SCHEDULE - Data Processing Obligations

1. **Background**

1.1 This Schedule sets out various obligations in relation to the processing of Protected Data uploaded to Upshot. If there is a conflict between the provisions of the rest of this Agreement and this Schedule, the provisions of this Schedule shall prevail.

1.2 FFTL provides Upshot as a facility to you under the Agreement and this includes storing Protected Data that your Users upload to Upshot.

1.3 For the purposes of this Agreement you are a Controller and FFTL is a Processor.

1.4 The terms of this Agreement are to apply to all data processing carried out by FFTL on your behalf and to all Protected Data held by FFTL in relation to such processing, whether such Protected Data is processed at the date of the Agreement or received afterwards.

1.5 In relation to this Agreement:

1.5.1 The subject matter of the data processing is the use of Upshot by Delivery Organisations and Facilitating Organisations, as allowed by FFTL pursuant to this Agreement.

1.5.2 the duration of the data processing is from the Start Date specified in the Key Terms until the earlier of (i) this Agreement being terminated for any reason or (ii) you making a reasonable and lawful request in writing that FFTL stops processing the Protected Data.

1.5.3 the nature and purpose of the data processing is to allow Delivery Organisations and Facilitating Organisations to use Upshot for the purposes specified in this Agreement.

1.5.4 the types of Protected Data which may be stored within Upshot are:

(a) names;

(b) dates of birth;

(c) contact details;

(d) membership numbers;

(e) details of membership/employment with Delivery Organisations;

(f) details of sessions (for example training) attended by Attendees;

(g) information as to Attendees' gender;

(h) information as to Attendees' sexual orientation;

(i) information as to Attendees' racial/ethnic origin;

(j) information as to Attendees' religious or other beliefs of a similar nature;

(k) information as to Attendees' physical or mental health; and/or

(l) any other types of Protected Data (as defined in clause 4) which need to be processed in furtherance of the Agreement.

1.5.5 the categories of data subjects are Users and Attendees.

2. General obligations

2.1 Both parties shall comply at all times with their applicable obligations under Data Laws.

2.2 FFTL shall process Protected Data received from you or collected on your behalf in connection with the Agreement only on your documented instructions. These may be specific instructions or instructions of a general nature as set out in:

2.2.1 This Agreement (including this Schedule); or

2.2.2 As otherwise notified by the Facilitating Organisation(s) and/or the Delivery Organisation(s) to FFTL during the term of this Agreement.

2.3 FFTL shall inform you immediately if, in its opinion, an instruction issued pursuant to would result in either FFTL or you breaching the Data Laws.

2.4 FFTL agrees to comply with any reasonable measures required by you to ensure that its obligations under the Agreement are satisfactorily performed in accordance with the Data Laws and to provide reasonable assistance in ensuring compliance with the Controller's obligations concerning data security, security breach notification, data protection impact assessments and consulting with the Information Commissioner's Office ("ICO").

2.5 Where FFTL processes Protected Data on your behalf it shall:

2.5.1 process the Protected Data only to the extent, and in such manner, as is necessary in order to comply with/benefit from the Agreement or as is required by law or any regulatory body including but not limited to the ICO.

2.5.2 not process Protected Data outside the European Economic Area ("**EEA**") except that you hereby consent to FFTL using service providers located outside of the EEA [as listed in the Upshot Third Party Processors Schedule]. Where Protected Data is transferred outside the EEA under this Agreement, both Parties shall comply with the obligations imposed under the Data Laws to ensure an adequate level of protection to any Protected Data that is transferred (for instance, by entering into the European Commission approved Standard Contractual Clauses); and

2.5.3 not transfer or disclose any Protected Data provided to it by you to any third party or sub-contract any processing without your prior consent except that you hereby consent to the engagement of FFTL's service providers [as listed in the Upshot Third Party Processors Schedule] and FFTL shall ensure that any third party to which it may sub-contract any processing has entered into a

written contract with FFTL which (i) contains obligations that are at least as protective of Protected Data as those contained in this Agreement, (ii) permits both FFTL and you to enforce those obligations, (iii) is governed by UK law and (iv) automatically terminates upon termination of this Agreement.

3. Security measures

3.1 FFTL agrees to implement appropriate technical and organisational measures to protect the Protected Data uploaded to Upshot pursuant to this Agreement against a Security Breach in compliance with the obligations set out in the Data Laws, including, where appropriate:

3.1.1 the pseudonymisation and encryption of Protected Data;

3.1.2 ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;

3.1.3 restoring the availability and access to personal data in the event of a physical or technical incident; and

3.1.4 regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring security of the processing.

3.2 If reasonably requested by you, within a reasonable timeframe FFTL will supply details to you of the technical and organisational systems in place to safeguard the security of the Protected Data held and to prevent unauthorised access to it and otherwise make available to you all information necessary to demonstrate compliance with the obligations stipulated in this Agreement and/or the Data Laws.

3.3 On reasonable prior notice but on not less than 72 (seventy two) hours, permit persons authorised by you to enter into any premises on which Protected Data provided by/via you to FFTL is processed (provided that FFTL owns or controls access to such premises) and to inspect FFTL's systems to ensure that adequate security measures are in place.

3.4 FFTL shall maintain security measures to a standard appropriate to:

3.4.1 the harm that might result from unlawful or unauthorised processing or accidental loss, damage or destruction of the Protected Data; and

3.4.2 the nature of the Protected Data.

3.5 In particular FFTL shall:

3.5.1 have in place and comply with an appropriate security policy;

3.5.2 ensure that appropriate security safeguards and virus protections are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;

3.5.3 prevent unauthorised access to the Protected Data;

3.5.4 ensure its storage of Protected Data conforms with industry practice such that the media on which Protected Data is recorded (including paper records and

records stored electronically) are stored in secure locations and access by personnel to Protected Data is strictly monitored and controlled;

3.5.5 have secure methods in place for the transfer of Protected Data;

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

3.5.7 take reasonable steps to ensure the reliability of any employees or other individuals who have access to the Protected Data;

3.5.8 ensure that any employees or other individuals required to access the Protected Data are informed of its confidential nature and comply with the obligations set out in this Schedule;

3.5.9 ensure that none of the employees or other individuals who have access to the Protected Data publish, disclose or divulge any of it to any third party unless directed in writing to do so by you;

3.5.10 have in place appropriate methods for detecting and dealing with a Security Breach;

3.5.11 have a secure procedure for backing up and storing back-ups separately from originals;

3.5.12 have an appropriate system in place to ensure that access to the Protected Data can be restored in a timely manner in the event of any physical or technical incident;

3.5.13 implement an effective system of regularly testing, assessing and evaluating the effectiveness of the measures used to ensure the security of the processing carried out under this Agreement; and

3.5.14 have a secure method of disposal, deletion or destruction of Protected Data required by you, including for back-ups, disks, print outs and redundant equipment.

4. Complaints and rights of data subjects

4.1 FFTL shall:

4.1.1 notify you (within five working days) if it receives:

(a) a request or complaint from a data subject concerning Protected Data; or

(b) a complaint or request relating to your obligations under the Data Laws;

4.1.2 provide you with reasonable co-operation and assistance in relation to any such complaint or request made, including by:

(a) providing details of any additional information as you may reasonably request;

(b) taking all steps necessary to enable you to respond to a request or complaint from a data subject within the relevant timescale set out in the GDPR and in accordance with your reasonable instructions;

(c) providing you with any Protected Data FFTL holds in relation to a data subject (within reasonable timescales required by you);

(d) using appropriate technical and organisational measures as far as this is possible, to assist you in responding to requests from data subjects to exercise their rights; and

(e) ensuring that (other than as set out above) no reply or other communication is made in response to such complaint or request unless approved by you except to the extent necessary to ensure compliance with the Data Laws.

5. **Notification of a Security Breach**

5.1 FFTL shall notify you as soon as reasonably possible after any Security Breach occurs and in any event no later than 36 hours after becoming aware of the Security Breach, and shall include in that notification a description of:

5.1.1 the nature of the Security Breach including details of the nature of the Protected Data affected, and the data subjects affected;

5.1.2 the likely consequences of the Security Breach; and

5.1.3 the measures taken or proposed to be taken by FFTL to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6. Confidentiality

6.1 All Protected Data provided to FFTL by you or obtained by FFTL in the course of work with you/carried out on your behalf shall be treated as confidential and may not be copied, disclosed or processed in any way without your express authority or as required by law or any regulatory body. All FFTL personnel processing Protected Data shall be committed to this confidentiality obligation.

6.2 FFTL agrees that on termination of this Agreement or in the event that it is notified by you that it is not required to process Protected Data, FFTL shall either (i) transfer a copy of all Protected Data held by it in relation to this Agreement to you in a format reasonably requested by you and/or, (ii) at your request, delete or destroy all such Protected Data using a secure method which ensures that it cannot be accessed by any third party and shall provide you with a written confirmation of secure deletion/destruction.

6.3 For the avoidance of doubt, FFTL's compliance with the obligation under Clause 6.2 shall be without prejudice to legal and regulatory requirements on FFTL to retain Protected Data.