Data Protection Addendum

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Master Agreement. Except as specifically modified below, the terms of the Master Agreement shall remain in full force and effect.

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 Master Agreement. Except where the context requires otherwise, references in this Addendum to the Master Agreement are to the Master 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 "**Applicable Laws**" means, as applicable, (a) European Union or Member State laws governing Company Personal Data; (b) any national laws implementing or transposing the GDPR; and (c) any relevant domestic laws;

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

1.1.3 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Master Agreement;

1.1.4 **Customer Data**" means all permitted electronic data stored by Customer or processed through use of the Subscription Services, Customer Data does not include Prohibited Information.

1.1.5 "**Contracted Processor**" means Vendor or a Sub-processor;

1.1.6 **"Customer Personal Information"** means any Company Data maintained by Company and processed by Vendor solely on Company's behalf, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, to the extent that such information is protected as "personal information" (or an analogous variation of such term) under applicable U.S. Data Protection Laws;

1.1.7 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.8 **"Prohibited Information"** means credit or debit card numbers, passwords, protected health information or personal identifiable information as defined in HIPAA (45 C.F.R. § 160.103), and information relating to a customer or consumer of a financial institution under GLBA (15 U.S.C. §§ 6801–6809)."

1.1.9 "**EEA**" means the European Economic Area;

1.1.10 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time including by the GDPR, including any laws implementing or supplementing the GDPR, including within the United Kingdom or any other jurisdiction;

1.1.11 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.12 "**Restricted Transfer**" means:

1.1.12.1 a transfer of Company Personal Data from Company to a Contracted Processor; or

1.1.12.2 an onward transfer of Company Personal Data from a Contracted Processor to another Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of executed Standard Contractual Clauses;

1.1.13 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for the Company pursuant to the Master Agreement;

1.1.14 **"Service Provider"** has the meaning set forth in Section 1798.140(v) of the CCPA.

1.1.15 "**Sub-processor**" means any entity appointed by or on behalf of Vendor to Process Personal Data on behalf of Company in connection with the Master Agreement.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

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

2. Authority

To the extent that Vendor processes Personal Data pursuant to the Master Agreement and this Addendum, each party acknowledges that, for the purpose of Data Protection Laws, Company is the Controller of the Personal Data and Vendor is the Processor. The

scope of this DPA shall cover all Personal Data processed by Vendor that falls within the scope of the GDPR.

3. Processing of Company Personal Data

3.1 Vendor shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data applicable to Vendor's provision of Services under the Master Agreement; and

3.1.2 not Process Company Personal Data other than pursuant to the Master Agreement, or on the Company's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform the Company of that legal requirement before the relevant Processing of that Personal Data.

3.2 Company:

3.2.1 instructs Vendor (and authorises Vendor to instruct each Sub-processor) to:

3.2.1.1 Process Company Personal Data; and

3.2.1.2 in particular, transfer Company Personal Data to any country or territory,

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

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1.

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws).

4. Personnel

Vendor shall take reasonable steps designed to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, in each case limiting access to those individuals who need to know/access the relevant Company Personal Data, as necessary for the purposes of the Master Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, and subjecting all such individuals to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

Vendor or its affiliate will maintain and enforce commercially reasonable physical and logical security methods and procedures to protect Company Personal Data. Vendor will test its systems for potential security vulnerabilities at least annually. Vendor will use commercially reasonable efforts to remedy any breach of security or unauthorised access, and reserves the right to suspend access to the in the event of a suspected or actual security breach. Customer acknowledges that the services and data transmitted are provided via the Internet, a publicly-available computer network, and that such networks are susceptible to failure, attack and hacking. Vendor shall implement appropriate technical and operational measures to ensure a level of security appropriate to the general risks involved in the Services as required by Article 32 of the GDPR. Notwithstanding any other provision, this section sets forth Processor's entire obligation to protect Company Personal Data on the Services. Customer will maintain and enforce commercially reasonable security methods and procedures to prevent misuse of the log-in information of its employees and other users. Vendor shall not be liable for any damages incurred by Customer or any third party in connection with any unauthorised access resulting from the actions of Customer or its representatives.

6. Subprocessing

6.1 Company authorises Vendor to appoint (and permit each Sub-processor appointed in accordance with this section 6 to appoint) Sub-processors in accordance with this section 6 and any restrictions in the Master Agreement.

6.2 Vendor may continue to use those Sub-processors already engaged by Vendor as at the date of this Addendum, subject to Vendor meeting the obligations set out in section 6.5.

6.3 Where Vendor intends to make changes to the use of any of its Sub-processors, it shall inform Company 30 days prior to the date of the appointment of the new Sub-processor. Where the Company objects to such a change (acting reasonably), the Company shall notify Vendor prior to the appointment date of the new Sub-processor. In such case, Vendor and the Company shall meet in good faith, and if no agreement can be found, the Company shall during a reasonable timeframe be entitled to terminate the Master Agreement and any active underlying Order Form on no less than 30 days' written notice.

6.4 On termination of the impacted services, pursuant to section 6.3, Company shall be liable for any contracted fees or charges for the remainder of the term of the Master Agreement and any Order Forms thereunder.

6.5 With respect to each Sub-processor, Vendor shall:

6.5.1 before the Sub-processor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate checks to ensure that the Sub-processor is capable of providing the level of protection for Company Personal Data required by Vendor;

6.5.2 ensure that the arrangement between on the one hand (a) Vendor, or the relevant intermediate Sub-processor, and on the other hand the Sub-processor, is governed by a written contract including terms which offer at least

a similar level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of Article 28(3) of the GDPR; and

6.5.3 provide to Company for review such copies of the Contracted Processors' agreements with Sub-processors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Company may request from time to time.

6.6 Vendor shall ensure that each Sub-processor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Company Personal Data carried out by that Sub-processor, as if it were party to this Addendum in place of Vendor.

7. Data Subject Rights

Vendor shall promptly notify the Company upon becoming aware of any request from a Data Subject under any Data Protection Laws in respect to Company Personal Data. If requested by Company, Vendor shall assist by implementing appropriate technical and organisational measures to assist the Company's obligations to respond to requests to exercise Data Subject rights. Vendor may apply an additional charge or charges, distinct from any charges or fees payable by Company under the Master Agreement or applicable Addendum for the provision of assistance in responding to any Data Subject Request. Charge(s) shall be at Vendor's discretion; however, shall be proportionate to any level of assistance and agreed in advance.

8. Personal Data Breach

8.1 Vendor shall notify Company without undue delay upon Vendor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information regarding such Personal Data Breach.

8.2 Vendor shall cooperate with Company and take such reasonable commercial steps to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Vendor shall provide reasonable assistance to Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of Company by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Laws, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Company Personal Data

10.1 The deletion, return or other treatment of Company Personal Data on termination of the Master Agreement shall be managed in accordance with the terms of the Master Agreement.

10.2 Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws

and always provided that Vendor shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws or the Master Agreement requiring its storage and for no other purpose.

11. Audit rights

11.1 Subject to sections 11.2 to 11.3, Vendor shall make available to Company on request all information reasonably necessary to demonstrate compliance with this Addendum, and shall, at Company's cost, allow for and contribute to audits, including inspections, by Company or an auditor mandated by Company in relation to the Processing of the Company Personal Data.

11.2 Company undertaking an audit shall give Vendor reasonable notice of any audit or inspection to be conducted under section 11.1

11.3 Save for any disclosures required for compliance with Data Protection Laws, Company undertakes to keep, and ensure its auditors keep, all results or findings from any audit confidential and shall indemnify Vendor against any and all losses incurred by Vendor as a result of any breach of this section.

12. Data Transfer

If Vendor or some of its Sub-processors are based in the United States, it may be necessary for Company Personal Data to be transferred outside of the EEA or UK in order to perform services pursuant to the Agreement. Where required, data transfer outside of the EEA or UK shall be done in compliance with the Standard Contractual Clauses. Vendor certifies its compliance and adherence to the EU and Swiss Privacy Shield framework and applicable principles. For restricted transfers not to the United States and therefore not covered by the Privacy Shield framework, Contracted Processor shall ensure adequate data transfer mechanisms are in place to ensure compliance with the Data Protection Laws and protection of Company Personal Data.

13. California Consumer Privacy Act

No Sale of Company Personal Information to Vendor. Company and Vendor hereby acknowledge and agree that in no event shall the transfer of Company Personal Information from Company to Vendor pursuant to the Agreement constitute a sale of information to Vendor, and that nothing in the Agreement shall be construed as providing for the sale of Company Personal Information to Vendor.

14. Survival

14.1 Any provision of this agreement that expressly or by implication is intended to come into or continue in force on or after termination or expiry of this agreement shall remain in full force and effect.

15. General Terms

(e) *Governing law and jurisdiction*

15.1 The parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Master Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity, termination or the consequences of its nullity and all non-contractual or other obligations arising out of or in connection with it.

(f) *Order of precedence*

15.2 Nothing in this Addendum reduces Vendor's obligations under the Master Agreement in relation to the protection of Personal Data or permits Vendor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Master Agreement. COMPANY AGREES AND ACCEPTS THAT IT SHALL NOT BE ENTITLED TO BRING A CLAIM UNDER BOTH THE MASTER AGREEMENT AND/OR THE RELEVANT ORDER FORM(S) AND THIS ADDENDUM FOR DAMAGE OR LOSS CAUSED BY THE SAME EVENT GIVING RISE TO THAT CLAIM. VENDOR'S ENTIRE AGGREGATE LIABLITY HEREUNDER SHALL BE AS STATED IN THE LIMITATION OF LIABILITY PROVISIONS AGREED BETWEEN COMPANY AND VENDOR IN THE MASTER AGREEMENT, AND VENDOR'S (OVERALL) AGGREGATE LIABLITY EXPOSURE TOWARDS THE COMPANY SHALL THEREFORE NOT BE EXPANDED AS A RESULT OF ENTERING INTO THIS ADDENDUM.

15.3 Subject to section 15.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Master 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.

Severance

15.4 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.

Annex 1

1. Subject-matter of the Processing: including client personal data in the Vendor's Services
2. Duration of the processing: the term as set forth in the Agreement
3. The nature of the processing: as set forth in the Agreement
4. The duration of the processing: as set forth in the Agreement
5. The type of personal data: Customer data as described in the Order Form or Master Service Agreement
6. The categories of data subjects: Employees, candidates and contractors as applicable

APPENDIX ONE

Standard Contractual Clauses (controller to processors)

C(2021) 3972 final ANNEX to the
COMMISSION IMPLEMENTING DECISION

on standard contractual clauses for the transfer of personal data to third countries pursuant to

Regulation (EU) 2016/679 of the European Parliament and of the Council

ANNEX

STANDARD CONTRACTUAL CLAUSES

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)[1] for the transfer of personal 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 - Optional

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 its 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[2] (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 thirty (30) calendar 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.[3] 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 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.

(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[4];

(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 one of the EU Member States, provided such law allows 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.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of 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 (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

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]*

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date: _____

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]*

1. Name: Learning Technologies Group Inc., through its division Affirmity

Address: 434 Fayetteville Street, 9th Floor, Raleigh, NC 27601, United States

Contact person's name, position and contact details: Art Machado, VP of Information Security, privacy@ltgplc.com

Activities relevant to the data transferred under these Clauses: Refer to the DPA

Signature and date: _____

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees of the Data Exporter

Categories of personal data transferred

As determined by the Company, but includes Company Personal Data in the Vendor's services.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable

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

Continuous

Nature of the processing

- *Collection,*
- *Storage,*
- *Recording,*
- *Organising,*
- *Making available,*
- *Combining,*
- *Blocking,*
- *Making anonymous,*
- *Erasure and deletion,*
- *Analysing*
- *Providing statistics.*

Purpose(s) of the data transfer and further processing

In connection with the SaaS services provided under the Master Agreement

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

For the duration of the Master Agreement

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

As above.

C. COMPETENT SUPERVISORY AUTHORITY

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

The Data Protection Commission, Ireland

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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.

Vendor will only use Customer Data for the purposes of fulfilling its obligations under the Agreement. Vendor will maintain and enforce physical and logical security procedures with respect to its access and maintenance of Customer Data contained on Vendor servers.

Vendor will use reasonable measures to secure and defend its location and equipment against "hackers" and others who may seek to modify or access the Vendor servers or the information found therein without authorization. Vendor will test its systems for potential security vulnerabilities at least annually.

Vendor has a written information security program ("Information Security Program") that includes administrative, technical, and physical safeguards that protect against any reasonably anticipated threats or hazards to the confidentiality of the Customer Data, and protect against unauthorized access, use, disclosure, alteration, or destruction of the Customer Data. In particular, the Vendor's Information Security Program shall include, but not be limited, to the following safeguards where appropriate or necessary to ensure the protection of Confidential Information and Personal Data.

Access Controls – policies, procedures, and physical and technical controls: (i) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorized persons and (ii) to authenticate and permit access only to authorized individuals.

Security Incident Procedures – policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Customer Data or information systems relating thereto, and procedures to identify and respond to validated security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes.

Contingency Planning – policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages Customer Data or systems that contain Customer Data, including a data backup plan and a disaster recovery plan.

Device and Media Controls – policies and procedures that govern the receipt and removal of hardware and electronic media that contain Customer Data into and out of a Vendor data center, and the movement of these items within a Vendor data center, including policies and procedures to address the final disposition of Customer Data.

Audit controls – hardware, software, and/or procedural mechanisms that record activity in information systems that contain or use Customer Data.

Data Integrity – policies and procedures to guard against the unauthorized disclosure, improper alteration, or unauthorized destruction of Customer Data.

Transmission Security – encryption of electronic information while in transit to guard against unauthorized access to Customer Data that is being transmitted over public communications networks.

Secure Disposal – policies and procedures regarding the disposal of Customer Data, taking into account available technology that can be used to sanitize storage media such that stored data cannot be practicably read or reconstructed.

Testing – Vendor shall regularly test the key controls, systems and procedures of its Information Security Program to verify that they are properly implemented and effective in addressing the threats and risks identified. Tests will be conducted or reviewed in accordance with recognized industry standards (e.g. ISO27001 or SSAE18 and their successor audit standards, or similar industry recognized security audit standards).

Adjust the Program – Vendor shall monitor, evaluate, and adjust, as it deems necessary, the Information Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of Customer Data, and internal or external threats to Affirmity or the Customer Data.

Security Training – Vendor shall provide annual security awareness and data privacy training for its employees that will have access to Customer Data.

Confidentiality - Vendor shall require that all Affirmity employees who are granted access to Customer Data undergo appropriate screening, where lawfully permitted, and enter into a confidentiality agreement prior to being granted such access.

Data Processor shall on request provide a summary of its information security policies it has implemented.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the Sub-processors as provided here:
https://www.ltgplc.com/sub-processor-list

If Vendor wishes to use the services of a new sub-processor, it shall notify the Company. If the Company reasonably objects to the appointment of the new sub-processor the parties shall discuss in good faith the reasons for such objection and whether measures can be undertaken to meet those reasons. If within a period of 30 days from Vendor being notified of an objection the parties have been unable to agree the measures, the Company shall be entitled to terminate the processing of the applicable Personal Data within 7 days of the end of such 30 day period.

ANNEX IV – PRIVACY NOTICE

Learning Technologies Group Plc. its subsidiaries, and its associated businesses ("LTG", "we" or "us") are committed to protecting and respecting your privacy. More information regarding our Privacy Policy is available at https://www.ltgplc.com/privacy-notice/