DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**Agreement**") is between Partner ("**Premier Performance Partners Limited T/A Performance Partners**") and _____ ("**Customer**") dated [from 22/5/2018]. For purposes of this Agreement, the parties recognize that Performance Partners Limited is a data Processor for Customer who is the data Controller.

In consideration of the mutual obligations set out herein, the parties hereby agree to the terms and conditions.

1. Definitions

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

1.1.1 "**Applicable Laws**" means (i) EU Data Protection Laws; and (ii) any other law applicable to Customer Personal Data, including but not limited to data protection or privacy laws of any other country including the UK;

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

1.1.3 "**EU Data Protection Laws**" means GDPR and as amended, replaced or superseded from time to time, including by laws implementing or supplementing GDPR and the Privacy and Electronic Communications Directive 2002/58/EC (as amended by Directive 2009/136) to be replaced by the Regulation on Privacy and Electronic Communications anticipated to come into effect in 2018;

1.1.4 "**GDPR**" means EU General Data Protection Regulation 2016/679 and as amended, replaced or superseded from time to time;

1.1.5 "**Services**" means the services Performance Partners Limited provides to Customer;

1.1.6 "**Customer Personal Data**" means any Personal Data processed by Performance Partners Limited on behalf of the Customer in connection with the Services, including but not limited to customers or employees of Customer;

1.1.7 "**Standard Contractual Clauses**" means the contractual clauses adopted by the European Commission governing the transfer of Personal Data outside of the EU;

1.1.8 "**Sub processor**" means any person (including any third party and any Performance Partners Limited Affiliate, but excluding an employee of Performance Partners Limited or any of its sub-contractors) appointed by or on behalf of Performance Partners Limited or any Performance Partners Limited Affiliate to process Customer Personal Data; and

1.1.9 "**Performance Partners Limited Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Performance Partners Limited, 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.

1.2 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 GDPR, and their associated terms shall be construed accordingly.

2. Customer Warranties and Representations

2.1. Customer warrants and represents it shall observe and comply with all Applicable Laws, privacy legislation and any other legal requirements with respect to Customer Personal Data.

2.2. Without limiting the foregoing warranties and representations in Section 2.1, Customer further warrants and represents that:

2.2.1. it has obtained all necessary consents to enable the lawful transfer of Customer Personal Data to Performance Partners Limited, Performance Partners Limited Affiliates and any Sub processors, to enable the Processing of the Customer Personal Data for the purposes set out in this Agreement;

2.2.2. it has obtained all necessary consents for transfer of Customer Personal Data outside the EEA to countries that do not offer an adequate level of data protection;

3. Processing of Customer Personal Data; Customer's Instructions to Performance Partners Limited

3.1. Annex 1 to this Agreement sets out certain information regarding the Processing of Personal Data as required by Article 28(3) of GDPR.

3.2. Performance Partners Limited and each Performance Partners Limited Affiliate, as Processor(s) under the Agreement, shall not process Customer Personal Data other than on the Customer's reasonable, lawful written instructions as specified in this Agreement, including in Annex 1, unless Processing is required by laws to which Performance Partners Limited or Performance Partners Limited Affiliate is subject, in which event Performance Partners Limited or Performance Partners Limited Affiliate shall to the extent permitted by law inform the Customer of the legal requirement before the relevant Processing of that Personal Data.

3.3. Customer instructs that Performance Partners Limited may disclose Customer Personal Data to a Performance Partners Limited Affiliate or Sub processor in order to provide the Services.

3.4. Performance Partners Limited and each Performance Partners Limited Affiliate shall ensure that all personnel who process the Customer Personal Data are obliged to keep said Personal Data confidential.

3.5. Customer acknowledges and agrees that Processing of Customer Personal Data may include storing or transferring Customer Personal Data outside of the EEA. Where applicable, Customer and Performance Partners Limited, including Performance Partners Limited Affiliate, hereby agree to the Standard Contractual Clauses, as set forth in Annex 3.

4. Data Security

4.1. 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, Performance Partners Limited and each Performance Partners Limited Affiliate shall in relation to the Customer 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 GDPR.

4.2. In assessing the appropriate level of security, Performance Partners Limited and each Performance Partners Limited Affiliate shall take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

4.3. Performance Partners Limited shall notify the Customer without undue delay upon Performance Partners Limited or any Sub processor becoming aware of a Personal Data Breach affecting the Customer Personal Data, providing the Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Applicable Laws.

5. Sub processing

5.1. Performance Partners Limited may only subcontract or outsource the processing of Customer Personal Data to Sub processors where Performance Partners Limited has: (a) received Customer's written consent; and (b) imposed on the Sub processor legally binding contractual terms that require the subcontractor to provide at least the same level of protection for Customer Personal Data as this Agreement.

5.2. Customer hereby generally consents to Performance Partners Limited (a) continuing to use those Sub processors already engaged by Performance Partners Limited as of the date of this Agreement, and (b) engaging any sub processors necessary to fulfil routine business operations, subject to Performance Partners Limited in each case as soon as practicable meeting the obligations set out in section 5.1(b). Customer approves the engagement of the Sub processors listed at Annex 2.

5.3. Where Performance Partners Limited requests to appoint a new Sub processor not encompassed within section 5.2, Customer shall respond to Performance Partners Limited's request for consent within thirty (30) days of receipt of the written request, or such other period of time as the parties may agree for Performance Partners Limited to respond. Customer's consent shall not be unreasonably withheld. If Customer will not consent to the appointment of a Sub processor and Performance Partners Limited deems the appointment essential to Performance Partners Limited's ability to perform under this Agreement, Performance Partners Limited may terminate this Agreement without penalty and Customer shall not be entitled to a refund of any prepaid fees for any unused portion of the remaining term.

6. Data Subject's Rights

Taking into account the nature of the Processing, Performance Partners Limited shall reasonably assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of GDPR.

7. Assistance to the Performance Partners Limited

Taking into account the nature of the Processing and the information available to Performance Partners Limited, Performance Partners Limited shall provide reasonable assistance to the Customer in ensuring compliance with the Performance Partners Limited's obligations under Articles 32-36 of GDPR as those obligations relate to Processing of Customer Personal Data. Articles 32-36 provide that Customer's obligations are to (i) keep data secure; (ii) notify Personal Data Breaches to Supervisory Authorities; (iii) advise Data Subjects when there has been a Personal Data Breach; (iv) carry out data protection impact assessments; and (v) consult with Supervisory Authorities where an

assessment indicates an unmitigated high risk to the Processing.

8. Deletion or Return of Customer Personal Data

8.1. Subject to section 8.2, the Customer may in its absolute discretion by written notice to Performance Partners Limited within fifteen (15) days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "Cessation Date"), require Performance Partners Limited and each Performance Partners Limited Affiliate, at the expense of the Customer, to (i) return a complete copy of all Customer Personal Data to the Customer at Customer's expense; and/or (ii) delete and procure the deletion of all other copies of Customer Personal Data processed by Performance Partners Limited, any Performance Partners Limited Affiliate or Sub processor. Performance Partners Limited and any relevant Performance Partners Limited Affiliate or Sub processor shall comply with any such written request within sixty (60) days of the Cessation Date.

8.2. Performance Partners Limited and each Performance Partners Limited Affiliate and Sub processor may retain Customer Personal Data to the extent required by law or for legitimate business purposes.

9. Audit rights

9.1. Subject to sections 9.2 and 9.3, Performance Partners Limited and any relevant Performance Partners Limited Affiliate shall make available to the Customer on reasonable request and at least forty-five (45) days' prior written notice, information reasonably necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to reasonable audits, including inspections, by the Customer in relation to their Processing of the Customer Personal Data.

9.2. Performance Partners Limited or any relevant Performance Partners Limited Affiliate need not give access to its premises for the purposes of such an audit or inspection (i) to any individual unless he or she produces reasonable evidence of identity, authority, and duty to maintain confidentiality with respect to the Personal Data and any Performance Partners Limited information reasonably considered confidential; or (ii) outside normal business hours at those premises, unless the audit or inspection by law needs to be conducted on an emergency basis and the Customer has given reasonable notice of such emergency to Performance Partners Limited or the relevant Performance Partners Limited Affiliate before any audit or inspection occurs.

9.3. The Customer will not exercise such audit right more frequently than once in any calendar year and Customer will bear the full cost and expense of any such audit, unless such audit discloses a security incident which directly impacts Customer's data and is caused by Performance Partners Limited or Performance Partners Limited's breach of this Agreement, in which case Performance Partners Limited will bear the reasonable cost and expense of such audit.

10. Indemnification

10.1. Performance Partners Limited shall defend, indemnify and hold Customer harmless from any and all claims, damages, liabilities, costs, and expenses (including reasonable counsel fees) Customer incurs or sustains arising out of any breach by Performance Partners Limited of its warranties, representations, and obligations in this Agreement, except to the extent Performance Partners Limited is responsible for the event giving rise to the claim, damage, liability, cost or expense.

10.2. Customer shall defend, indemnify and hold Performance Partners Limited (including Performance Partners Limited Affiliates and Sub processors) harmless from any and all claims, damages, liabilities, costs, and expenses (including reasonable counsel fees) that Performance Partners Limited,

Performance Partners Limited Affiliates or Sub processors incurs or sustains arising out of any breach by Customer of the warranties, representations, and obligations in this Agreement except to the extent Performance Partners Limited, Performance Partners Limited Affiliates or Performance Partners Limited Sub processors are responsible for the event giving rise to the claim, damage, liability, cost or expense.

11. General

11.1. *Conflicts with other agreements*. In the event of inconsistencies between the provisions of this Agreement and any other agreements between the parties, 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 Agreement, the provisions of this Agreement shall prevail.

11.2. *Changes in Applicable Laws*. Performance Partners Limited or Customer may by at least thirty (30) days' written notice to the other from time to time propose any variations to this Agreement which the Performance Partners Limited reasonably considers to be necessary to address the requirements of any Applicable Laws and the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in the notice as soon as is reasonably practicable. Performance Partners Limited need not obtain the consent of any Performance Partners Limited Affiliate to amend this Agreement pursuant to this section 11.2 or otherwise.

11.3. *Severance*. Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement 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 provision had never been contained therein.

11.4. *Governing law and jurisdiction*. The parties to this Agreement submit to the exclusive jurisdiction of the state and federal courts located in New York, New York with respect to any disputes or claims howsoever arising under this Agreement. This Agreement is governed by the laws of the State of New York without regard to conflicts of law rules.

11.5. *Terms that survive on termination*. Sections 10 and 11 of this Agreement shall survive termination.

IN WITNESS WHEREOF, this Agreement is entered into and effective from the date first set out above.

[Performance Partners Limited]	**[Customer]**
Signature _____	Signature _____
Name _____	Name _____
Title _____	Title _____
Date Signed _____	Date Signed _____

Please provide all the contact information requested for your Data Privacy Contact below. We will contact your Data Privacy Contact in the event of a data security breach or an update to our privacy and security policies.

Data Privacy Contact Name: _____

Data Privacy Contact Phone Number: _____

Data Privacy Contact Email Address: _____

ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data

If not otherwise specified in this Agreement, the subject matter and duration of the Processing of the Customer Personal Data are as follows:

Performance Partners Limited processes personal data on behalf of the Customer. It is at the discretion of the Customer, as the data controller to determine the duration and purpose of data processing.

The nature and purpose of the Processing of Customer Personal Data

Customer will be provided with an assessment delivery platform, EPIC. Upon entering in to an engagement with the Performance Partners Limited, Customer will have the option to deliver assessment invitations to their candidates or employees. Assessment takers will receive an email with the login and link to get access to an online assessment to answer a simple questionnaire about a person's behaviour at work. A designated individual will receive a report based on the results of the assessment delivered by EPIC platform. It will describe strengths and stressors.

The data collected from the Customer is to provide services. Servicing the Customer account consists of:

- Create EPIC account;
- Generate personalized reports based on results from participant responses;
- OR register for related events to the assessments used.

The types of Customer Personal Data to be processed

- Customer candidate/employee data personal data (email address provided)

The categories of Data Subject to whom the Customer Personal Data relates

The personal data transferred concern the following categories of data for the Customer:

- Names, business contact information and user names of the Performance Partners Limited's account administrators;
- Names, email address and gender of the data subjects;
- Data subject business/user demographic information;

Data subject source session data which may include personal data sent by the data subject to the Internet, or received by data subject from the Internet;

The obligations and rights of Company and Company Affiliates

The obligations and rights of Performance Partners Limited and Performance Partners Limited Affiliates are set out in this Agreement.

ANNEX 2: SUBPROCESSORS

1. Hosting and Backup Services

- Inscape/ Wiley Publishing, LLC
  Corporate Office: 400 Highway 169 S., Suite 300, Minneapolis, MN 55426

ANNEX 3: STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: [Insert name of party exporting data - Customer]
Address:
Tel.: _____; fax: _____; e-mail: _____
Other information needed to identify the organization:
……
(The data exporter)

And

Name of the data importing organisation: [Insert name of party importing data - Performance Partners Limited]
Address:
Tel.:; fax: _____; e-mail:
Other information needed to identify the organisation:
……
(the data importer)

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

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

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

4. The parties do not object to a data subject being represented by an association or other body if

the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

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

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

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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

Clause 8

Cooperation with supervisory authorities

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

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

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub processor preventing the conduct of an audit of the data importer, or any sub processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Sub processing

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

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

3. The provisions relating to data protection aspects for sub processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

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

Clause 12

Obligation after the termination of personal data processing services

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

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

On behalf of the data exporter: [Populated with details of, and deemed signed on behalf of, the data exporter:]
Name (written out in full):
Position:
Address:
Signature…….

On behalf of the data importer: [Populated with details of, and deemed signed on behalf of, the data importer:]
Name (written out in full):
Position:
Address:
Signature…….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is Customer:

Data exporter is the legal entity that has executed the Data Processing Agreement based on the Standard Contractual Clauses as a Data Exporter established within the European Economic area and Switzerland that have purchased the Service on the basis of one or more Order Form(s).

Data importer
[Performance Partners Limited is a training & assessment based learning organization which Processes Personal Data, where such data is Customer Data, upon the instruction of the data exporter in accordance with the terms of the Agreement and the Data Processing Addendum.

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

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

Customers, business Performance Partners Limited, and vendors of the data exporter
Employees or contact persons of data exporter

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

- Personal data, name and email address (usually business email address)
- (Optionally entered) Demographical Data, Opt out is clearly available.

Processing operations
The personal data transferred will be subject to the following basic processing activities:

The objective of Processing of Personal Data by the data importer is the performance of the Service pursuant to the delivery of assessment based learning.

DATA EXPORTER [Populated with details of, and deemed to be signed on behalf of, the data exporter:]
Name:……
Authorised Signature ……
DATA IMPORTER [Populated with details of, and deemed to be signed on behalf of, the data importer:]
Name:……

Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. Section 1 of this Appendix 2 shall apply to the processing operations provided by the Data Importer, whereas Section 2 shall apply to the processing operations subcontracted to a Subcontractor.

1. Description of the technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

This Appendix describes the technical and organizational security measures and procedures that the Data Importer shall, as a minimum, maintain to protect the security of personal data created, collected, received, or otherwise obtained. Data importer will keep documentation of technical and organizational measures identified below to facilitate audits and for the conservation of evidence.

1.1. Access Control to Processing Areas
1.2. Access Control to Data Processing Systems
1.3. Access Control to Use Specific Areas of Data Processing Systems
1.4. Transmission Control
1.5. Input Control
1.6. Availability Control
1.7. Separation of Processing for Different Purposes
1.8. General Controls

2. Description of the technical and organizational security measures implemented by the Subcontractor in accordance with Clauses 4(d) and 5(c):

2.1. Access Control to Processing Areas

Subcontractor implements suitable measures in order to prevent unauthorized persons from gaining physical access to the data processing equipment where the personal data are processed or used. This is accomplished by:

a) The equipment on which the personal data is processed is placed within a physically protected site secured against accidents, hazards such as fire and flooding, attacks and physical access by unauthorized and/or uncontrolled individuals.
b) Access authorizations are established for staff and third parties to this site. The list of entitled individuals is reviewed periodically to reflect fluctuations and changes in roles and responsibility.
c) This access list is under control of IT management. Changes to this list are limited to a maximum of 3 entitled persons.
d) Access to the site is established only to the identified group of people needed to support the required service level.
e) Secured doors are in place to access the physical site. Access to the site is tracked.
f) Access to the site is protected by a 2 factor identification based on an access card combined with scanned biometric information.
g) In addition the site access is supervised and secured by an appropriate security system and/or security organization using a video control system.
h) The physical site is only entered when work requiring access on site has to be done.

2.2. Access Control to Data Processing Systems

Subcontractor implements suitable measures to prevent its data processing systems from being used or logically accessed by unauthorized persons. This is accomplished by:

a) User Identification and user authentication methods to grant access to the processing system are in place. Individual authentication credentials such as user IDs or similar are used that, once assigned, cannot be re-assigned to another person.
b) Access control and authorizations are defined according to a 'need to have' principle and are implemented in such a way that users are uniquely identified and approved by business owners. A deactivation of user authentication credentials in case the person is disqualified from accessing the data or in case of non-use for a substantial period of time is done, except for those accounts authorized solely for technical management.
c) Privileged accounts are reserved for specific IT functions and not used outside of the required need of usage. System administrators are identified and named and an up to date list with area covered is provided if requested.
d) Password rules are in place to control access.

Internet facing or end user facing endpoints are protected to prevent unwanted access to the systems and to avoid infiltration of malicious software. This covers areas as firewalls, antivirus detection, malware detection, and others and is adjusted to new technologies based on the overall development.

2.3. Access Control to Use Specific Areas of Data Processing Systems

Subcontractor commits that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by its access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by:

a) Policies related to the access to personal data are in place and trained. To ensure that staff will only access personal data and resources required to perform their job duties, staff is informed about their obligations and the consequences of any violations of such obligations.
b) Special requests within the application, such as moving records and transferring sub accounts, are logged within the system.
c) On request of the data exporter additional dedicated confidentiality agreements for sensitive data are put in place with all persons accessing this information.
d) Specific encryption technology for very sensitive data elements, such as passwords has been implemented.

2.4. Transmission Control

Subcontractor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

a) State-of-the-art network and network access protection technologies are used
b) Monitoring of the completeness and correctness of the transfer of data is supported by using networking protocols (TCP) with error correction features.
c) If data has to be copied to specific media's for transport to a 3rd party, these media's will be treated with discernment in accordance with the sensitivity of the data.

d) Authentication information which is being transferred within the public network is always encrypted. When accessed via the Internet encrypted transfer for all other data is used whenever feasible.

2.5. Input Control

Subcontractor implements suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or re- moved. This is accomplished by:

a) An authorization policy for the input of data, as well as for the reading, alteration and deletion of stored data is in place as described in section, Access Control to Data Processing Systems'.
b) If required for an adequate protection a role based access control is put in place supporting the segregation of duty concept. Whereas the data subcontractor has the responsibility to support such a concept where technically possible, the data exporter is responsible for the application of these concepts in the usage of the application based on an overall risk approach.

2.6. Availability Control

Subcontractor implements suitable measures to ensure that personal data are protected from accidental destruction or loss. This is accomplished by:

a) Availability is managed and designed based on an overall service level concept.
b) The physical site where the data processing equipment is located is protected against general environmental hazards and unauthorized access. It is protected with specific measures against power loss through UPS and Diesel engines. It monitors and controls temperature and humidity at the site and alerts when reaching limits.
c) Availability of the network access to the site is enhanced through WAN based redundancies, network access redundancies to the site and within the site through redundant datacenter based networks.
d) Redundancies of the Infrastructure components itself (server and storage array's) are in place.
e) The redundancy measures are checked on a regular base. The results are documented accordingly.
f) State of the art functionalities are used on DB level to target for a minimum loss of transactional information in case of a technical failure. This is done by using DB features supporting minimal loss of transaction information where possible and meaningful.
g) The database is replicated in a disaster recovery site. Fail over to the DR site can be accomplished in a time frame of one hour or less.
h) To reduce unscheduled downtimes proactive infrastructure maintenance is done. During these maintenance windows proactive tasks are executed to keep the infrastructure on a sup- ported level aligned with the providers of the infrastructure components.
i) After serious events a structured After Action Review will be executed to detect mitigation actions and potential proactive measures.
j) Technical and application related changes are following change management processes, supported where possible by multiple tiers where changes are applied first before being applied to the production environment.
k) Technical Backups are implemented and executed based on a predefined policy to allow recovering data and application in accordance with the overall backup policy. This backup covers technical failures or human errors of technical staff and implements data copies with short retention times. These backup copies are securely stored at a specifically protected sited, separated from the site where the primary data resides. Backups are taken based on a defined

service definition (backup frequency and retention) and also establish a target recovery time objective to get the backup restored to the primary location in case of loss of the primary data.

l) If storage media are end of life and will be decommissioned specific destruction mechanism will be used to delete the stored data securely.

2.7. Separation of processing for different purposes

Subcontractor implements suitable measures to ensure that data collected for different purposes can be processed separately. This is accomplished by:

a) Access to data is separated through application security for the appropriate users.
b) Application roles and resulting access is based on roles based on function to be done.

2.8. General Controls

Subcontractor will in addition apply the following procedures:

a) A general IT Security Policy is in place. Specific documentation to support local regulations and requirements in the area of data protection may be made available based on joint agreements between the Data Exporter and the Subcontractor.
b) Regular at least yearly checks of the herein described measures are scheduled and executed.
c) To detect security or data integrity related threats, to investigate violation of privacy issues or other malicious attacks the Subcontractor may use enhanced monitoring and surveillance techniques to detect any misuse or threatening behaviour without disclosing this be- forehand.
d) Any issue impacting the service levels defined or specific security incidents impacting the data exporters system will be documented and communicated accordingly.

On behalf of the data exporter:
Company: _____
Name (written out in full): _____
Position: _____
Address: _____

Signature _____

On behalf of the data importer:
Company: _____
Name (written out in full): _____
Position: _____
Address: _____

Signature _____