GDPR Addendum

1. **Background**

1.1 We refer to the agreement between Chartbeat, Inc. and the undersigned ("**Customer")** for the provision of Chartbeat services, a copy of which is attached as Annex 1 to this letter (the "**Agreement**").

1.2 On 25 May 2018, the General Data Protection Regulation (Regulation (EU 2016/679) (the "**GDPR**") comes into effect. The GDPR regulates the processing of personal data, and introduces significant changes compared with existing European data protection legislation.

1.3 In particular, Article 28 of the GDPR specifies certain provisions which must be included in contracts between "controllers" and "processors" (as such terms are defined in the GDPR).

1.4 As a result, the parties wish to enter into this GDPR Addendum in order to amend the Agreement, with effect from and including the date of this letter (the "**Variation Date**").

2. **Variation**

2.1 In consideration of the mutual promises set out in this GDPR Addendum, with effect from the Variation Date, the parties agree to the following amendments to the Agreement:

(a) Annex 2 to this letter shall be inserted as a new Schedule to the Agreement and shall form a part of the Agreement.

(b) The provisions of Annex 2 shall replace any provisions in the Agreement which expressly conflict, or are inconsistent, with any provisions of Annex 2. If there is any ambiguity between the provisions of the Agreement (excluding the GDPR Addendum) and the GDPR Addendum, the provisions of the GDPR Addendum shall prevail.

2.2 Except as set out in this paragraph 2, the provisions of the Agreement shall remain unchanged and shall continue in force.

3. **Law and jurisdiction**

3.1 This letter and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and interpreted in accordance with the laws of New York.

3.2 The parties irrevocably agree that the courts of New York have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that arise out of, or in connection with, this letter or its subject matter or formation.

4. **Your agreement to this GDPR Addendum**

4.1 Please sign and return the enclosed copy of this letter to acknowledge your agreement to the GDPR Addendum and the variation of the Agreement.

4.2 If you do not sign and return the enclosed copy of this letter to us, or notify us in writing that you object to its terms, on or before June 30, 2018, we will proceed on the basis that you accept the provisions of the GDPR Addendum, and the variation of the Agreement, and that you are continuing your business relationship with us with that intention.

4.3 We look forward to continuing our business relationship with you.

Signed ……

For and on behalf of Chartbeat, Inc

We agree to the provisions of the GDPR Addendum and the variation of the Agreement with effect from the Variation Date on the terms set out above.

Signed ……

For and on behalf of: _____ (Legal Name of Customer)

Date ……

Annex 1

The Agreement

Annex 2

GDPR Addendum

1. **Definitions and interpretation**

1.1 In this Addendum, unless the context otherwise requires:

"Customer Personal Data" means all Personal Data processed by Chartbeat on behalf of the Customer under or in connection with this Agreement.

"Data Protection Laws" means any laws and regulations relating to privacy or the use or processing of data relating to natural persons, including: (a) EU Directives 95/46/EC and 2002/58/EC (as amended by 2009/136/EC) and any legislation implementing or made pursuant to such directives, including (in the UK) the Data Protection Act 1998 (the **"DPA"**) and the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (b) from 25 May 2018 , EU Regulation 2016/679 (**"GDPR"**); and (c) any laws or regulations ratifying, implementing, adopting, supplementing or replacing GDPR; and (d) any guidance or codes of practice issued by a governmental or regulatory body or authority in relation to compliance with the foregoing; in each case, to the extent in force, and as such are updated, amended or replaced from time to time.

"Data Controller" and "**Data Processor**" have the meanings set out in the DPA until 25 May 2018, and thereafter the meaning given to the term "controller" and "processor" (respectively) in Article 4 of GDPR.

"DP Regulator" means any governmental or regulatory body or authority with responsibility for monitoring or enforcing compliance with the Data Protection Laws.

"Data Subject Request" means a request from a Data Subject to exercise its rights under the Data Protection Laws in respect of that Data Subject's Personal Data.

"Permitted Region" means the United Kingdom and the European Economic Area.

"Security Breach" means any actual loss, unauthorised or unlawful processing, destruction, damage, or alteration, or unauthorised disclosure of, or access to the Customer Personal Data.

"Sub-Processor" means a subcontractor (including any affiliates of Chartbeat) appointed by Chartbeat to process Customer Personal Data.

1.2 In this Schedule, the terms **"Data Subject"**, **"Personal Data"**, **"process"**, **"processing"**, **"transfer"** (in the context of transfers of Personal Data) and **"technical and organisational measures"** shall have the meanings and otherwise be interpreted in accordance with the DPA until 25 May 2018, and thereafter the GDPR.

2. Compliance with Data Protection Laws

2.1 Chartbeat shall comply with its obligations under the Data Protection Laws as they apply to it as a Data Processor of the Customer Personal Data.

2.2 The Customer shall comply with its obligations under the Data Protection Laws as they apply to it as a Data Controller of the Customer Personal Data in order for Chartbeat to process the Personal Data as otherwise contemplated by this Agreement and in particular shall: (a) ensure that any instructions that it issues to Chartbeat shall comply with the Data Protection Laws;(b) have sole responsibility for the accuracy, quality and legality of the Customer Personal Data

(c) have established the legal basis for processing under Data Protection Laws; and (d) provided all notices and obtaining all consents as may be required under Data Protection Laws.

2.3 Each party shall maintain records of all processing operations under its responsibility that contain at least the minimum information required by the Data Protection Laws, and shall make such information available to any DP Regulator on request.

3. Processing and security

3.1 In performing its obligations under this Agreement, Chartbeat shall only process the types of Personal Data, and only in respect of the categories of Data Subjects, and only for the nature and purposes of processing and duration, as is set out below:

Subject matter of processing	Chartbeat processes information about visitors to your website in connection with the Service it provides to you and also processes your employee/user information in connection with their use of the Service.
Nature and purpose of processing	Chartbeat is processing data in order to help its Customer understand what is happening on the Customer Website at any given moment.
Categories of Personal Data	Site visitor IP addresses and randomly-generated user IDs stored in first party cookies on your domain. Your employees' user contact information.
Categories of data subjects	Visitors to the Customer Website. Employees/users of the Chartbeat Services.
Duration	For the duration of the Agreement and for 90 days after termination of performance of the Services under the Agreement.

3.2 In processing the Customer Personal Data as a Data Processor, Chartbeat shall:

(a) process Customer Personal Data only in accordance with the Customer's written instructions from time to time provided such instructions are lawful (including those set out in this Agreement) unless it is otherwise required by applicable law (in which case, unless such law prohibits such notification on important grounds of public interest, Chartbeat shall notify the Customer of the relevant legal requirement before processing the Customer Personal Data);

(b) notify the Customer as soon as reasonably practicable if it receives a Data Subject Request in respect of Customer Personal Data;

(c) provide the Customer with its full co-operation and assistance in relation to any Data Subject Request in respect of Customer Personal Data;

(d) not disclose any Customer Personal Data to any Data Subject which has requested the same except in relation to Customer Personal Data of which Chartbeat is also a Data Controlleror to a third party following such a request (including any subcontractor or affiliate) other than at the written request of the Customer or as expressly provided for in this Agreement;

(e) taking into account:

(i) the state of the art;

(ii) the nature, scope, context and purposes of the processing; and

(iii) the risk and severity of potential harm,

protect the Customer Personal Data by ensuring that it has in place appropriate technical and organisational measures, including measures to protect the Customer Personal Data against the risks of a Security Breach; and

(f) take commercially reasonable steps to ensure that only persons authorized by Chartbeat process Customer Personal Data and that such persons are (i) subject to binding obligations to maintain the confidentiality of the Customer Personal Data; and (ii) trained on both (1) the requirements of the Data Protection Laws, and (2) their obligations in respect of Customer Personal Data under this Agreement.

3.3 Chartbeat shall, without undue delay after discovering any Security Breach or any failure or defect in security which leads, or might reasonably be expected to lead, to a Security Breach (together a "**Security Issue**") notify the Customer of the same.

3.4 Where a Security Issue arises, Chartbeat shall:

(a) as soon as reasonably practicable, provide the Customer with full details of the Security Issue, the actual or expected consequences of it, and the measures taken or proposed to be taken to address or mitigate it;

(b) co-operate with the Customer, and provide the Customer with all reasonable assistance in relation to the Security Issue; and

(c) unless required by applicable law not make any notifications to a DP Regulator or any Data Subjects about the Security Issue without the Customer's prior written consent (not to be unreasonably withheld or delayed).

4. Return or destruction of Personal Data

4.1 Subject to paragraph 4.2, Chartbeat shall (at the Customer's option) except in relation to Customer Personal Data of which Chartbeat is also a Data Controller and except as required by law or in order to defend any actual or possible legal claims, as the Customer so directs, take reasonable steps to return or irretrievably delete all Customer Personal Data in its control or possession when it no longer requires such Customer Personal Data to exercise or perform its rights or obligations under this Agreement, and in any event on expiry or termination of this Agreement.

4.2 To the extent that Chartbeat is required by applicable law to retain all or part of the Customer Personal Data (the **"Retained Data"**), Chartbeat shall:

(a) cease all processing of the Retained Data other than as required by the applicable law;

(b) keep confidential all such Retained Data in accordance with Section 4 (Confidentiality); and

(c) continue to comply with the provisions of this Addendum in respect of such Retained Data.

5. Audit

5.1 Chartbeat shall permit the Customer or its representatives to access any relevant premises, personnel or records of Chartbeat on reasonable notice to audit and otherwise verify compliance with this Addendum, subject to the following requirements:

(a) the Customer may perform such audits no more than once per year or more frequently if required by Data Protection Laws;

(b) the Customer shall use a third party to perform the audit on its behalf, and such third party shall be professionally qualified and shall have executed a confidentiality agreement acceptable to Chartbeat before the audit;

(c) audits must be conducted during regular business hours, subject to Chartbeat's policies, and may not unreasonably interfere with Chartbeat's business activities and must be limited to Chartbeat's systems that contain Customer Personal Data;

(d) the Customer must provide Chartbeat with any audit reports generated in connection with any audit at no charge unless prohibited by applicable law. The Customer may use the audit reports only for the purposes of meeting its audit requirements under Data Protection Laws and/or confirming compliance with the requirements of this Addendum as they apply to Chartbeat's processing of Customer Personal Data;

(e) the audit reports shall be confidential;

(f) to request an audit, the Customer must first submit a detailed audit plan to Chartbeat at least 6 (six) weeks in advance of the proposed audit date. The audit must describe the proposed scope, duration and start date of the audit. Chartbeat will review the audit plan and inform the Customer of any concerns or questions (for example, any request for information that could compromise Chartbeat's confidentiality obligations or its security, privacy, employment or other relevant policies). Chartbeat will work cooperatively with the Customer to agree a final audit plan;

(g) nothing in this paragraph 5 shall require Chartbeat to breach any duties of confidentiality owed to any of its clients, employees or Third Party Providers; and

(h) all audits are at the Customer's sole cost and expense;

6. Co-operation and assistance

6.1 Chartbeat shall promptly co-operate with the Customer, and provide such information and assistance as the Customer may reasonably require, to enable the Customer to:

(a) comply with the Customer's obligations under the Data Protection Laws (including Articles 32-36 of GDPR in respect of Customer Personal Data; and

(b) deal with and respond to all investigations and requests for information relating to the Customer Personal Data from any DP Regulator.

6.2 If Chartbeat receives any complaint, notice or communication from a DP Regulator or other third party (excluding a Data Subject Request) which relates directly or indirectly to Customer Personal Data or to either party's compliance with the Data Protection Laws, it shall notify the Customer as soon as reasonably practicable.

7. Sub-Processors

7.1 The Customer generally agrees that Chartbeat may engage Third Party Providers including any advisers, contractors, or auditors to Process Personal Data ("**Sub-Processors**").

7.2 If Chartbeat engages a new Sub-Processor ("**New Sub-Processor**"), Chartbeat shall inform the Customer of the engagement by sending an email notification to the Customer and the Customer may object to the engagement of such New Sub-Processor by notifying Chartbeat within 5 Business Days of Chartbeat's email, provided that such objection must be on reasonable, substantial grounds, directly related to such New Sub-Processor's ability to comply with substantially similar obligations to those set out in this Addendum. If the

Customer does not so object, the engagement of the New Sub-Processor shall be deemed accepted by the Customer.

7.3 Chartbeat shall ensure that its contract with each New Sub-Processor shall impose obligations on the New Sub-Processor that are materially equivalent to the obligations to which Chartbeat is subject to under in this Data Processing Addendum.

7.4 Any sub-contracting or transfer of Personal Data pursuant to this paragraph 7 shall not relieve Chartbeat of any of its liabilities, responsibilities and obligations to the Customer under this Agreement and Chartbeat shall remain liable for the acts and omissions of its Sub-Processor.

8. Transfer of Personal Data

Unless the transfer is based on an "adequacy decision", is otherwise "subject to appropriate safeguards" or if a "derogation for specific situations" applies, each within the meanings given to them in Articles 45, 46 and 49 of the GDPR respectively, Chartbeat shall not transfer, access or process such Personal Data outside the Permitted Region.