DATA PROCESSING ADDENDUM (v1.0)

Progressive Voice Services Limited trading as Meetupcall of Premier House, Carolina Court, Doncaster, DN45RA **("Meetupcall")** and _____ having its place of business at _____, **("Customer")** have entered into the Meetupcall Customer Agreement (including by accepting Meetupcall's terms and conditions online), the **"Agreement"**, under which Meetupcall has agreed to provide the Service and related technical support to Customer.

This Data Protection Addendum **("Addendum"**) will be effective and replace any previously applicable data protection addendum as from the Addendum Effective Date (as defined below).

If you are signing this Addendum on behalf of Customer, you represent and warrant that:

(i) you have full legal authority to bind your employer, or the applicable entity, to these Terms;
(ii) you have read and understand this Addendum; and
(iii) you agree, on behalf of the party you represent, to this Addendum.

Introduction

This Addendum sets out terms that apply to Meetupcall's Processing of Customer Data (including without limitation Personal Data) under the Agreement.

1. Definitions

a. **"Addendum Effective Date"** means the date on which Customer signed this Addendum.

b. **"Adequate Country"** means a country which is deemed adequate by the European Commission under Article 25(6) of Directive 95/46/EC or Article 45 of GDPR.

c. **"Alternative Transfer Mechanism"** means an alternative data export solution for the lawful transfer of Customer Data (as recognised under EU Data Protection Law) outside the EEA.

d. **"Customer Data"** means any data submitted to Meetupcall by the Customer, or collected by Meetupcall on behalf of the Customer, connected with the provision and delivery of the Service and related technical support.

e. **“Data Controller”** means the party that determines the purposes and means of the Processing of Personal Data.

f. **“Data Processor”** means the party that Processes Personal Data on behalf of, or under the instruction of, the Data Controller.

g. **“Data Protection Authority”** means the competent body in the jurisdiction charged with enforcement of applicable Data Protection Law.

h. **“Data Protection Laws”** means with respect to a party, all privacy, data protection, information security-related and other laws and regulations applicable to such party, including, where applicable, EU Data Protection Law.

i. **“Data Subject”** means the identified or identifiable person who is the subject of Personal Data.

j. **“EEA”** means the European Economic Area, United Kingdom and Switzerland.

k. **“EU Data Protection Law”** means (i) prior to 25th May 2018, European Union Directive 95/46/EC; and (ii) on and after 25th May 2018, European Union Regulation 2016/679 (“GDPR”).

l. References to **“instructions”** or **“written instructions”** and related terms mean Data Controller’s instructions for Processing of Customer Data, which consist of (1) the terms of the Agreement and this Addendum, (2) Processing enabled by Data Controller through the Service, and (3) other reasonable written instructions of Data Controller consistent with the terms of the Agreement.

m. **“Model Contracts”** means the Standard Contractual Clauses for Processors as approved by the European Commission under Decision 2010/87/EUin the form

n. **“Processing”** has the meaning given to it in the applicable EU Data Protection Law and “process”, “processes” and “processed” will be interpreted accordingly.

o. **“Personal Data”** means any information included in the Customer Data relating to an identified or identifiable natural person; an identifiable person is one who can be identified , directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

p. **“Security Incident”** means any unauthorised or unlawful confirmed breach of security that leads to the accidental or unlawful destruction,

loss, alteration, unauthorised disclosure of or access to Personal Data in Data Processor’s control.

q. **“Sensitive Data”** means Personal Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

r. **“Subprocessor”** means any Third Party engaged by Data Processor or its affiliates to process any Customer Data pursuant to the Agreement or this Addendum.

s. **“Third Party”** shall mean any natural or legal person, public authority, agency or any otherbody other than the Data Subject, Data Controller, Data Processor, or Subprocessors or other persons who, under the direct authority of the Data Controller or Data Processor, are authorised to Process the data.

t. Other capitalised terms not defined herein have the meanings given in the Agreement.

2. General Termination

a. This Addendum forms part of the Agreement and except as expressly set forth in this Addendum, the Agreement remains unchanged and in full force and effect. If there is any conflict between this Addendum and the Agreement, this Addendum shall prevail to the extent of that conflict in connection with the Processing of Customer Data.

b. All activities under this Addendum (including without limitation Processing of Customer Data) remain subject to the applicable limitations of liability set forth in the Agreement.

c. Data Controller agrees that any regulatory fines or penalties incurred by Data Processor in relation to the Customer Data that arise as a result of, or in connection with, Data Controller’s failure to comply with its obligations under this Addendum or any applicable Data Protection Laws shall count toward and reduce Data Processor's liability under the Agreement as if it were liability to Data Controller under the Agreement.

d. This Addendum will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

e. This Addendum will automatically terminate upon expiration or termination of the Agreement.

3. Scope and Applicability of this Addendum

a. This Addendum applies where and to the extent that Meetupcall processes Customer Data that is subject to EU Data Protection Law on behalf of Customer in the course of providing the Service pursuant to the Agreement, as detailed at Appendix A.

b. Part A (being Sections 5-11 (inclusive) as well as Appendixes A and B of this Addendum) shall apply to the processing of Customer Data within the scope of this Addendum from the Addendum Effective Date.

c. Part B (being Sections 12-14 (inclusive) of this Addendum) shall apply to the processing of Customer Data within the scope of this Addendum from and including 25th May 2018. For the avoidance of doubt, Part B shall apply in addition to, and not in substitution for, the terms in Part A.

Part A: General Data Protection Obligations

5. Role and Scope of the Processing

a. Customer will act as the Data Controller and Meetupcall will act as the Data Processor under this Addendum. Both Customer and Meetupcall shall be subject to applicable Data Protection Laws in the carrying out of their responsibilities as set forth in this Addendum.

b. Customer retains all ownership rights in the Customer Data, as set forth in the Agreement. Except as expressly authorised by Customer in writing or as instructed by Customer, Meetupcall shall have no right directly or indirectly to sell, rent, lease, combine, display, perform, modify, transfer or disclose the Customer Data or any derivative work thereof. Meetupcall shall act only in accordance with Customer's instructions regarding the Processing of the Customer Data except to the extent prohibited by applicable Data Protection Laws.

c. Additional instructions not consistent with the scope of the Agreement require prior written agreement of the parties, including agreement on any additional fees payable by Customer.

d. Notwithstanding the above, Customer acknowledges that Meetupcall shall have a right to use Aggregated Anonymous Data as detailed in the Agreement.

e. Meetupcall shall not disclose the Customer Data to any Third Party in any circumstances other than in compliance with Customer’s instructions or in compliance with a legal obligation to disclose. Meetupcall shall inform Customer in writing prior to making any such legally required disclosure, to the extent permitted by Data Protection Laws.

f. Customer agrees it will not submit any Sensitive Data to the Service and acknowledges that Meetupcall makes no special provisions to support the processing of Sensitive Data.

6. Subprocessing

a. Customer agrees that Meetupcall is authorised to use Subprocessors (including without limitation cloud infrastructure providers) to Process the Personal Data, provided that Meetupcall:

(i) enters into an agreement with any Subprocessor, imposing data protection obligations substantially similar to this Addendum; and

(ii) remains liable for compliance with the obligations of this Addendum and for any acts or omissions of the Subprocessor

that cause Meetupcall to breach any of its obligations under this Addendum.

b. Information about Subprocessors, including their functions and locations, is available at: https://www.meetupcall.com/subprocessors (as may be updated by Meetupcall from time to time in accordance with this Addendum).

7. Security

a. Meetupcall shall implement and maintain appropriate technical and organisational security measures to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Personal Data, in accordance with Meetupcall's security standards described in Appendix B (“Security Measures”).

b. Customer is responsible for reviewing the information made available by Meetupcall relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and that Meetupcall may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service purchased by Customer.

8. Onward Transfer

a. Meetupcall may, subject to complying with this Section 8, store and process Customer Data anywhere in the world where Meetupcall, its affiliates or Subprocessors maintain data processing operations.

b. To the extent that Meetupcall processes any Personal Data protected by GDPR and/or originating from the EEA in the United States or another country outside the EEA that is not designated as an Adequate Country, then the parties shall sign the Model Contracts.

c. The parties agree that Meetupcallis the “data importer” and Customer is the “data exporter” under the Model Contracts (not withstanding that Customer may be an entity located outside of the EEA).

9. Regulatory Compliance

a. At Customer’s request and expense, Meetupcall shall reasonably assist Customer as necessary to meet its obligations to Data Protection Authorities.

b. Meetupcall shall (at Customer's expense) reasonably assist Customer to respond to requests from individuals in relation to their rights of data access, rectification, erasure, restriction, portability and objection. In the event that any such request is made directly to Meetupcall, Meetupcall shall not respond to such communication directly without Customer's prior authorisation unless required by Data Protection Laws.

10. Reviews of Data Processing

a. At Customer’s request, Meetupcall shall provide Customer with written responses to all reasonable requests for information made by Customer relevant to the Processing of Personal Data under this Addendum, including responses to security and audit questionnaires, in each case solely to the extent necessary to confirm Meetupcall’s compliance with this Addendum.

b. Except as expressly required by Data Protection Laws, any review under this Section will:

   (i) be conducted no more often than once per year during Meetupcall’s normal business hours, in a manner so as not to interfere with standard business operations;

   (ii) be subject to Meetupcall’s reasonable confidentiality and security constraints;

   (iii) be conducted at Customer’s expense; and

   (iv) not extend to any information, systems or facilities of Meetupcall’s other customers or its Third Party infrastructure providers.

c. Any information provided by Meetupcall under this Section 10 constitutes Meetupcall’s Confidential Information under the Agreement.

11. Return or deletion of data

a. Upon request by Customer at the termination or expiration of the Agreement, Meetupcall shall, delete or return, at Customer's choice, all of the Personal Data from Meetupcall’s systems in accordance with our data retention policy. Within a reasonable period following deletion, at Customer’s request, Meetupcall will provide written confirmation that Meetupcall’s obligations of data deletion or destruction have been fulfilled.

b. Not withstanding the foregoing, Customer understands that Meetupcall may retain Customer Data as required by Data Protection Laws, which data will remain subject to the requirements of this Addendum.

c. Information on how long it takes us to delete or return data is published on our data retention policy at: *http://www.meetupcall.com/data-retention-policy* (as may be updated by Meetupcall from time to time in accordance with this Addendum).

Part B: GDPR Obligations from 25 May 2018

12. Additional Security

a. Upon becoming aware of a confirmed Security Incident, Meetupcall shall notify Customer as set out in the Security Measures.

13. Changes to Subprocessors

a. When any new Subprocessor is engaged, Meetupcall will, at least ten (10) calendar days before the new Subprocessor processes any Customer Data, inform Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) by sending an email to the Billing Email Address.

b. Customer may object in writing to Meetupcall's appointment of a new Subprocessor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If Meetupcall cannot provide an alternative Subprocessor, or the parties are not otherwise able to achieve resolution as provided in the preceding sentence, Customer, as its sole and exclusive remedy, may terminate the Agreement for convenience, on condition that Customer provides written notice to Meetupcall within five (5) calendar days of being informed of the engagement of the Subprocessor.

14. Further cooperation

a. Where and when required by Data Protection Laws, Meetupcall will provide the relevant Data Protection Authorities with information related to Meetupcall’s Processing of Personal Data. Meetupcall further agrees that it will maintain such required registrations and where necessary renew them during the term of this Addendum. Any changes to Meetupcall’s status in this respect shall be notified to Customer immediately.

b. To the extent Meetupcall is required under Data Protection Laws, Meetupcall shall (at Customer's expense) provide reasonably requested information regarding the Service or prior consultations with Data Protection Authorities to enable Customer to carry out data protection impact assessments.

15. **Indemnity**

a. If one party is held liable for a violation of this Addendum committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred in accordance with the provisions of the "Limitation of Liability" Section of the Agreement.

b. Each party's liability, taken together in the aggregate, arising out of or related to this Addendum whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement. For the avoidance of doubt, Meetupcall's total liability for all claims from the Customer or any third party arising out of or related to the Agreement and this Addendum shall apply in the aggregate for all claims under both the Agreement and this Addendum.

Executed for and on behalf of Meetupcall

Signed: ----------

Name: ----------

Role: ----------

Date: ----------

Executed for and on behalf of Customer

Signed: ----------

Name: ----------

Role: ----------

Date: ----------

Appendix A

Details of Processing Subject Matter: The subject matter of the data processing under this Addendum is the Customer Data.

Duration of the Processing: The duration of the data processing under this Addendum is until the termination of the Agreement plus the period from the expiry of the Agreement until deletion of all Customer Data by Meetupcall in accordance with the terms of the Addendum.

Nature and Purpose of the Processing: The purpose of the Processing under this Addendum is the provision of the Service to Customer and the performance of Meetupcall's obligations under the Agreement (including this Addendum) or as otherwise agreed by the parties.

Categories of Data: Data relating to individuals provided to Meetupcall via the Service by (or at the direction of) Customer. Customer Data does not contain any Sensitive Data as Customer is prohibited under this Addendum from submitting Sensitive Data to the Service. More details on categories of information can be found at: *http://www.meetupcall.com/data-we-collect*

Data Subjects: Data subjects include the individuals about whom data is provided to Meetupcall via use of the Service by (or at the direction of) Customer.

Appendix B

Security Measures Introduction

Meetupcall considers protection of Customer Data a top priority. As further described in these Security Measures, Meetupcall uses commercially reasonable organisational and technical measures designed to prevent unauthorised access, use, alteration or disclosure of Customer Data stored on systems under Meetupcall's control.

1. Access to Customer Data.

Meetupcall limits its personnel's access to Customer Data as follows:

a. Requires unique user access authorisation through secure logins and passwords, including individually-assigned Secure Socket Shell (SSH) keys for external engineer access;

b. Limits the Customer Data available to Meetupcall personnel on a "need to know" basis;

c. Restricts access to Meetupcall's production environment by Meetupcall personnel on the basis of business need; and

d. Encrypts user security credentials for production access.

2. Data Encryption.

Meetupcall provides industry-standard encryption for Customer Data both in transit and at rest as follows:

a. Customer Data is encrypted in transit and at rest;

b. Uses strong encryption methodologies to protect Customer Data, including AES 256-bit encryption for Customer Data stored in Meetupcall's production environment.

3. Data Management

a. Meetupcall logically separates each of its customers' data and maintains measures designed to prevent Customer Data from being exposed to or accessed by other customers.

4. Network Security, Physical Security and Environmental Controls

a. Meetupcall uses a variety of techniques designed to detect and/or prevent unauthorised access to systems processing Customer Data, including firewalls and network access controls.

b. Meetupcall maintains measures designed to assess, test and apply security patches to all relevant systems and applications used to provide the Service.

c. Meetupcall monitors privileged access to applications that process Customer Data, including cloud services.

d. The Service is hosted on and operates from only ISO27001 certified data centres.

5. Independent Security Assessments.

Meetupcall periodically assesses the security of its systems and the Service as follows:

a. Annual detailed security and vulnerability assessments of the Service conducted by independent third-party security experts.

b. Annual penetration testing of Meetupcall systems and applications to test for exploits including, but not limited to, XSS, SQL injection, access controls, and CSRF.

c. Monthly vulnerability scanning.

6. Incident Response.

If Meetupcall becomes aware of a Security Incident, Meetupcall will:

a. Take reasonable measures to mitigate the harmful effects of the Security Incident and prevent further unauthorised access or disclosure.

b. Upon confirmation of the Security Incident, notify Customer in writing of the Security Incident without undue delay. Notwithstanding the foregoing, Meetupcall is not required to make such notice to the extent prohibited by Laws, and Meetupcall may delay such notice as requested by law enforcement and/or in light of Meetupcall’s legitimate needs to investigate or remediate the matter before providing notice.

c. Each notice of a Security Incident will include: The extent to which Customer Data has been, or is reasonably believed to have been, used, accessed, acquired or disclosed during the Security Incident;

(ii) A description of what happened, including the date of the Breach and the date of discovery of the Security Incident, if known;

(iii) The scope of the Security Incident, to the extent known; and (iv) A description of Meetupcall 's response to the Security Incident, including steps Meetupcall has taken to mitigate the harm caused by the Security Incident.

7. Business Continuity Management

a. Meetupcall maintains processes to ensure failover redundancy with its systems, networks and data storage.

8. Personnel Management

a. Meetupcall performs employment verification, including proof of identity validation and criminal background checks for all new hires.

b. Meetupcall provides training for its personnel who are involved in the processing of the Customer Data to ensure they do not collect, process or use Customer Data without authorisation and that they keep Customer Data confidential.

c. Meetupcall conducts routine and random monitoring of employee systems activity.

d. Upon employee termination, whether voluntary or involuntary, Meetupcall immediately disables all access to critical and noncritical systems, including Meetupcall’s physical facilities.