Data Processing Addendum

Background

This Data Processing Addendum ("DPA") is an addendum to, and forms part of, the main services agreement (the "**Main Agreement**") between (1) Team Challenge Apps Ltd, incorporated and registered in Scotland with company number SC517746 whose registered office is at Clyde Offices, 2nd Floor, 48 West George Street, Glasgow, G2 1BP (hereinafter the "**Processor**") and (2) the client signed up to use the service (hereinafter the "**Controller**"), hereinafter collectively referred to as '**Parties**' and individually '**Party**'. In the case of conflict or ambiguity between any provision contained in the Main Agreement and any provision in this DPA, the provision in the DPA shall take precedence.

The following attached schedules also form part of this DPA :

- Schedule 1: Services, Processing, Personal Data and Data Subjects
- Schedule 2: Security Measures

The Parties have agreed to enter into this DPA to ensure compliance with Data Protection Legislation (as defined below) applicable to the Processing of Personal Data by the Processor for and on behalf of the Controller under this DPA.

Definitions

1. Agreed Terms

The terms and expressions set out in this DPA shall have the following meanings:

1. **Data Protection Legislation**: all applicable data protection and privacy legislation in force from time to time in the UK including the retained UK law version of the General Data Protection Regulation ((EU) 2016/679) ("**UK GDPR**"), the Data Protection Act 2018 (and regulations made thereunder) or any successor legislation, and all

other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data (including, without limitation, the privacy of electronic communications).

2. "**Controller**", "**Processor**", "**Processing**" and "**Data Subject**" shall have the meanings given to them in the Data Protection Legislation; In short, "Controller" means an entity which determines the purposes and means of the Processing of Personal Data, "Processor" means an entity that Processes Personal Data on behalf of the Controller.

3. **ICO** means the Information Commissioner's Office;

4. **Personal Data** means all such "personal data" as defined in the Data Protection Legislation as is, or is to be, Processed by the Processor on behalf of the Controller;

5. **Services** means those services described in Schedule 1 which are provided by the Processor to the Controller and which the Controller uses for the purposes described in Schedule 1.

6. "**Security Measures**" means the security measures set out in Schedule 2

7. Clause, Schedule and paragraph headings shall not affect the interpretation of this DPA. A person includes a natural person, corporate or unincorporated body (whether or not having separate legal personality). The Schedules form part of this DPA and shall have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Schedules. A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established. Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular. Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.

It Is Agreed as follows:

2. Scope of Processing

1. The Controller determines the purposes and means of the Processing of Personal Data. The Controller shall at all times comply with its obligations pursuant to Data Protection Legislation, including ensuring that it has a sufficient and valid lawful basis for providing any Personal Data to the Processor, and authorising the Processor, to perform its obligations, activities and exercise its rights under this DPA.

2. The terms of this DPA supersede any other arrangement, understanding or agreement made between the Parties at any time relating to Processing of Personal Data.

3. This DPA concerns the Processor's Processing of Personal Data on behalf of the Controller in connection with the Processor's provision of the Services as described in Schedule 1.

4. The nature and the purpose of the Processing, including operations and activities, are specified in Schedule 1. The Processor shall Process Personal Data received from the Controller:

    4.1. for the purposes of the Services and as set out in Schedule 1;

    4.2. to the extent and in such manner as is necessary for those purposes; and

    4.3. in accordance with the documented instructions of designated contacts at the Controller (which must be specific instructions) unless the Processor is required to do otherwise by law (in which case the Processor will inform the Controller of such legal requirement prior to the processing, unless prohibited from doing so on legal grounds).

5. The Processor shall immediately inform the Controller if, in the Processor's opinion, an instruction infringes Data Protection Legislation.

6. The Processor shall appropriately respond to any request from the Controller requiring the Processor to amend, transfer or delete, or stop the further Processing of the Personal Data.

7. Where the Processor Processes Personal Data on behalf of the Controller it shall:

    7.1. Process the Personal Data only to the extent, and in such manner, as is necessary in order to properly provide the Services and comply with its obligations to the Controller or as is required by law or any regulatory body including but not limited to the ICO;

    7.2. implement and maintain appropriate technical and organisational measures, and take all steps necessary, to protect the Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure;

    7.3. if so requested by the Controller (and within reasonable timescales required by the Controller) supply reasonably sufficient detail of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access;

    7.4. make available to the Controller all information reasonably necessary to demonstrate compliance with the obligations detailed in this DPA; and

    7.5. upon the Controller’s request, and at the Controller’s cost, allow for and contribute to audits, including inspections, conducted by the Controller or

the Controller's approved professionally-appointed auditor provided that the Controller gives to the Processor reasonably sufficient (and no less than 8 weeks') written notice and such audits are limited to once every calendar year.

8. The Processor shall notify the Controller (within two working days) if it receives:

    8.1. a request from a Data Subject for access to, correction, restriction, portability or deletion of that person's Personal Data or an objection from that person regarding the Processing of their Personal Data; or

    8.2. a complaint or request relating to the Controller's obligations under the Data Protection Legislation.

9. Taking into account the nature of the Processing, the Processor agrees to provide the Controller with all reasonable assistance, insofar as this is possible, in relation to fulfilling the Controller's obligation to respond to requests for exercising the Data Subject's rights under Data Protection Legislation, including (where appropriate and applicable) by:

    9.1. providing the Controller with reasonably sufficient detail of the complaint or request;

    9.2. complying with a data access request within the relevant timescale and in accordance with the Controller's instructions;

    9.3. providing the Controller with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Controller under UK GDPR);

    9.4. providing the Controller with any information reasonably requested by the Controller in order to enable the Controller to fulfil its obligation under Data Protection Legislation; provided that the Controller shall bear any costs accrued by the Processor related to any such co-operation and assistance.

3. Security Measures

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, to ensure a level of security appropriate to the risk, the Processor shall implement the technical and organisational measures as required in Data Protection Legislation and as outlined in Schedule 2.

2. The Processor shall provide reasonable assistance to the Controller, taking into account relevant information available to the Processor, if the Controller is obliged to perform an impact assessment and/or consult the ICO in connection with the

Processing of Personal Data. The Controller shall bear any costs accrued by the Processor related to such assistance.

4. Notification of any Breach

1. The Processor shall notify the Controller without undue delay after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by the Processor on behalf of the Controller ("**Personal Data Breach**"). The Processor acknowledges that the Controller is responsible for notifying the Personal Data Breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, to the ICO or and/or applicable supervisory authority (unless the Controller determines that the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of individuals) and the Processor shall provide all reasonably necessary assistance to the Controller in relation to this.

2. The Processor's notification to the Controller shall, insofar as the Personal Data Breach affects Personal Data relating to the Controller, as a minimum describe (i) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) the likely consequences, in the reasonable opinion of the Processor, of the Personal Data Breach; (iii) the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

3. In the event the Controller is obliged to communicate a Personal Data Breach to the Data Subjects, the Processor shall provide all reasonable assistance to the Controller provided that the Controller shall bear any costs related to such assistance provided by the Processor and to such communication to the Data Subject. The Processor shall nevertheless bear any such reasonable costs for those aspects of the Personal Data Breach attributed to circumstances for which the Processor is responsible.

5. Sub-Processing

1. Only to the extent where Personal Data is Processed by the Processor in its capacity as processor for and on behalf of the Controller, the Processor shall not engage another data processor (a "**Sub-Processor**") without the Controller's written authorisation. However, so far as is necessary for the purposes and/or performance of the Main Agreement, the Controller hereby grants to the Processor written authorisation to use as Sub-Processors the data hosting and storage, server

management, email delivery, IT support and error handling provider(s) as listed in the Processor's privacy policy (https://app.bigteamchallenge.com/privacy).

2. The Processor shall inform the Controller of any intended subsequent changes concerning addition or replacement of any of its Sub-Processors engaged under this Clause 5, and the Controller has the right to raise reasonable objections to such changes in writing. If there is no clear objection made by the Controller in writing to the Processor within 3 working days of being informed about such a change by the Processor, then the change shall be deemed accepted by the Controller. If such an objection is made within that time period, provided such objection within that time period reflects a genuine privacy concern of the Controller and is made in writing providing a detailed explanation of the objection, the Parties shall enter into good faith discussions in an attempt to agree a commercially suitable workaround. However, if the Parties do not arrive at a suitable workaround or such a workaround is not possible, the Processor shall have the right to terminate the Main Agreement (including this DPA) upon notice in writing to the Controller.

3. Any Sub-Processor engaged under this Clause 5 shall provide sufficient guarantees to implement appropriate technical and organisational measures to comply with Data Protection Legislation. The Processor shall remain fully liable to the Controller for the performance of any Sub-Processor engaged under this Clause 5, who will have a written agreement with the Processor containing obligations which provide a level of protection for the Personal Data equivalent in all material respects to this DPA.

6. Liability

The limitations and exclusions of liability set out in the Main Agreement shall apply to this DPA.

7. Confidentiality

1. The Processor shall ensure that persons authorised by it to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

2. The Controller is subject to a duty of confidentiality regarding any documentation and information received by the Processor related to the Processor's (and its Sub-Processors') Processing obligations under this DPA, including any documentation and information regarding any technical and organisational security measures.

8. Term and Termination

1. This DPA is valid for as long as the Main Agreement remains in effect or the Processor continues Processing Personal Data on behalf of the Controller.
2. Subject to the duration and retention requirements in Schedule 1, the Processor shall, upon the termination of the Main Agreement and at the choice of the Controller, delete or return all the Personal Data to the Controller, unless an applicable law requires ongoing storage by the Processor of the Personal Data or certain aspects of it (and the Processor shall inform the Controller if this is the case).

9. International Data Transfer

1. Where the Processor transfers Personal Data to a third country / international organisation in accordance with Clause 5 (engagement of Sub-Processors) it shall ensure that appropriate safeguards are in place in relation to the protection and rights of Data Subjects and in accordance with the Data Protection Legislation. Specifically, such safeguards include approved data protection clauses (including (i) the international data transfer agreement and (ii) the addendum to the European Commission's standard contractual clauses for international data transfers both issued by the ICO); or an approved certification mechanism.

10 General

1. This DPA shall be governed by the Scots Law and the Parties irrevocably submit to the exclusive jurisdiction of the courts of Scotland.

Schedule 1

Services, Processing, Personal Data, and Data Subjects

1. Services

The "Services" referred to in Sub-Clause 1.5 means the Big Team Challenge software-as-a-service product, website and mobile apps, plus any development and support in relation to the Controller's challenge.

A further description of the Services is set out in the Main Agreement and any applicable documentation.

The Controller uses the Services for the following purposes: Providing the Controller's virtual activity challenge to its Customers; administering the Controller's challenge; supporting the Controller's challenge and participant technical support.

The above constitutes the subject-matter and nature of the Processing by the Processor.

2. Processing

The Personal Data will be subject to the following basic Processing activities carried out by the Processor:

- Personal Data will be Processed to the extent necessary to provide the Services in accordance with both the provisions of the Main Agreement and the Controller's instructions.
- Technical support, hosting, email notification, debugging and error correction to ensure the normal running of the Services. This includes resolving technical issues both generally in the provision of the Services and specifically in answer to a Controller or Controller's subject query. This operation may relate to all aspects of Personal Data Processed but will be limited to anonymous metadata where possible.

3. Personal Data

The Personal Data Processed concern the following categories: full name, email address, company/employer/charity/local authority, record of correspondence, challenge data (for example, step count, distance covered, altitude, date and time).

The Services allow (but do not require) Controllers to ask for additional registration fields for their users to fill in. These include, but are not limited to, department, age, staff ID number.

4. Data Subjects

The Personal Data Processed concern the following categories of Data Subjects:

- The Controller's employees
- The Controller's customers (or, if the Controller is a charity, the Controller's donors, applicants or users)
- The Controller's subcontractors' employees
- (If not covered in the above three categories) the Controller's applicants opted into the challenge set up by the Controller

5. Duration/retention

See Clause 8 of the DPA. The Processor shall retain user data in relation to a Controller (including Personal Data) until termination of the Main Agreement. After this, the Processor then deletes – or at least renders anonymous – that data. If the Controller requests for its data to be deleted sooner than the above mentioned period, or returned to the Controller prior to deletion, the Processor will carry out that instruction, in accordance with the terms

of the Main Agreement, unless determined otherwise by applicable law or contractual obligation.

Schedule 2

Security Measures

The following are the Security Measures referred to in Sub-Clauses 1.6 and 3:

1. The Processor will ensure that in respect of all Personal Data it receives from or Processes on behalf of the Controller it maintains security measures to a standard appropriate to:

    1.1. the harm that might result from unlawful or unauthorised Processing or accidental loss, damage or destruction of the Personal Data; and

    1.2. the nature of the Personal Data.

2. In particular the Processor shall, to ensure a level of security appropriate to the risk:

    2.1. have in place and comply with its security policy;

    2.2. ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in Processing the Personal Data in accordance with best industry practice;

    2.3. prevent unauthorised access to the Personal Data;

    2.4. ensure its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

    2.5. have secure methods in place for the transfer of Personal Data (for instance, by using encryption);

    2.6. put password protection on computer systems on which Personal Data is stored and ensure that only authorised personnel are given details of the password;

    2.7. take reasonable steps to ensure the reliability of Processor personnel or other persons representing the Processor who have access to the Personal Data;

2.8. ensure that none of the personnel or other persons who have access to the Personal Data publish, disclose, distribute or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller;

2.9. have in place methods for dealing with breaches of security and notify the Controller as soon as any such security breach occurs;

2.10. have a secure procedure for backing up and storing back-ups;

2.11. have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print outs and redundant equipment; and

2.12. adopt such organisational, operational and technological Processes and procedures appropriate to the Services provided to the Controller.

This DPA is automatically incorporated into, and forms part of, the Main Agreement when entered into by the Parties. The Controller, however, may wish to acknowledge its agreement to this DPA by execution below. If the Controller decides to do so, please download this DPA, sign it where indicated below and return it to privacy@bigteamchallenge.com

This DPA cannot be amended or modified by either Party except with a separate written document signed by each Party.

SIGNED for and on behalf of the Controller	SIGNED for and on behalf of Team Challenge Apps Ltd (the Processor)
by	by **David Rushton**
Position	Position **Data Protection Officer**
Signature	Signature