Subscriber's customers' Nonpublic Information Resources with Supplier's Information Resources.

15.2 NOT establish interconnection to Subscriber's and Subscriber's customers' Nonpublic Information Resources without the prior written consent of Subscriber.

15.3 Provide Subscriber access to any applicable Supplier facilities during normal business hours for the maintenance and support of any equipment (e.g., router) provided by Subscriber for connectivity to Subscriber's and Subscriber's customers' Nonpublic Information Resources.

15.4 Use any equipment provided by Subscriber for connectivity to Subscriber's and Subscriber's customers' Nonpublic Information Resources only for the furnishing of those services or functions explicitly authorized by Subscriber.

15.5 If the agreed upon connectivity methodology requires that Supplier implement a Security Gateway, maintain logs of all sessions using such Security Gateway. These session logs must include sufficiently detailed information to identify the end user or application, origination IP address, destination IP address, ports/service protocols used and duration of access. These session logs must be retained for a minimum of twelve (12) months.

15.6 Permit Subscriber to gather information relating to access, including Supplier's access, to Subscriber's and Subscriber's customers' Nonpublic Information Resources. This information may be collected, retained and analyzed by Subscriber to identify potential security risks without further notice. This information may include trace files, statistics, network addresses, and the actual data or screens accessed or transferred.

15.7 Shall permit Subscriber to immediately suspend or terminate any interconnection to Subscriber and Subscriber's customers' Nonpublic Information Resources if Subscriber, in its sole discretion, believes there has been a Security Incident or unauthorized access to or misuse of Subscriber Data or Subscriber Information Resources.

16. **Vulnerability Scanning & Penetration Testing**. During the term of this Agreement or while Subscriber Data is processed by Supplier (whichever is later), the Supplier shall:

16.1 Use industry standard tools and manual techniques to assess the security of solution(s) provided by the Supplier and used in support of Subscriber employees, Subscriber suppliers, and/or Subscriber customers.

16.2 Perform at least quarterly, and immediately following all significant changes and upgrades, vulnerability scan externally and internally facing Information Resources, including networks, servers, applications and databases, with applicable industry-standard security vulnerability scanning software to uncover security vulnerabilities, ensure that such Information Resources are properly hardened.

16.3 Test, at least quarterly, to identify any unauthorized wireless networks.

16.4 Upon request, the Supplier will provide Subscriber a copy of the Vulnerability Scanning results, which shall be treated as Supplier Confidential Information unless disclosure is otherwise required by applicable law.

16.5 Have a third-party complete penetration testing at least annually and provide the results to Subscriber on request. In the event vulnerability findings are identified as a result of this testing, the Supplier shall provide, in a timely manner, sufficient technical personnel and support to fix the issues identified and to continue conducting further ethical hacks until Subscriber is assured that the identified incidents and their underlying causes have been cured.

17. **Logging**. The Supplier shall:

17.1 Log privileged accounts on all devices and applications.

17.2 Log record access (read), write, change, logon attempts, failed access attempts, changes to access controls lists, identifiers, or group/role privileges, updates to security software or the functionality of software and applications, and execution of any program that can bypass access controls.

17.3 Implement a real-time syslog server and restrict access to security logs to authorized individuals, and protect security logs from unauthorized modification and a centralized SIEM solution for monitoring security logs. If a SIEM solution is not available and Subscriber approves in writing, review, on no less than a weekly basis, all security and security-related audit logs for anomalies and document and resolve all logged security problems in a timely manner.

17.4 Retain all security and server logs for a period of one year (with 90 days available online) or as required to comply with regulatory requirements, whichever is greater. The log will record all logical access attempts both valid and invalid. The log will include the name (ID), data and time of the login, records accessed, and activity performed. If possible, the log will also have an entry for log-out.

18. **Wireless Networking**. If using wireless networking technologies to perform or support Services for Subscriber, the Supplier shall ensure that all Subscriber Data transmitted is protected by the use of appropriate encryption technologies sufficient to protect the confidentiality of Subscriber Data; provided, however, that in any event such encryption shall use no less than key lengths of 256-bits for symmetric encryption and 256-bits for asymmetric encryption. The use of RF-based wireless headsets, keyboards, microphones, and pointing devices, such as mice, touch pads, and digital drawing tablets, is excluded from this requirement.

19. **Subscriber Owned or Provided Devices**. The Supplier shall return all Subscriber-owned or -provided devices (including personal systems, tokens and/or software) as soon as practicable, but in no event more than fifteen (15) days after the sooner of: (a) expiration or Termination of this Agreement; (b) Subscriber's request for the return of such property; or (c) the date when the Supplier no longer needs such devices.

20. **Call Recording Data**. If the Supplier is processing Call Recording Data on behalf of Subscriber, then this paragraph shall apply to the Supplier:

20.1 Software Requirements for Collecting Call Recording Data:

(a) Software used for processing Call Recording Data must provide individual, authenticated accounts with an access audit trail.

(b) Software used for processing Call Recording Data must have the capability to turn recordings on or off.

20.2 Enablement of Supplier's Call Recording Capabilities:

(a) The Supplier shall not enable, activate, nor make operational any call recording capabilities for Call Recording Data collected and processed on behalf of Subscriber unless (1) requested by and (2) approved by Subscriber in writing.

(b) The percentage of Call Recording Data recorded by the Supplier must comply with the percentage allowed in writing by Subscriber. Specific permission must be obtained for 100% recording of Call Recording Data.

(c) If the Supplier intends to use Call Recording Data for the Supplier's internal training purposes, the Supplier shall use utilize technical mechanisms to redact all personal data and sensitive personal data from Call Recording Data.

20.3 Notice of Recording:

(a) Prior to recording Call Recording Data, the Supplier shall notify a party that the Supplier is about to record the conversation (a "**Recording Notice**").

(b) The Supplier shall ensure the Recording Notice:

(i) complies with all applicable laws and regulations.

(ii) includes the clear and specific purpose of the recording, such as for quality monitoring, workforce management, agent and customer service representative training, evaluation and verification, dispute resolution or accurate incident reconstruction.

(c) The Supplier shall implement a Recording Notice for both inbound recorded calls received by and outbound recorded calls made by Supplier.

20.4 Option Not to Record:

The Supplier's processes shall include the ability not to record inbound and outbound calls if so requested by the initiator of the call while still providing the requested service(s) to Subscriber.

20.5 Use and Access of Call Recording Data:

(a) Use of the Call Recording Data must be consistent with the Recording Notice.

(b) Call Recording Data must only be accessed by authorized users with accounts on the call recording system.

(c) Call Recording Data must not be shared through email or stored using other electronic distribution methods such as file shares unless otherwise authorized in writing by Subscriber.

20.6 Storage and Transmission of Call Recording Data:

(a) The Supplier shall protect filed or electronically stored Call Recording Data in accordance with this Agreement and applicable law.

(b) The Supplier shall encrypt sensitive personal data in storage and in transit.

20.7 Copies of Call Recording Data:

(a) The Supplier must have Subscriber's written authorization prior to making any copy, archival copy, or reproduction of Call Recording Data Processed on behalf of Subscriber.

(b) Copies, archival copies and reproductions of Call Recording Data are subject to the same access control and data protection requirements as the original Call Recording Data.

20.8 Call Recording Data Retention:

(a) The Supplier shall promptly delete Call Recording Data after the Supplier satisfies the specific purpose stated in the Recording Notice.

(b) The Supplier shall not retain Call Recording Data for no longer than the shorter of (i) the maximum period specified under applicable law; or (ii) sixty (60) calendar days after the original recording was made, unless otherwise authorized by Subscriber in writing.

20.9 Call Recording Data:

The Supplier shall comply with all applicable laws when processing Call Recording Data including applicable laws concerning Recording Notices, consent, transfers of Call Recording Data outside country borders and restrictions on types of information that may be received.

Annex A

Definitions

"**Demilitarized Zone**" or "**DMZ**" shall mean a network or sub-network that sits between a trusted internal network, such as a corporate private Local Area Network (LAN), and an untrusted external network, such as the public Internet. A DMZ helps prevent outside users from gaining direct access to internal Information Resources.

"**Call Recording Data**" shall mean any data that is recorded and/or stored relating to Subscriber employee and customer interaction voice calls including calls across transfers, holds, conference calls, inbound and outbound calls.

"**Industry Best Practice**" means processes and technology processes that form of practice reasonably expected of a leading supplier in the same or substantially similar sector seeking to comply with its regulatory and contractual responsibilities."

"**Information Resource(s)**" means systems, applications, networks, network elements, and other computing and information storage devices, including smart phones, tablets, and USB memory sticks.

"**Mobile and Portable Devices**" means mobile and/or portable computers, devices, media and systems capable of being easily carried, moved, transported or conveyed. Examples of such devices include laptop computers, tablets, USB hard drives, USB memory sticks, Personal Digital Assistants (PDAs), and wireless phones, such as smartphones.

"**Nonpublic Information Resources**" means those Information Resources to which access is restricted and cannot be gained without proper authorization and identification.

"**Security Gateway**" shall mean a set of control mechanisms between two or more networks having different trust levels which filter and log traffic passing, or attempting to pass, between networks, and the associated administrative and management servers. Examples of Security Gateways include firewalls, firewall management servers, hop boxes, session border controllers, proxy servers, and intrusion prevention devices.

"**Strong Authentication**" means the use of authentication mechanisms and authentication methodologies stronger than the passwords required under the Requirements. Examples of Strong Authentication mechanisms and methodologies include digital certificates, two-factor authentication, and one-time passwords.

"**Strong Encryption**" means the use of encryption technologies with minimum key lengths of 256-bit for symmetric encryption and 1024-bits for asymmetric encryption whose strength provides reasonable assurance that it will protect the encrypted information from unauthorized access and is adequate to protect the confidentiality and privacy of the encrypted information, and which incorporates a documented policy for the management of the encryption keys and associated processes adequate to protect the confidentiality and privacy of the keys and passwords used as inputs to the encryption algorithm.

EXHIBIT 3 – PCI COMPLIANCE EXHIBIT

Whereas Subscriber is required to adhere to the Payment Card Industry Data Security Standard (PCI DSS) promulgated by the PCI Security Standards Council; and

Whereas Supplier processes, transmits, and/or stores cardholder data in the performance of services provided to Subscriber, and is therefore considered a "service provider" under Requirement 12.8 of the PCI DSS; and

Whereas Requirement 12.8.2 of the PCI DSS requires Subscriber to maintain a written agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data that the service provider possesses; and

Whereas Requirement 12.8.4 of the PCI DSS requires Subscriber to maintain a program to monitor the service provider's PCI DSS compliance status,

1. Supplier agrees that it is responsible for the security of cardholder data and sensitive authentication data (as defined in PCI DSS) that it possesses, including the functions relating to storing, processing, and transmitting of the cardholder data.

2. Supplier affirms that, as of the effective date of this Agreement, it has complied with all applicable requirements to be considered PCI DSS compliant, and has performed the necessary steps to validate its compliance with the PCI DSS.

3. Supplier agrees to supply to Subscriber the current status of Supplier's PCI DSS compliance status, and evidence of its most recent validation of compliance, upon execution of this Agreement. Supplier must supply to Subscriber a new status report and evidence of validation of compliance at least annually.

4. Supplier will immediately notify Subscriber if it learns that it is no longer PCI DSS compliant and will immediately provide Subscriber the steps being taken to remediate the non-compliance status. In no event should Supplier's notification to Subscriber be later than seven (7) calendar days after Supplier learns it is no longer PCI DSS complaint.

5. Supplier acknowledges that any indemnification provided for under this Agreement applies to the failure of the Supplier to be and to remain PCI DSS compliant.

6. Supplier represents and warrants that for the life of this Agreement, the software and services used for processing transactions shall be compliant with standards established by the PCI Security Standards Council (https://www.pcisecuritystandards.org/index.shtml), as amended from time to time. Supplier agrees to indemnify and hold Subscriber, its officers, employees, and agents, harmless for, from and against any and all claims, causes of action, suits, judgments, assessments, costs (including reasonable attorneys' fees) and expenses arising out of or relating to any loss of Subscriber customer credit card or personally identifiable information managed, retained or maintained by Supplier, including but not limited to fraudulent or unapproved use of such credit card or identity information.

EXHIBIT 4 – BUSINESS ASSOCIATE AGREEMENT

We do not keep HIPAA related information.

EU Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Subscriber (as data exporter) and Service Provider (as data importer), each a "party," together "the parties," have agreed on the following Contractual Clauses (the "Clauses" or "Standard Contractual 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.

Name of the data exporting organization: ("Subscriber")

Customer Name:

E-mail:

Other information needed to identify the organization:

And

Name of the data importing organization: EnterpriseJungle, Inc. ("Service Provider")

Address: 8749 Holloway Dr. West Hollywood, CA 90069

Tel.: (323) 251-2667 E-mail: j@EnterpriseAlumni.com

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.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) *'the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organizational security measures'* means those measures aimed at 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.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect 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, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(ii) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
(iii) any accidental or unauthorized access, and

(iv) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

2 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the

data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

(a) The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

(b) The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

(c) The data importer shall promptly inform the data exporter about the existence of legislation

applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

(a) The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

(b) The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

(c) The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

(d) The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

---

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter:

Subscriber Shared Services

Name:

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature: _____

(stamp of organization)

On behalf of the data importer:

EnterpriseJungle, Inc.

Name: James Sinclair

Position: Principal

Address: 8749 Holloway Dr. West Hollywood, CA 90069

Other information necessary in order for the contract to be binding (if any):

Signature: DocuSigned by: James Sinclair D60B9A61EF2B449...

(stamp of organization)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the Parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

Data exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and that have purchased Services and transfers personal data to data importer on the basis of the Agreement.

Data importer

Service Provider's Solution, *EnterpriseJungle*, is a fully integrated platform to manage, engage and create an alumni network to increase talent pools, accelerate resource planning and reduce internal costs of recruitment. Service Provider's Services involves the processing personal data provided by, and pursuant to the requests of, the data exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects:

- Employees of data exporter (who are natural persons)
- Data exporter's Users authorized by data exporter to use the Services

Categories of data

The personal data transferred concern the following categories of data:

- Former Employer's Name
- Former Employee's previous number

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

EnterpriseJungle does not reveal any special categories of data.

Processing operations

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

Signing the Standard Contractual Clauses, Appendix 1 on behalf of:

DATA EXPORTER:

Subscriber

By: _____

Name: _____

Title: _____

Date: _____

DATA IMPORTER:

EnterpriseJungle, Inc.

By: DocuSigned by: James Sinclair D60B9A61EF2B449...

Printed Name: James Sinclair

Title: Principal

APPENDIX 2 - DESCRIPTION OF THE TRANSFER

This Appendix forms part of the Clauses and must be completed and signed by the parties Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. Personnel. Data Importer personnel will not process Customer Data without authorization. Personnel are obligated to maintain the confidentiality of any Customer Data and this obligation continues even after their engagement ends.

2. Data Privacy Contact. The data privacy officer of the Data Importer can be reached at the following address: 8749 Holloway Dr. West Hollywood, CA 90069, Attn: Chief Privacy Officer.

3. Technical and Organizational Measures. The Data Importer has implemented and will maintain appropriate technical and organizational measures, internal controls, physical and technical safeguards, and information security routines to protect the Customer Data, as defined in the Agreement, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth in the Agreement are hereby incorporated into this Appendix 2 by this reference and are binding on the Data Importer as if they were set forth in this Appendix 2 in their entirety.