

## Data Protection Addendum

This Data Protection Addendum ("**Addendum**") forms part of the Subscription Agreement ("**Principal Agreement**") between: (i) ChallengeRunner, LLC ("**ChallengeRunner**") and (ii) [**Customer Name**] on behalf of itself and its affiliates (collectively, "**Company**").

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 Principal Agreement. Except as modified below, the terms of the Principal 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 Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal 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 (a) European Union or Member State laws with respect to any Company Personal Data in respect of which Company is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Company Personal Data in respect of which Company is subject to any other Data Protection Laws;

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

1.1.3 "**Contracted Processor**" means ChallengeRunner or a Subprocessor;

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

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

1.1.6 "**EU Data Protection Laws**" means the GDPR and laws implementing or supplementing the GDPR;

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

1.1.8 "**Restricted Transfer**" means:

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

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

in each case, where such transfer would be prohibited by Data Protection 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 the Standard Contractual Clauses to be established under Sections 5.4.3 or 11 below;

- 1.1.9 "Services" means the services and other activities to be supplied to or carried out by or on behalf of ChallengeRunner for Company pursuant to the Principal Agreement;
  - 1.1.10 "Standard Contractual Clauses" means the contractual clauses set out in Annex 2, amended as indicated (in square brackets and italics) in that Annex;
  - 1.1.11 "Subprocessor" means any person (including any third party, but excluding an employee of ChallengeRunner or any of its sub-contractors) appointed by or on behalf of ChallengeRunner to Process Personal Data on behalf of any Company in connection with the Principal Agreement; and
- 1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processor**", "**Processing**" 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. Processing of Company Personal Data

- 2.1 For the purposes of this Addendum, Company is the Controller and ChallengeRunner is the Processor.
- 2.2 ChallengeRunner shall:
- 2.2.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and
  - 2.2.2 not Process Company Personal Data other than on the Company's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case ChallengeRunner shall to the extent permitted by Applicable Laws inform the Company of that legal requirement before the relevant Processing of that Personal Data.
- 2.3 Company:
- 2.3.1 instructs ChallengeRunner (and authorises ChallengeRunner to instruct each Subprocessor) to:
    - 2.3.1.1 Process Company Personal Data; and
    - 2.3.1.2 in particular, transfer Company Personal Data to any country or territory,  
  
as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and
  - 2.3.2 shall comply with all applicable Data Protection Laws in respect of its processing of Company Personal Data and any processing instructions it issues to ChallengeRunner.

- 2.3.3 warrants and represents that it has provided notice and obtained (or will obtain) any and all consents and rights necessary under Data Protection Laws for ChallengeRunner to Process Company Personal Data pursuant to the Principal Agreement.
  - 2.3.4 warrants and represents that it has a legitimate lawful basis under the Data Protection Laws for Processing the Company Personal Data;
  - 2.3.5 warrants and represents that it provides clear and sufficient information to data subjects, in accordance with the Data Protection Laws, of the purpose for which it will process their personal data, the legal basis for such purposes, and such other information s is required by Article 13 of the GDPR.
  - 2.3.6 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 2.3.1 on behalf of Company.
  - 2.3.7 shall indemnify, keep indemnified and defend at its own expense ChallengeRunner against all costs, claims, damages or expenses incurred by the ChallengeRunner or for which the ChallengeRunner may become liable due to any failure by Company or its employees, subcontractors or agents to comply with any of its obligations under this Addendum or the Data Protection Laws.
- 2.4 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). Company may make reasonable amendments to Annex 1 by written notice to ChallengeRunner from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this Section 2.4) confers any right or imposes any obligation on any party to this Addendum.

### **3. ChallengeRunner Personnel**

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

### **4. 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, ChallengeRunner shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.
- 4.2 In assessing the appropriate level of security, ChallengeRunner shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

### **5. Subprocessing**

- 5.1 Company authorises ChallengeRunner to appoint (and permit each Subprocessor appointed in accordance with this Section 5 to appoint) Subprocessors in accordance with this Section 5 and any restrictions in the Principal Agreement.
- 5.2 ChallengeRunner may continue to use those Subprocessors already engaged by ChallengeRunner as at the date of this Addendum, subject to ChallengeRunner as soon as practicable meeting the obligations set out in Section 5.4.
- 5.3 ChallengeRunner shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within thirty (30) of receipt of that notice, Company notifies ChallengeRunner in writing of any objections (on reasonable grounds) to the proposed appointment:
  - 5.3.1 ChallengeRunner shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and
  - 5.3.2 where such a change cannot be made within thirty (30) days from ChallengeRunner's receipt of Company's notice, notwithstanding anything in the Principal Agreement, Company may by written notice to ChallengeRunner with immediate effect terminate the Principal Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor.
- 5.4 With respect to each Subprocessor, ChallengeRunner or shall:
  - 5.4.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with Section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;
  - 5.4.2 ensure that the arrangement between on the one hand (a) ChallengeRunner, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;
  - 5.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) ChallengeRunner, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Company Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the Company; and
  - 5.4.4 provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (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.
- 5.5 ChallengeRunner shall ensure that each Subprocessor performs the obligations under Sections 2.2, 3, 4, 6.1, 7.2, 8, 10.1, as they apply to Processing of Company Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of ChallengeRunner.

## 6. Data Subject Rights

- 6.1 Taking into account the nature of the Processing, ChallengeRunner shall assist Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company's obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
- 6.2 ChallengeRunner shall:
- 6.2.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and
  - 6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Contracted Processor is subject, in which case ChallengeRunner shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

## 7. Personal Data Breach

- 7.1 ChallengeRunner shall notify Company without undue delay upon ChallengeRunner or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
- 7.2 ChallengeRunner shall co-operate with Company and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

## 8. Data Protection Impact Assessment and Prior Consultation

ChallengeRunner 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 Law, 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.

## 9. Deletion or return of Company Personal Data

- 9.1 Subject to Sections 9.2 and 9.3 ChallengeRunner shall promptly and in any event within sixty (60) days of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.
- 9.2 Subject to Section 9.3, Company may in its absolute discretion by written notice to ChallengeRunner within fifteen (15) days of the Cessation Date require ChallengeRunner to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as may be mutually agreed to between Company to ChallengeRunner; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any Contracted Processor. ChallengeRunner shall comply with any such written request within forty-five (45) of the Cessation Date.

- 9.3 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 ChallengeRunner 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 requiring its storage and for no other purpose.
- 9.4 Upon Company request, ChallengeRunner shall provide written certification to Company that it has fully complied with this Section 9.

## **10. Audit rights**

- 10.1 Subject to Sections 10.2 and 10.3, ChallengeRunner shall make available to Company on request all information reasonably necessary to demonstrate compliance with this Addendum, and shall 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 by the Contracted Processors, unless ChallengeRunner promptly informs the Company that, in its opinion, any exercise of Company's rights under this Section 10.1 would violate a Data Protection Law.
- 10.2 Information and audit rights of Company only arise under Section 10.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).
- 10.3 Company shall give ChallengeRunner reasonable notice of any audit or inspection to be conducted under Section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

## **11. Restricted Transfers**

- 11.1 Subject to Section 11.3, Company (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from Company to that Contracted Processor.
- 11.2 The Standard Contractual Clauses shall come into effect under Section 11.1 on the later of:
- 11.2.1 the data exporter becoming a party to them;
  - 11.2.2 the data importer becoming a party to them; and
  - 11.2.3 commencement of the relevant Restricted Transfer.
- 11.3 Section 11.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

## **12. General Terms**

- 12.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

- 12.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and
- 12.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.
- 12.2 Each party shall comply with all relevant Data Protection Laws and the terms of this Addendum, at its own cost and nothing set forth in this Addendum relieves either party of its own direct responsibilities and liabilities under the Data Protection Laws. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.
- 12.3 Subject to Section 12.2, 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 Principal 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.
- 12.4 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.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

**[Company]**

Signature \_\_\_\_\_

Name \_\_\_\_\_

Title \_\_\_\_\_

Date Signed \_\_\_\_\_

**ChallengeRunner, LLC**

Signature \_\_\_\_\_

Name \_\_\_\_\_

Title \_\_\_\_\_

Date Signed \_\_\_\_\_



## **ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA**

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

### **Subject matter and duration of the Processing of Company Personal Data**

*The subject matter and duration of the Processing of the Company Personal Data are set out in the Principal Agreement and this Addendum.*

### **The nature and purpose of the Processing of Company Personal Data**

*The Company Personal Data will be subject to automated and manual Processing operations by ChallengeRunner including collection, use, analysis, transfer, storage, and erasure to provide Company with services as specified in the Principal Agreement.*

### **The types of Company Personal Data to be Processed**

*Company as data controller may submit Personal Data to the Services, the extent of which is determined solely by the Company, and may include:*

- *Individuals' names, email addresses, activity data (as determined in the Company's sole discretion), telephone numbers, and office location.*
- *Other Personal Data submitted through the Services.*

### **The types of Special Categories of Data to be Processed**

*Company as data controller may choose to submit Special Categories of Personal Data to the Services, the extent of which is solely determined by Company in compliance with Data Protection Law, and may include the following categories, if any:*

- *Information related to an individual's health.*

### **The categories of Data Subject to whom the Company Personal Data relates**

*Company as data controller may submit Personal Data to the Services, the extent of which is solely determined by Company, and may include Personal Data relating to the following categories of Data Subjects:*

- *Company's employees and personnel.*

### **The obligations and rights of Company**

*The obligations and rights of Company are set out in the Principal Agreement and this Addendum.*

## ANNEX 2: 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: [COMPANY]

Address: [REDACTED]

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

.....  
(the data **exporter**)

And

Name of the data importing organisation: ChallengeRunner, LLC

Address: [REDACTED]

Tel.: [REDACTED]; fax: [REDACTED]; e-mail: support@challengerunner.com

.....  
(the data **importer**)

each a “party”; together “the parties”,

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

#### *Clause 1*

#### **Definitions**

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; [If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words “except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of “personal data” is expanded to include those data” are added.]*
- (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; [If these Clauses are

*not governed by the law of a Member State, the words "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" are deleted.]*

- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## *Clause 2*

### ***Details of the transfer***

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

## *Clause 3*

### ***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

#### Clause 4

##### ***Obligations of the data exporter***

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; *[If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.]*
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

#### Clause 5

##### ***Obligations of the data importer***

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it

- agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
  - (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
  - (d) that it will promptly notify the data exporter about:
    - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
    - (ii) any accidental or unauthorised access, and
    - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
  - (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
  - (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
  - (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
  - (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
  - (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
  - (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

## *Clause 6*

### ***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually

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

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

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

#### *Clause 7*

##### ***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
  - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

#### *Clause 8*

##### ***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

#### *Clause 9*

##### ***Governing Law***

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

#### *Clause 10*

##### ***Variation of the contract***

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

#### *Clause 11*

##### ***Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

#### *Clause 12*

##### ***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of

the personal data transferred and will not actively process the personal data transferred anymore.

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

**On behalf of the data exporter:**

Name (written out in full):

Position:

Address:

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

Signature.....

**On behalf of the data importer:**

Name (written out in full):

Position:

Address:

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

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: [TO BE COMPLETED]

### Data importer

The data importer is: ChallengeRunner, LLC is headquartered in Cincinnati, Ohio. ChallengeRunner, LLC has been instructed by data exporter to provide the services specified in the Principal Agreement, involving the processing of certain personal data (described below).

### Data subjects

The personal data transferred may include the following categories of data subjects, the extent of which is solely determined by the data exporter:

- Employees and personnel of data exporter.

### Categories of data

The personal data transferred may include the following categories of data, the extent of which is determined solely by the data exporter:

- Individuals' names, email addresses, activity data (as determined in the data exporter's sole discretion), telephone numbers, and office location.
- Other Personal Data submitted through the Services.

### Special categories of data

The personal data transferred may include the following special categories of data, if any, the extent of which is solely determined by data exporter in compliance with Data Protection Law:

- Information related to an individual's health.

### Processing operations

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

- In order to provide the services specified in the Principal Agreement, the data importer will collect data input by the data exporter's employees and personnel into the data importer's software and/or received by integrations with the data exporter's employee's third-party activity trackers; the data would then be transferred to the data importer's servers, located in Cincinnati, Ohio through a secure connection. There, the data would be analysed by certain software of the data importer. The data importer will then provide the data exporter with information in its software.

### DATA EXPORTER

Name:.....

Authorised Signature .....

### 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.

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

***[ChallengeRunner to fill in and provide details as to their technical and organizational security measures]***

**1. Entrance Control**

Data importer implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used. This is accomplished by:

- [\_\_\_\_\_]
- [\_\_\_\_\_]
- [\_\_\_\_\_]
- [\_\_\_\_\_]
- [\_\_\_\_\_]

**2. Server Access Control**

Data importer implements suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished by:

- [\_\_\_\_\_]
- [\_\_\_\_\_]
- [\_\_\_\_\_]
- [\_\_\_\_\_]
- [\_\_\_\_\_]

**3. Data Access Control**

Data importer ensures that the persons entitled to use its data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This is accomplished by:

- [\_\_\_\_\_]
- [\_\_\_\_\_]

- [REDACTED]
- [REDACTED]
- [REDACTED]

**4. Transfer Control**

Data importer 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:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

**5. Enter Control**

Data importer 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 removed. This is accomplished by:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

**6. Data Processing Control**

Data importer implements suitable measures to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal. This is accomplished by:

- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]

**7. Loss Control**

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

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

**8. Separation Control**

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

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

*(signatures to Appendix 2 follow)*

DATA EXPORTER

Name:.....

Authorised Signature .....

DATA IMPORTER

Name:.....

Authorised Signature .....