Data Processing Addendum

This Data Processing Addendum ("**Addendum**") is incorporated into and forms part of the Subscription Agreement ("**Subscription Agreement**") between the applicable iCIMS contracting entity under the Subscription Agreement ("**iCIMS**") and the entity that executed the Subscription Agreement and/or Order Form ("**Subscriber**") acting on its own behalf and as agent for each Subscriber Affiliate.

About this Addendum:

1. This Addendum consists of four parts: the main body of the Addendum, Appendix 1, Appendix 2, and Appendix 3 (including Annexes 1 and 2). Appendix 3 shall only be applicable to the extent required by Data Protection & Privacy Laws.
2. If the Standard Contractual Clauses in Appendix 3 are applicable, the Subscriber's signature of the Subscription Agreement and/or applicable Order Form(s) shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Annexes. Please note that the contracting entity under the Subscription Agreement and/or Order Form may be an iCIMS Affiliate.
3. Subscriber must review Appendices 1 and 2, as well as Annexes 1 and 2 of Appendix 3, for accuracy and completeness.

iCIMS acknowledges that Subscriber and each Subscriber Affiliate is/are Controller(s) in relation to the Personal Data under their respective control as the legal person competent to determine purposes and methods of the Processing of the Personal Data and the relevant means, including the adequacy of the security measures. Subscriber hereby appoints iCIMS as a Processor to Process Subscriber Personal Data as described in the Subscription Agreement and Appendix 1 which further details the subject-matter, type, and purpose of Processing, the types of data, and categories of Data Subjects. iCIMS accepts the appointment and undertakes to duly fulfil the obligations set forth in this Addendum. Subscriber shall serve as a single point of contact for iCIMS with regards to any notification or information to be given to either Subscriber or any Subscriber Affiliate under this Addendum and is responsible for the internal coordination, review and submission of instructions or requests of Subscriber Affiliates to iCIMS.

Unless otherwise defined below, all capitalized terms have the meaning given to them in the Subscription Agreement and/or exhibits thereto. Any examples in this Addendum are illustrative and not the sole examples of a particular concept.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Subscription Agreement. Except where the context requires otherwise, references in this Addendum to the Subscription Agreement are to the Subscription Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 **"Business"** has the meaning assigned to it in the CCPA (as defined below);

1.1.2 **"Business Purpose"** has the meaning assigned to it in the CCPA (as defined below);

1.1.3 "**California Consumer Privacy Act of 2018**" or "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations;

1.1.4 "**Contracted Processor**" means iCIMS or one of its Subprocessors;

1.1.5 "**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Subscriber Personal Data;

1.1.6 "**Data Protection & Privacy Laws**" means all data protection and privacy laws applicable to the Processing of Personal Data under this Addendum, including local, state (e.g., the CCPA), national and/or foreign laws, treaties, and/or regulations, the GDPR (as defined below), and implementations of the GDPR into national law, as each may be amended from time to time;

1.1.7 "**Data Subject**" means an identified or identifiable natural person whose rights are protected by Data Protection & Privacy Laws, including, but not limited to, a "Consumer" as defined in the CCPA;

1.1.8 "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, including as implemented or adopted under the laws of the United Kingdom. Where applicable, references to the "GDPR" include "Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the Processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC;

1.1.9 "**iCIMS Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with iCIMS, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.10 **"Personal Data"** means any information relating to a Data Subject, including, but not limited to, "Personal Information" as defined in the CCPA;

1.1.11 **"Personal Data Breach"** means (i) a "personal data breach," as defined in the GDPR, affecting Subscriber Personal Data and (ii) any "Data Breach," as defined in iCIMS' Incident Response Procedures that may be accessed at https://www.icims.com/gc/, affecting Subscriber Personal Data;

1.1.12 **"Process"** and **"Processing"** mean any operation or set of operations performed on Subscriber Personal Data or sets of Subscriber Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing, or destroying;

1.1.13 **"Processor"** means the entity which Processes Subscriber Personal Data on behalf of the Controller;

1.1.14 "**Restricted Transfer"** means:

1.1.14.1 a transfer of Subscriber Personal Data from any Subscriber Group Member to a Contracted Processor; or

1.1.14.2 an onward transfer of Subscriber Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor;

in each case, where such transfer would be prohibited by Data Protection & Privacy Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection & Privacy Laws) in the absence of appropriate safeguards such as the Standard Contractual

Clauses to be established under Section 6.4.3 or Section 13. For the avoidance of doubt, where a transfer of Subscriber Personal Data is of a type authorized by Data Protection & Privacy Laws in the exporting country, such transfer shall not be a Restricted Transfer;

1.1.15 **"Sell"** has the meaning assigned to it in the CCPA;

1.1.16 **"Service Provider"** has the meaning assigned to it in the CCPA;

1.1.17 **"Standard Contractual Clauses"** means the clauses set forth, or incorporated by reference, in Appendix 3;

1.1.18 "**Subprocessor**" means any entity engaged by iCIMS, including any iCIMS Affiliate, to Process Subscriber Personal Data on behalf of any Subscriber Group Member in connection with the Subscription Agreement, including, but not limited to, "Service Provider" as defined in the CCPA;

1.1.19 "**Subscriber Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Subscriber, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.20 "**Subscriber Group Member**" means Subscriber or any Subscriber Affiliate;

1.1.21 "**Subscriber Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Subscriber Group Member pursuant to or in connection with the Subscription Agreement;

1.1.22 "**Supervisory Authority**" means, as applicable, an appointed government entity with the authority to enforce Data Protection & Privacy Laws, such as a supervisory authority as defined in the GDPR or "Commissioner" as defined under Swiss member state law and/or the UK GDPR; and

1.1.23 "**UK GDPR**" means, collectively, the United Kingdom ("**UK**") General Data Protection Regulation and amended Data Protection Act 2018, in each case as may be amended or superseded from time to time.

1.2 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Roles & Scope

2.1 This Addendum applies to the Processing of Subscriber Personal Data by iCIMS to provide the Subscription. For the purposes of this Addendum, Subscriber and Subscriber Affiliates are the Controller(s) and iCIMS is the Data Processor and/or Service Provider (to the extent that iCIMS Processes Personal Data for a Business Purpose under the Subscription Agreement).

2.2 For the avoidance of doubt, iCIMS is not responsible for complying with data protection and privacy laws applicable to Subscriber or Subscriber's industry that are not applicable to the Subscription, such as those not generally applicable to online service providers.

3. Processing of Subscriber Personal Data

3.1 iCIMS and each iCIMS Affiliate shall:

3.1.1 comply with Data Protection & Privacy Laws in the Processing of Subscriber Personal Data;

3.1.2 be prohibited from: (i) Selling Subscriber Personal Data; (ii) retaining, using, or disclosing the Subscriber Personal Data for a commercial purpose other than providing the Subscription and related services under the Subscription Agreement; and (iii) retaining, using, or disclosing the Subscriber Personal Data outside of the direct business relationship between iCIMS and Subscriber;

3.1.3 Process Subscriber Personal Data only on the relevant Subscriber Group Member's documented instructions for the following purpose:

3.1.3.1 Processing in accordance with the Subscription Agreement and applicable Order Form(s);

3.1.3.2 Processing initiated by Candidates and Users in their use of the Subscription; and

3.1.3.3 Processing to render Subscriber Personal Data anonymous, de-identified, and non-personal;

3.1.3.4 Processing to comply with other documented reasonable instructions provided by Subscriber (e.g., via email);

where such instructions are consistent with the terms of the Subscription Agreement, unless Processing is required by Data Protection & Privacy Laws to which the relevant Contracted Processor is subject, in which case iCIMS or the relevant iCIMS Affiliate shall to the extent permitted by Data Protection & Privacy Laws inform the relevant Subscriber Group Member of that legal requirement before the relevant Processing of that Subscriber Personal Data. For the avoidance of doubt, an instruction, approval, request or similar action given via the Subscription, including Subscriber's configuration of any settings or options in the Subscription (as Subscriber may be able to modify from time to time), is considered a Subscriber's Processing instruction. The parties agree that for the purpose of the Standard Contractual Clauses, the Processing of Subscriber Personal Data by iCIMS is deemed to be in compliance with Subscriber's instructions if expressly authorized by the Subscription Agreement; and

3.1.4 immediately inform the Subscriber if, in its opinion, an instruction from Subscriber infringes Data Protection & Privacy Laws.

3.2 Each Subscriber Group Member:

3.2.1 Instructs, subject to section 3.1, iCIMS and each iCIMS Affiliate (and authorizes iCIMS and each iCIMS Affiliate to instruct each Subprocessor) to:

3.2.1.1 Process Subscriber Personal Data; and

3.2.1.2 in particular, transfer Subscriber Personal Data to any country or territory permitted by Subscriber, which, for the avoidance of doubt, includes (i) the location(s) of the iCIMS data center(s) identified in this Addendum and/or the Subscription Agreement and applicable Order Form(s), and (ii) the locations of Processing by the Subprocessors identified in this Addendum and/or the Standard Contractual Clauses,

as reasonably necessary for the provision of the Subscription and consistent with the Subscription Agreement; and

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in section 3.2.1 on behalf of each relevant Subscriber Affiliate.

3.3 Appendix 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Subscriber Personal Data as required by Article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection & Privacy Laws). By itself, nothing in Appendix 1 confers any additional right or imposes any additional obligation on any party to this Addendum.

4. iCIMS and iCIMS Affiliate Personnel

iCIMS and each iCIMS Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Subscriber Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Subscriber Personal Data, as strictly necessary for the purposes of the Subscription Agreement, and to comply with Data Protection & Privacy Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, iCIMS and each iCIMS Affiliate shall in relation to the Subscriber Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR or as otherwise contained in Data Protection & Privacy Laws and the measures set forth in the Subscriber Data Security Addendum attached as Appendix 2. iCIMS may update Appendix 2 from time to time as provided in the Subscription Agreement, provided however, iCIMS shall not make changes to Appendix 2 that materially diminish the protections for Subscriber Data set forth therein.

5.2 In assessing the appropriate level of security, iCIMS and each iCIMS Affiliate shall take account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed.

6. Subprocessing

6.1 Each Subscriber Group Member authorizes iCIMS and each iCIMS Affiliate to appoint (and permit each Subprocessor appointed in accordance with this Section 6 to appoint) Subprocessors in accordance with this Section 6 and any restrictions in the Subscription Agreement.

6.2 iCIMS and each iCIMS Affiliate may continue to use those Subprocessors already engaged by iCIMS or any iCIMS Affiliate as at the date of this Addendum, subject to iCIMS and each iCIMS Affiliate in each case as soon as practicable meeting the obligations set out in Section 6.4. The list of Subprocessors used to provide the Subscription and their country or location of Processing may be accessed at https://icims.help/GDPR-subprocessors. iCIMS provides a mechanism which may be accessed at https://www.icims.com/gc for Subscriber to subscribe to receive email notice when iCIMS intends to add or replace a Subprocessor, and if Subscriber subscribes, iCIMS shall provide notification to Subscriber of such changes.

6.3 Subscriber may object to iCIMS' proposed Subprocessor changes by notifying iCIMS within thirty (30) days of iCIMS' notice in accordance with the mechanism set forth in Section 6.2 (the "**Objection Period**") if Subscriber reasonably determines such Subprocessor is unable to Process Subscriber Personal Data in accordance with the

terms of this Addendum. If iCIMS receives a Subprocessor objection notice from Subscriber within the Objection Period:

6.3.1 iCIMS shall work with Subscriber in good faith to make available a reasonable change in the provision of the Subscription or recommend a reasonable change to Subscriber's configuration or use of the Subscription which avoids the use of the proposed Subprocessor; and

where such a change cannot be made within thirty (30) days from iCIMS' receipt of Subscriber's objection notice, notwithstanding anything in the Subscription Agreement, Subscriber may by written notice to iCIMS, with immediate effect, terminate the applicable Order Form(s) with respect only to those Subscriptions (i.e., product offering, portal, module, line item) which cannot be provided by iCIMS without the use of the objected-to new Subprocessor (the "**Terminated Service Portion**"). iCIMS will refund to Subscriber any prepaid fees covering the remainder of the Subscription Period for the Terminated Service Portion following the effective date of termination with respect to such Terminated Service Portion, without imposing a penalty for such termination on Subscriber.

6.4 With respect to each Subprocessor, iCIMS or the relevant iCIMS Affiliate shall:

6.4.1 before the Subprocessor first Processes Subscriber Personal Data (or, where relevant, in accordance with Section 6.2), carry out due diligence to ensure that the Subprocessor is capable of providing the level of protection for Subscriber Personal Data required by the Subscription Agreement;

6.4.2 ensure that the arrangement between on the one hand (a) iCIMS, or (b) the relevant iCIMS Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand, the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Subscriber Personal Data as those set out in this Addendum and meet the requirements of Data Protection & Privacy Laws, which include, but are not limited to, Article 28(3) of the GDPR; and

6.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) iCIMS, or (b) the relevant iCIMS Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand, the Subprocessor.

6.5 iCIMS shall be liable for the acts and omissions of its Subprocessors to the same extent iCIMS would be liable if performing the services of each Subprocessor directly under the terms of this Addendum.

6.6 The parties agree that any copy of a Subprocessor agreement that iCIMS must provide to Subscriber pursuant to the Standard Contractual Clauses may have all commercial, proprietary, and confidential information, and clauses unrelated to this Addendum and the Standard Contractual Clauses, removed or redacted by iCIMS beforehand; and, that such copy will be provided by iCIMS, in a manner mutually agreed upon by the parties, only upon request by Subscriber.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing and the information available to iCIMS as a Processor, iCIMS and each iCIMS Affiliate shall assist each Subscriber Group Member by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Subscriber Group Members' obligations to respond to requests to exercise Data Subject rights under Data Protection & Privacy Laws. To the extent legally permitted, Subscriber shall be responsible for any costs arising from iCIMS' provision of such

assistance that is beyond the scope of such technical and organizational measures and standard assistance provided iCIMS in the ordinary course of business.

7.2 iCIMS will, at its election and as necessary to enable Subscriber to meet its obligations under Data Protection & Privacy Laws, either (i) provide Subscriber the ability within the Subscription to correct or delete Subscriber Personal Data or restrict its Processing; or (ii) make such corrections, deletions, or restrictions on Subscriber's behalf if such functionality is not available within the Subscription. To the extent any Subscriber Personal Data of a Data Subject is not accessible to Subscriber through the Subscription, iCIMS will, as necessary to enable Subscriber to meet its obligations under Data Protection & Privacy Laws, provide reasonable assistance to make such Subscriber Personal Data available to Subscriber.

7.3 During the term of the Subscription Agreement, Subscriber may extract Subscriber Personal Data from the Subscription in accordance with the Documentation and the relevant provisions of the Subscription Agreement, including so that Subscriber can provide the Personal Data to a Data Subject who makes an applicable Data Subject Request (as defined below) for such Personal Data.

7.4 For the avoidance of doubt, Subscriber is responsible for responding to and complying with a Data Subject's request to exercise their rights under Data Protection & Privacy Laws regarding their Personal Data in the Subscription ("**Data Subject Request**"). The Subscription includes controls that Subscriber may use to assist Subscriber with responding to a Data Subject Request. If Subscriber is unable to use the controls within the Subscription to assist Subscriber with responding to the Data Subject Request, iCIMS will reasonably cooperate with Subscriber to enable Subscriber to respond to the Data Subject Request. If iCIMS directly receives a Data Subject Request outside of the Subscription that specifically names Subscriber, iCIMS will promptly redirect the Data Subject to submit its request to Subscriber, promptly notify Subscriber of such request, and not otherwise respond to such request unless expressly authorized by Subscriber.

8. Personal Data Breach

8.1 In accordance with iCIMS' documented incident response policies and procedures, iCIMS shall notify Subscriber without undue delay and in any event within 24 hours of iCIMS becoming aware of a Personal Data Breach affecting Subscriber Personal Data, providing Subscriber with at least the following information (to the extent such information is known or available to iCIMS): (i) a description of the nature of the Personal Data Breach, the categories and approximate number of Data Subjects and Personal Data records concerned, (ii) name and contact details of a contact person at iCIMS for further information, (iii) a description of the likely consequences of the Personal Data Breach, and (iv) a description of the measures taken or proposed to be taken for the remedy or mitigation of the Personal Data Breach. When it is not possible to provide such information at the same time, the information may be provided in phases without undue further delay. iCIMS will promptly take all measures and actions that are reasonably necessary to remedy or mitigate the effects of the Personal Data Breach and shall keep Subscriber informed of all developments in connection with the Personal Data Breach to allow Subscriber and each Subscriber Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under Data Protection & Privacy Laws.

8.2 iCIMS shall co-operate with Subscriber and each Subscriber Group Member and take such reasonable steps as are directed by Subscriber to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

8.3 Subscriber shall notify iCIMS promptly after becoming aware of any misuse of Subscriber's accounts or authentication credentials or any Personal Data Breach related to the Subscription.

8.4 Neither party's notification of or response to a Personal Data Breach under this Section 8 is an acknowledgment by such party of any fault or liability with respect to the Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

iCIMS and each iCIMS Affiliate shall, to the extent Subscriber does not otherwise have access to the relevant information, and to the extent it is available to iCIMS, provide reasonable assistance to each Subscriber Group Member with any data protection impact assessments or like assessments (e.g., privacy impact assessment), and prior consultations with Supervising Authorities or other competent data privacy authorities, which Subscriber reasonably considers to be required of any Subscriber Group Member by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection & Privacy Law, in each case solely in relation to Processing of Subscriber Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors. To the extent legally permitted, Subscriber shall be responsible for any costs arising from iCIMS' provision of such assistance that is beyond the scope of standard assistance provided by iCIMS in the ordinary course of business.

10. Deletion or Return of Subscriber Personal Data

10.1 Subject to Sections 10.2 and 10.3, iCIMS and each iCIMS Affiliate shall promptly and in any event within thirty (30) days of Subscriber's written request or the date of cessation of any Subscription involving the Processing of Subscriber Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Subscriber Personal Data, in accordance with iCIMS' documented data storage and retention policies and procedures.

10.2 Subject to Section 10.3, Subscriber may, in its absolute discretion, by written notice to iCIMS and within ten (10) days of the Cessation Date, request that iCIMS and each iCIMS Affiliate return a complete copy of all Subscriber Personal Data to Subscriber in a format and method as set forth in the Subscription Agreement.

10.3 Each Contracted Processor may retain Subscriber Personal Data (i) to the extent required by Data Protection & Privacy Laws and only to the extent and for such period as required by Data Protection & Privacy Laws, and/or (ii) on its backup media and backup servers until such time as the backup copies are scheduled to be deleted (not to exceed one (1) year from the Cessation Date or deletion request, as applicable); provided, however, that iCIMS and each Contracted Processor shall ensure the confidentiality of all such Subscriber Personal Data and shall ensure that such Subscriber Personal Data is not Processed in violation of Data Protection & Privacy Laws.

10.4 After the Cessation Date, upon the written request of Subscriber, iCIMS shall provide written certification, within thirty (30) days of receiving the request, that it has deleted and/or returned all copies of Subscriber Personal Data governed by Data Protection & Privacy Laws in accordance with iCIMS' documented data storage and retention policies and procedures. The parties agree that for the purpose of the Standard Contractual Clauses, iCIMS is required to provide certification of deletion of Subscriber Personal Data only upon the written request by Subscriber.

11. Assistance

iCIMS shall not undertake any task that according to Data Protection & Privacy Laws is assigned to be performed by the Subscriber, in their capacity as Data Controller.

12. Audit Rights

12.1 If a Supervisory Authority requires an audit of the facilities from which iCIMS Processes Subscriber Personal Data in order to ascertain or monitor Subscriber's compliance with Data Protection & Privacy Laws, iCIMS will

reasonably cooperate with such audit. Subscriber is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time iCIMS expends for any such audit, in addition to the rates for services performed by iCIMS.

12.2 Subscriber agrees that iCIMS' then-current SOC2 audit report (or comparable industry-standard successor reports) and/or iCIMS' ISO 27001 and 27701 certifications (collectively, "**Audit Reports**") will be used to satisfy any audit or inspection rights or requests by or on behalf of Subscriber, and iCIMS shall make such Audit Reports available to Subscriber upon written request thereof. If such Audit Reports do not provide sufficient information for Subscriber to ascertain iCIMS' compliance with Data Protection & Privacy Laws, iCIMS will make available to Subscriber such information in iCIMS' possession or control as Subscriber may reasonably request with a view to demonstrating iCIMS' compliance with the obligations of Data Processors under Data Protection & Privacy Laws in relation to its Processing of Subscriber Personal Data. Subscriber shall promptly notify iCIMS with information regarding any non-compliance discovered during the course of an audit. The parties agree that the audits described in the Standard Contractual Clauses shall be carried out in accordance with the specifications set forth in Sections 12.1 and 12.2.

13. Restricted Transfers

For Restricted Transfers, the parties agree that such Restricted Transfers shall be governed by the Standard Contractual Clauses, which are incorporated into and made subject to this Addendum by this reference.

14. Certification of Obligations

iCIMS hereby certifies that it understands its obligations under this Addendum and shall comply with them.

15. General Terms

15.1 *Governing law and jurisdiction.* The parties to this Addendum hereby agree to the governing law and submit to the choice of jurisdiction stipulated in the Subscription Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity. If the Standard Contractual Clauses are in effect between the parties, then this Addendum shall be governed by the laws of the jurisdiction stipulated for this purpose in the Standard Contractual Clauses.

15.2 *Order of precedence.* Nothing in this Addendum reduces iCIMS' or any iCIMS Affiliate's obligations under the Subscription Agreement in relation to the protection of Personal Data or permits iCIMS or any iCIMS Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Subscription Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail, except with respect to provisions of this Addendum that expressly clarify a specific provision of the Standard Contractual Clauses. In addition, subject to Section 15.1 and the preceding provisions of this Section 15.2, with regard to the subject matter of this Addendum, in the event of any conflict or inconsistency between the provisions of this Addendum and any other agreements between the parties, including the Subscription Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail. The parties hereto agree that this Addendum shall amend and replace any other amendment or addendum pertaining to the Processing of Subscriber Personal Data entered into by the parties.

15.3 *Third-Party Beneficiary Rights.* Except where required by Data Protection & Privacy Laws and/or as explicitly provided for by the Standard Contractual Clauses, the terms of this Addendum and the Standard Contractual Clauses do not create any third-party beneficiary rights for any individual Data Subjects.

15.4 *Changes in Data Protection & Privacy Laws*. In the event that Data Protection & Privacy Laws are amended, replaced, or repealed, the parties shall, where necessary, negotiate in good faith a solution to enable the Processing of Subscriber Personal Data to be conducted in compliance with Data Protection & Privacy Laws.

15.5 *Severance*. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

APPENDIX 1: DETAILS OF PROCESSING OF SUBSCRIBER PERSONAL DATA

This Appendix 1 includes certain details of the Processing of Subscriber Personal Data.

Subject matter and duration of the Processing of Subscriber Personal Data

The subject matter and duration of the Processing of the Subscriber Personal Data are set out in the Subscription Agreement and this Addendum.

The nature and purpose of the Processing of Subscriber Personal Data

Subscriber Personal Data will be Processed in accordance with the Subscription Agreement for the purposes of enabling Subscriber Group Members to use the Subscription.

The types of Subscriber Personal Data to be Processed

Personal Data relating to the Subscriber's Candidates and Users that is transferred to iCIMS via the Subscription.

The categories of Data Subjects to whom the Subscriber Personal Data relates

Data Subjects include the Subscriber's Candidates and Users as those terms are defined in the Subscription Agreement. Subscriber may submit special categories of Personal Data to the Subscription, the extent of which is determined and controlled by the Subscriber in its sole discretion. If applicable, Subscriber agrees that it has reviewed and assessed the restrictions and safeguards applied to the special categories of Personal Data, including the measures described in Annex II of the Standard Contractual Clauses and has determined that such restrictions and safeguards are sufficient.

The obligations and rights of Subscriber and Subscriber Affiliates

The obligations and rights of Subscriber and Subscriber Affiliates are set out in the Subscription Agreement and this Addendum.

APPENDIX 2: SUBSCRIBER DATA SECURITY ADDENDUM

iCIMS' technical and organizational measures to protect Subscriber Data processed under the Subscription Agreement, including Subscriber Personal Data, are set forth in the Subscriber Data Security Addendum that may be accessed at https://www.icims.com/gc.

APPENDIX 3: STANDARD CONTRACTUAL CLAUSES

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30

days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: The entity identified as Subscriber in the Addendum, the Subscription Agreement, and/or applicable Order Form(s), as applicable.

Address: The address of Subscriber specified in the Addendum, the Subscription Agreement, and/or applicable Order Form(s), as applicable.

Contact person's name, position, and contact details: The name, position, and contact details of Subscriber's contact person specified in the Addendum, the Subscription Agreement, and/or applicable Order Form(s), as applicable.

Activities relevant to the data transferred under these Clauses:

Data exporter's subscription to the iCIMS Talent Cloud products identified in the Subscription Agreement.

Signature and date: The signature and date set forth in the Addendum, the Subscription Agreement, and/or applicable Order Form(s) shall be deemed the signature and date applicable here.

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: The entity identified as iCIMS in the Addendum, the Subscription Agreement, and/or applicable Order Form(s), as applicable.

Address: Bell Works, 101 Crawfords Corner Road, Suite 3-100, Holmdel, NJ 07733

Contact person's name, position, and contact details: The name, position, and contact details of iCIMS' contact person specified in the Addendum, the Subscription Agreement, and/or applicable Order Form(s), as applicable.

Activities relevant to the data transferred under these Clauses:

Provision by data importer of the iCIMS Talent Cloud products which Process Personal Data, where such data is Subscriber Data (as defined in the Subscription Agreement), upon the instruction of the data exporter in accordance with the terms of the Subscription Agreement and the Addendum.

Signature and date: The signature and date set forth in the Addendum, the Subscription Agreement, and/or applicable Order Form(s) shall be deemed the signature and date applicable here.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects include the data exporter's Candidates and Users as those terms are defined in Section 1 of the Subscription Agreement.

Categories of personal data transferred

The Personal Data relating to the data exporter's Candidates and Users that is transferred to iCIMS via the Subscription.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Data exporter may submit special categories of data to the Subscription, the extent of which is determined and controlled by the data exporter in its sole discretion. If applicable, data exporter agrees that it has reviewed and assessed the restrictions and safeguards applied to the special categories of Personal Data, including the measures described in Annex II and has determined that such restrictions and safeguards are sufficient.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Data exporter transfers personal data to iCIMS via the Subscription on a continuous basis in accordance with the frequency of the Subscription's use by data exporter's Candidates and Users.

Nature of the processing

Subscriber Personal Data will be processed by data importer to provide the Subscription to data exporter in accordance with the Subscription Agreement.

Purpose(s) of the data transfer and further processing

Subscriber Personal Data will be transferred and further processed for the purposes of enabling data exporter to use the Subscription in accordance with the Subscription Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Subscriber Personal Data is retained in accordance with any retention periods configured by data exporter via the Subscription, or if such retention periods are not configured, in accordance with the Subscription Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Details of Subprocessors used to provide the Subscription are available at https://icims.help/GDPR-subprocessors

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

An Coimisiún um Chosaint Sonraí / Data Protection Commission (Ireland)

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons, are set forth in Appendix 2 of the Addendum.