## ANNEX

### Standard Contractual Clauses (processors)

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

Name of the data exporting organisation:.....

Address:.....

Tel.:.....; fax:..... ; e-mail: .....

Other information needed to identify the organisation

.....

(the data **exporter**)

And

Name of the data importing organisation: Korn Ferry, on behalf of itself and its affiliates

Address: 1900 Avenue of the Stars, Suite 2600, Los Angeles, CA 90067, U.S.A.

Tel.: +1-310-552-1834; fax: +1-310-553-6452; e-mail: privacy@kornferry.com

Other information needed to identify the organisation:

N/A

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

*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 organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

---

[1] 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 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.

*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 organisational 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, unauthorised 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).

***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 organisational security measures specified in Appendix 2 before processing the personal data transferred;

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

(i) 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,

(ii) any accidental or unauthorised access, and

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

(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

---

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, defence, 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 recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

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***

1. 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.

2. 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.

3. 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***

1. 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.

2. 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.

3. 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.

4. 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.

---

[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.

*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.

**On behalf of the data exporter:**

Name (written out in full):

Position:

Address:

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

Signature.....

(stamp of organisation)

**On behalf of the data importer:**

Name (written out in full): Jonathan M. Kuai

Position: General Counsel and Co-Chief Privacy Officer

Address: 1900 Avenue of the Stars, Suite 2600, Los Angeles, CA, 90067, U.S.A.

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

Signature.....

(stamp of organisation)

## 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**

The data exporter is (please specify briefly your activities relevant to the transfer):

.....
.....
.....

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

Korn Ferry, incorporated in Delaware, USA, is a global executive search, recruitment, remuneration, talent management and management consulting firm providing leadership and talent management solutions, recruitment solutions, recruitment process outsourcing project recruitment, search, sales training and consulting services, work measurement and consulting services to its clients worldwide, as well as online software and other tools for use by licensees in the evaluation of their employees.

**Data subjects**

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

(1) Job candidates (e.g., prospective personnel), of the Data Exporter;

(2) Job seekers, individuals who wish to be considered for positions within Data Exporter's organization;

(3) Employees or other personnel of Data Exporter;

(4) Data Exporter-nominated participants in Data Importer's assessment processes and consulting services; and

(5) individuals providing feedback with respect to such Data Exporter employees, at the request of Data Exporter.

**Categories of data**

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

For Data Exporter's assessment participants: Names, e-mail addresses, business address, phone numbers, job titles, demographic data, roles, and relationship to person receiving feedback (e.g. manager, subordinate, colleague, customer, and other) of such employees and individuals, responses to surveys, evaluation data (answers to questionnaires, inventories and tests,

performance on job-related simulations, information obtained from others about data subjects, and information obtained from the observations and conclusions of staff and contractors involved in the assignment), login and passwords to data importer's website(s).

For Data Exporter's job candidates and job seekers in the context of recruitment process outsourcing services: Name, gender, job source, job field (job family), job type (full time/part time), job location, prior employment, educational background, professional qualifications, credentials and certifications, memberships of professional organizations, language or other skills, business address, home address, telephone number, email address, source (e.g. Direct, Job Aggregator, etc.), candidate type (internal, external), candidate current employer, candidate current job title, function (e.g. Corporate Affairs, Engineering/Scientific, etc.), compensation, citizenship, work authorization status, national identification number, interest level, professional goals, hiring manager name, details contained in letters of application, resumes and CVs, information from employers or other references, photographs, login and passwords to data importer's website(s).

For Data Exporter employees or other personnel: Name, email address, business address, phone number, position (job title, employee ID, hire date, unit/department/location, supervisor(s) and subordinate(s)).

Information required to access the online services, including SaaS applications, such as login and password, instant messaging account, answers to security questions; access logs, activity logs; asset identifiers; network logging data; software usage and pattern tracking information; and electronic content produced by data subjects using systems, including online interactive and voice communications such as blogs, chat, webcam use and network sessions.

For mobile reinforcement application or eLearning, technical/device information (IP address, device brand and model, operating system and version, browser brand and version); and training history and results (training completion, training score).

For the Alliance subscription platform, name, email, job title, pages clicked, files downloaded, virtual Instructor Led Training (vILT) sessions registered, and for support, device and connection information such as IP address and API token when service is used.

For digital learning environments, profile information provided by subscribers and learners, the recording of learning activities, progress towards completion of learning plans, and completion of required tasks and certifications.

**Special categories of data (if appropriate)**

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

- Information on race and ethnic origin, sexual orientation, disability and veteran status may be transferred, if requested by Data Exporter, to assist the Data Exporter in meeting its diversity goals.

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

The Data Importer will collect data from the Data Exporter at the Data Exporter's direction. The data may be collected from Data Exporter platforms, such as: recruitment marketing, applicant tracking system, customer relationship management database, customer satisfaction and human resources information systems, and performance management metrics. Data Importer may also process personal data to enable the delivery of sales and/or customer experience training and consulting, and related services.

In the context of recruitment process outsourcing services, the Data Importer may process that data to provide recruitment services and up-to-date recruitment metrics regarding the prospective personnel, which will enable the Data Exporter to analyze such data for recruitment purposes. If requested by Data Exporter, Data Importer may sort data by different categories and compare the data against information on the total number of candidates, number of applications, submissions for a position, interviews, offers and acceptances, number and length of openings, filled, on-hold or cancelled positions, and others.

Personal data will be processed for communication and analysis purposes, including generating emails to assessment participants, rated and rating persons, association and collation of the information and responses from a survey or assessment into a report, and validating assessments. The Data Importer may produce group reports for the Data Exporter, enabling a comparison of the participants' results with company-specific norms rather than general norms, prepare normative statistics, and disseminate statistical information for research purposes and support ongoing research programmes by the Data Importer (e.g., on differences in managerial competence among countries, organisational levels, etc.).

Notwithstanding anything contained in this Appendix 1, the Clauses do not apply where the parties process Personal Data as independent data controllers, or equivalent, under applicable data protection law, nor do these terms apply to information provided by Korn Ferry regarding candidates in connection with an executive or professional search.

DATA EXPORTER

Name:.....

Authorised Signature .....

DATA IMPORTER

Name: Jonathan M. Kuai

Authorised Signature .....

## APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

**Korn Ferry**
**Security Practices**

Korn Ferry maintains and enforces various policies, standards and processes designed to secure confidential data, including personal information. Following is a description of some of the core technical and organisational security measures implemented by Korn Ferry.

### 1. Information Security Policies and Standards

Korn Ferry implements security requirements for staff and all subcontractors, vendors, or agents who have access to personal information. These are designed to:

- Prevent unauthorized persons from gaining access to personal information processing systems (physical access control);
- Prevent personal information processing systems from being used without authorization (logical access control);
- Ensure that persons entitled to use a personal information processing system gain access only to such personal information as they are entitled to access in accordance with their access rights and that, in the course of processing or use and after storage, personal information cannot be read, copied, modified or deleted without authorization (data access control);
- Ensure that personal information cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the target entities for any transfer of personal information by means of data transmission facilities can be established and verified (data transfer control);
- Ensure the establishment of an audit trail to document whether and by whom personal information have been entered into, modified in, or removed from personal information processing (entry control);
- Ensure that personal information is processed solely as instructed (control of instructions);
- Ensure that personal information is protected against accidental destruction or loss (availability control); and
- Ensure that personal information collected for different purposes can be processed separately (separation control).

These security requirements are kept up to date, and revised at least annually or whenever relevant changes are made to the information system that uses or houses personal information, or to how that system is organized.

### 2. Physical Security

Korn Ferry maintains commercially reasonable security systems at all its sites at which an information system that uses or houses personal information is located. Korn Ferry reasonably restricts access to such personal information appropriately.

**3. Organizational Security**

When media are to be disposed of or reused, procedures have been implemented to prevent any subsequent retrieval of any personal information stored on them before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures have been implemented to prevent undue retrieval of personal information stored on them.

All security incidents involving personal information are managed in accordance with appropriate incident response procedures.

**4. Network Security**

Korn Ferry maintains network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection and/or prevention systems, access control lists and routing protocols.

**5. Access Control**

Only authorized staff can grant, modify or revoke access to an information system that uses or houses personal information.

User administration procedures define user roles and their privileges, how access is granted, changed and terminated; addresses appropriate segregation of duties; and defines the logging/monitoring requirements and mechanisms.

All employees of Korn Ferry are assigned unique User-IDs.

Access rights are implemented adhering to the "least privilege" approach.

Korn Ferry implements commercially reasonable physical and electronic security to create and protect passwords.

***6. Virus and Malware Controls***

Korn Ferry installs and maintains anti-virus and malware protection software on the system.

**7. Personnel**

Korn Ferry personnel are required to read, sign, and abide by Korn Ferry's Code of Business Conduct, IT Security Policy, and Confidential Information Policy as a condition of employment. Personnel are subject to disciplinary measures for violations of these policies. New employees undergo background checks, which may include reference checks, education verification and criminal background checks, where allowed by applicable law and in accordance with local practices. In addition, Korn Ferry implements a security awareness program to train personnel about their security and privacy obligations. This program includes training about data privacy and security practices; physical security controls; and security incident reporting.

**8. Business Continuity**

Korn Ferry implements appropriate disaster recovery and business resumption plans.