Data Processing Addendum

(European Union GDPR April 2023)

This Data Processing Addendum ("DPA") forms part of the Buzzspark Terms and Conditions (https://buzzspark.io/terms), the Buzzspark Privacy Policy (https://buzzspark.io/privacy) and any other written or electronic agreement by and between Buzzspark and its affiliates (collectively, "Buzzspark Limited" referred to herein as "Buzzspark") and the undersigned customer of Buzzspark ("Customer") for the purchase of online services ("Services") from Buzzspark (the "Agreement") to reflect the parties' agreement with regard to the Processing of Personal Data.

How to execute this DPA

1. To complete this DPA, Customer must
    a. Complete the information and sign as customer on page 9;
    b. Complete the information and sign as the data exporter on pages 11, 19 and 21;
    c. Complete the information as data exporter on page 20.
    d. Send the completed and signed DPA to Buzzspark by email, indicating the email address associated with your Buzzspark account, to dpo@buzzspark.io.

2. Upon receipt by Buzzspark of signed DPA from Customer, Buzzspark will sign this DPA and send to the Customer the completed and signed DPA.

3. Upon receipt by the Customer of the signed DPA via email, this DPA will become legally binding.

Data Processing Terms

In the course of providing the Services to Customer pursuant to the Agreement, Buzzspark may Process Personal Data on behalf of Customer. Both Buzzspark and Customer agree to comply with the following provisions with respect to any Personal Data submitted by or for Customer to Buzzspark or collected and processed by or for Customer using Buzzspark Services.

In connection with the Service, the parties anticipate that Buzzspark may process outside of the European Economic Area ("EEA") and United Kingdom, Personal Data in respect of which the Customer or any member of the Customer Group may be a data controller under applicable EU Data Protection Laws.

1. Definitions

1.1. In this DPA, the following terms shall have meanings set below and cognate terms shall be constructed accordingly:

1.1.1. “Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.1.2. “Applicable Laws” means (a) European Union, the European Economic Area or member state, Switzerland and the United Kingdom, laws with respect to any Customer Personal Data in respect of which any Customer Group Member is subject to EU Data Protection Laws and Regulations; and (b) any other applicable law with respect to any Customer Personal Data in respect of which any Customer Group Member is subject to any other Data Protection Laws and Regulations;

1.1.3. “Customer Group” means Customer and any of Customer’s Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area (“EEA”) and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Buzzspark, is not a “Customer” as defined under the Agreement.

1.1.4. “Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

1.1.5. “Customer Data” means what is defined in the Agreement as “Your Data” or “Your Original Data.”

1.1.6. “Data Protection Laws and Regulations” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, and, to the extent applicable, the data protection or privacy laws of any other country applicable to the Processing of Personal Data under the Agreement.

1.1.7. “Data Subject” means the identified or identifiable person to whom Personal Data relates.

1.1.8. “GDPR” means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the

processing of personal data and on the free movement of such data.

1.1.9. "Party" means either the Data Processor or Data Controller, and "parties" means both the Data Processor and Data Controller.

1.1.10. "Personal Data" means any information about a natural person that is identified or identifiable to the natural person, either alone or in combination with other information, that Buzzspark will process or have access to as part of providing the Services, including any such information that is created by means of the Services.

1.1.11. "Personal Data Breach" means 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.

1.1.12. "Processing" means any operation or set of operations which is performed upon Personal Data, including such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data.

1.1.13. "Processor" means the entity which Processes Personal Data on behalf of the Controller.

1.1.14. "Service Data" means any electronic data, communications or other materials, including Personal Data, which is collected, stored, transmitted or otherwise processed via Buzzspark Services, by, or on behalf of, Customer and Customer's Authorised Users.

1.1.15. "Standard Contractual Clauses" means the clauses attached hereto as Schedule 2 pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

1.1.16. "Subprocessor" means any Processor engaged by Buzzspark.

1.2. The terms, "Commission", "Member State", and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Personal Data

2.1. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data when using the Services provided by Buzzspark, Customer is the Controller, Buzzspark is the Processor and that Buzzspark will engage Subprocessors pursuant to the requirements set forth in Section 5 “Subprocessors” below.

2.2. Customer’s Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3. Buzzspark’s Processing of Personal Data. Buzzspark shall treat Personal Data as Confidential Information and shall Process Personal Data in a manner compliant with Data Protection Laws and Regulations and the requirements regarding the collection, use and retention of Personal Data of Data Subjects. Buzzspark will only process Personal Data to the extent necessary to perform the Services in accordance with the Agreement and in accordance with Customer’s written instructions.

2.4. Details of the Processing. The subject-matter of Processing of Personal Data by Buzzspark is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

3. Rights of Data Subjects

3.1. Data Subject Request. Buzzspark shall promptly notify Customer if Buzzspark receives a request from a Data Subject to exercise their rights under the Data Protection Laws and Regulations with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable). Taking into account the nature of the request, Buzzspark shall assist Customer by appropriate technical and organisational measures, to the extent legally required, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations provided that: (a) Customer has instructed Buzzspark in writing to do so, and (b) Customer reimburses Buzzspark for the costs arising from this assistance. Failing such action by Customer to comply with the requests of the Data Subject, Buzzspark may at its own discretion fulfil the request, insofar as possible, within a

reasonable time.

4. Buzzspark Personnel and Confidentiality

4.1. Confidentiality. Buzzspark shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and Service Data and have received appropriate training on their responsibilities.

4.2. Reliability. Buzzspark shall take commercially reasonable steps to ensure the reliability of any Buzzspark personnel who may have access to the Customer Personal Data or Service Data or Buzzspark personnel who may be engaged in the Processing of Personal Data.

4.3. Limitation of Access. Buzzspark shall ensure that Buzzspark's access to Personal Data and Service is limited to those Buzzspark personnel who need to know/access the relevant Personal Data and Service Data while performing Services in accordance with the Agreement.

4.4. Data Protection Officer. Buzzspark has appointed a data protection officer, who can be reached at dpo@buzzspark.io.

5. Subprocessors

5.1. Appointment of Subprocessors. Customer acknowledges and agrees that Buzzspark may engage third-party Subprocessors in connection with the provision of the Services. Buzzspark has entered into a written agreement with each Subprocessor imposing on the Subprocessor the same obligations that apply to Processor with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Subprocessor under this Agreement.

5.2. List of Current Subprocessors. Buzzspark shall make available to Customer the current list of Subprocessors for the Services identified in Schedule 3 (List of Current Subprocessors).

5.3. Notification of New Subprocessors. Customer may find on Buzzspark's Privacy Policy page (https://buzzspark.io/privacy), a mechanism to subscribe to notifications of new Subprocessors for the Services, to which Customer may subscribe. If Customer subscribes, Buzzspark shall provide notification of a new Subprocessor(s) before authorising any new Subprocessor(s) to Process Personal Data in connection with the provision of the Services. Notification will be supplied in the form of an email to the email address submitted when subscribing for notification alerts at https://buzzspark.io/privacy.

5.4. Objection Right for New Subprocessors. Customer may object to Buzzspark's use of a new Subprocessor by notifying Buzzspark promptly in writing (via an email to dpo@buzzspark.io) within fifteen (15) business days after receipt of Buzzspark's notice sent in accordance with the mechanism set out in Section 5.3.

5.5. In the event Customer objects to a new Subprocessor, as permitted in the preceding sentence, the objection must be based on reasonable grounds (e.g. if the Controller proves that significant risks for the protection of its Personal Data exist at the Subprocessor). If Buzzspark and Customer are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party. Customer shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

5.6. Liability. Where the Subprocessor fails to fulfil its data protection obligations, Buzzspark will remain liable to the Customer for the performance of such Subprocessor's obligations.

6. Ownership of Service Data

6.1. As between Customer and Buzzspark, Customer retains all right, title and interest in and to the Personal Data collected through use of the Service.

7. Security & Audit

7.1. Controls for the Protection of Customer Data. Buzzspark will implement and maintain the technical, physical, administrative and organisational measures to protect personal data against theft, unauthorised or unlawful acquisition, access, or processing, accidental loss, destruction, alteration, or damage as described in Schedule 2 - Appendix 2 of the DPA, as well as any other minimum security requirements required by laws generally applicable to Processors. Buzzspark will not materially decrease the overall security of the Services during a Subscription Term.

7.2. Buzzspark shall keep and provide to Customer on request a record of Personal Data and processing activities and shall make available to Customer all information necessary (and allow for and contribute to audits or inspections) to demonstrate compliance with Buzzspark's data processing obligations set out in this Agreement. Customer shall be responsible for any costs arising from Buzzspark's contribution to any such audits or inspections, which shall be limited to one per year unless otherwise required by a supervisory authority.

8. Breach of Personal Data Security

8.1. After becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Buzzspark or its Subprocessors of which Buzzspark becomes aware (a "Customer Data Incident"), Buzzspark shall notify Customer without undue delay, within forty-eight (48) hours. Buzzspark shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Buzzspark deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Buzzspark's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Authorised Users.

8.2. Buzzspark's notice shall include the following information to the extent it is reasonably available to Buzzspark at the time of the notice, and Buzzspark shall update its notice as additional information becomes reasonably available:

8.2.1. the dates and times of the Customer Data Incident;

8.2.2. the facts that underlie the discovery of the Customer Data Incident;

8.2.3. a description of the Personal Data involved in the Customer Data Incident; and

8.2.4. the measures planned or underway to remedy or mitigate the vulnerability giving rise to the Customer Data Incident.

9. Data Protection Impact Assessment and Prior Consultation

9.1. Upon Customer's request, Buzzspark shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of any Customer Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Laws and Regulations, in each case solely in relation to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Buzzspark.

10. Return or Destruction of Service and Company Personal Data

10.1. On termination of the Services Agreement upon the deletion of an account ("Termination of Service"), or on Customer's written request at any time, Buzzspark shall destroy any Service Data that is within its control.

10.2. Prior to the Termination of Service, Customer may export Service Data as a CSV file via their account or request Buzzspark provide such export of Service Data.

10.3. Upon deletion of any user account or Aggregated Data by the Customer or Customer's Authorised Users via the Service that contains Personal Data collected by Customer through the Service, such Service Data is destroyed within thirty (30) days.

10.4. Subject to Section 10.5, Customer may in its absolute discretion by written notice via email to Buzzspark at dpo@buzzspark.io within seven (7) days of the Termination of Service require Buzzspark to (a) return a complete copy of all Customer Personal Data to Customer; and (b) delete and procure the deletion of all other copies of Customer Personal Data Processed by Processor and any Subprocessor.

10.5. Processor and Subprocessors employed by Buzzspark may retain Customer 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 Buzzspark shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

11. Data Transfers

11.1. In connection with the Services, the parties acknowledge that Buzzspark's Services environment is located in the United Kingdom in respect of which the Customer or any member of the Customer Group may be a data controller, under applicable Data Protection Laws and Regulations.

11.2. Transfers outside of Europe. In connection with the Service, the parties anticipate that Buzzspark may transfer or authorise the transfer of Personal Data to countries outside the European Economic Area ("EEA"), Switzerland and United Kingdom and Process Personal Data in respect of which the Customer or any member of the Customer Group may be a data controller, under applicable Data Protection Laws and Regulations.

12. Miscellaneous

12.1. GDPR. Buzzspark will Process Personal Data in accordance with the GDPR requirements directly applicable to Buzzspark's provision of its Services.

12.2. Legal effect. This DPA shall only become legally binding between Customer and Buzzspark when the steps set out in the Section "How To Execute This DPA" above have been fully completed.

12.3. Modification of DPA. This DPA may not be amended or modified except through a written Agreement signed by both Parties hereto.

12.4. Duration. The DPA will remain in force as long as Buzzspark Processes Personal Data on behalf of Customer under the Agreement.

List Of Schedules

Schedule 1: Details of the Processing
Schedule 2: Standard Contractual Clauses
Schedule 3: List of Current Subprocessors and their Locations

The parties' authorised signatories have duly executed this Agreement:

Customer

Signature: _____

Company Name: _____

Print Name: _____

Title: _____

Date: _____

Buzzspark

Signature: _____

Company Name: _____

Print Name: _____

Title: _____

Date: _____

SCHEDULE 1 – Details Of The Processing

Nature and Purpose of Processing
Buzzspark will Process Personal Data as necessary to perform the Services pursuant to the Agreement.

Duration of Processing
Subject to Section 10 of the DPA, Buzzspark will Process Personal Data for the duration of the Agreement.

Categories of Data Subjects
The personal data transferred concern the following categories of data subjects:

- Data Exporter's individuals who have been nominated by the Data Exporter to manage the Buzzspark Services (user accounts)

- Individuals who have created User Generated Content that has been aggregated by the Buzzspark Services, either via direct submission or from a public source (content creators), where Buzzspark Services have been used to provide user generated content management services.

Type of Personal Data
The personal data transferred concern the following categories of data:

The following categories of personal data will be stored by Buzzspark when storing User Accounts:

- First Name
- Last Name
- Display Name
- Email Address
- Password encrypted hash
- Timezone (Geo-Data)
- Last known IP Address

The following categories of personal data may be stored by Buzzspark when storing Content Creators:

- Source ID (Unique ID from Content Source)
- Source User Handle
- Source Username
- Latitude / Longitude (Geo-Data)

As not all public sources contain the above information, the actual content stored may be less than what is listed above. In addition to aforementioned, additional personal data may be stored by Buzzspark as defined by Data Importer when configuring the Buzzspark Services to collect additional data in its use of Buzzspark as a user generated content platform.

SCHEDULE 2: 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.

Data Exporter: _____

Address: _____

_____

Tel.: _____

Email: _____

(the data exporter)

And

Data Importer: _____

Address: _____

_____

Tel.: _____

Email: _____

(the data importer)

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

HAVE AGREED on the Contractual Clauses (the Clauses) found in schedule 2 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;

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;

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

a. 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.

b. 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.

c. 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.

d. 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;

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

a. 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.

b. 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 of 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.

c. 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

a. 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:

i. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

ii. to refer the dispute to the courts in the Member State in which the data exporter is established.

b. 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

a. 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.

b. 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.

c. 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

a. 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.

b. 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.

c. 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.

d. 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

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.

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 : _____

Position: _____

Address: _____

_____

Signature _____

On behalf of the data importer:

Name : _____

Position: _____

Address: _____

_____

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: _____
Data exporter operates:
(briefly specify your activities relevant to the transfer)

_____

_____

_____

Data importer
The data importer is: Buzzspark Limited

Data importer is a provider of user generated content platform as a Software as a Service (SaaS).

Data subjects
The personal data transferred concern the following categories of data subjects:

- Data Exporter's individuals who have been nominated by the Data Exporter to manage the Buzzspark Services (user accounts)

- Individuals who have created User Generated Content that has been aggregated by the Buzzspark Services, either via direct submission or from a public source (content creators), where Buzzspark Services have been used to provide user generated content management services.

Categories of data
The personal data transferred concern the following categories of data:

The following categories of personal data will be stored by Buzzspark when storing User Accounts:

- First Name
- Last Name
- Display Name
- Email Address
- Password encrypted hash
- Timezone (Geo-Data)
- Last known IP Address

The following categories of personal data may be stored by Buzzspark when storing Content Creators:

- Source ID (Unique ID from Content Source)
- Source User Handle
- Source Username
- Latitude / Longitude (Geo-Data)

As not all public sources contain the above information, the actual content stored may be less than what is listed above.

In addition to aforementioned, additional personal data may be stored by Buzzspark as defined by Data Importer when configuring the Buzzspark Services to collect additional data in its use of Buzzspark as a user generated content platform.

Special categories of data (if appropriate)
Buzzspark will not be processing any special categories of data.

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

The data importer will host and process Personal Data in the course of providing its Services to data exporter pursuant to the Agreement.

DATA EXPORTER

Name : _____

Position: _____

Signature _____

DATA IMPORTER

Name : _____

Position: _____

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):

Buzzspark currently observes the security practices described in this Appendix 2. Notwithstanding any provision to the contrary otherwise agreed to by Data Exporter, Buzzspark may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalised terms not otherwise defined herein shall have the meanings as set forth in the Buzzspark Terms and Conditions.

1. Access Control

Physical and environmental security:
Your Data collected via Buzzspark Services is stored on our servers, which are located in London, United Kingdom. Buzzspark uses data centers that are PCI-DSS compliant and meet the ISO/IEC 27001:2013 Information Security Management and ISO 9001:2015 Quality Management standards.

These data centers feature steel perimeter fencing, swipe card access with access recorded, CCTV with minimum 45-day retention, intrusion alarm systems and 24x7 environment monitoring with engineers on standby to deal with any alerts.

Authentication:
Buzzspark has implemented a uniform password policy for Buzzspark Services. Customers interacting with the Buzzspark Services via the user interface must authenticate before accessing non-public data or services.

Buzzspark employees do not have access to user account passwords. If a password is forgotten or otherwise lost, users are required to reset their passwords using industry standard methods.

Authorisation:
Your Data is stored in storage systems accessible to Customers via only application user interfaces and application programming interfaces. Your Data is kept safe and separate from data of other Customers via access controls. Customers are not allowed direct access to the underlying application infrastructure. The authorisation model in each of Buzzspark Services is designed to ensure that only the appropriately assigned individuals can access relevant features and data sets. Authorisation to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access is via an API key generated via Oauth.

A limited subset of Buzzspark employees have access to Buzzspark Services and to customer data via controlled interfaces. This access is limited to an as needs basis to allow the Buzzspark employees to provide effective customer support, to troubleshoot potential problems, and to detect and respond to security incidents. Employees are granted access by role, with privilege grants and roles reviewed regularly.

Buzzspark employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

Preventing Unauthorised Access
Buzzspark implements industry standard access controls for the internal networks that support Buzzspark Services. Network access control mechanisms are designed to prevent network traffic using unauthorised ports or protocols from reaching the Buzzspark Services infrastructure.

Buzzspark has implemented an Intrusion Detection and Prevention solution to protect all access to all Buzzspark Services. Buzzspark login pages include brute-force attack protection.

2. Transmission Control

In-transit Data
Buzzspark enforces HTTPS encryption (also referred to as SSL or TLS) on every one of its login, user interface pages and all other pages comprising the Buzzspark Services. HTTPS implementation uses industry standard algorithms and certificates.

At-rest Data
Buzzspark stores hashed user passwords as per industry standard practices for security.

3. PCI-DSS

Buzzspark payment systems meet the Payment Card Industry (PCI) Data Security Standard, and data is stored on PCI compliant servers. Buzzspark may store the last 4 digits of a Customer's credit card to assist with identifying the Customer account for subscription purposes. Full credit card data is stored securely with our PCI-compliant payment provider.

4. Personal Data Breach Protocol

If a personal data breach is detected, Buzzspark will take appropriate steps to minimise damage to Buzzspark Services and Customers or unauthorised disclosure.

Buzzspark will notify its affected Customers without undo delay. Buzzspark's personal data breach notice will include as information that is available at the time of the notice. To the best of Buzzspark's ability, it will provide:

- the date(s) and time(s) of the breach;
- the facts that underlie the discovery of the breach;
- a description of the data involved in the breach; and
- the measures planned or underway to fix the issue.

5. Retention

Customers control the data collected by the Buzzspark Services and stored within their account. Buzzspark never sells personal data to any third party.
Buzzspark will purge Customer Data within a timely period at the termination of the Customer's Agreement as outlined within the Buzzspark Terms and Conditions.

Specific Customer Data can be purged based upon written requests from the Customer as outlined in the Buzzspark Terms and Conditions.

6. Availability

Buzzspark's data center providers use commercially reasonable efforts to ensure a minimum of 99% uptime. Buzzspark Services are designed to ensure redundancy and seamless failover. This design assists Buzzspark in maintaining and updating its applications and backend while limiting downtime.

Customer data in production is mirrored in a database cluster of no less than five nodes. All databases are backed up and maintained using at least industry standard methods.

7. Processing Separation

Buzzspark does not use Customer data for purposes other than to provide and improve the Buzzspark Services that would require separate processing.

Schedule 3: List of Current Subprocessors and their Locations

Amazon Web Services, Inc.
- Headquarters: Seattle, Washington, USA
- Data storage: London, UK

Cloudflare Group
- Headquarters: California, San Francisco, USA
- Data Storage: Global

Crisp IM SAS
- Headquarters: Nantes, France
- Data Storage: EU

Microsoft Ireland Operations, Ltd.
- Headquarters: Dublin, Ireland
- Data Storage: EU

Clearbit
- Headquarters: California, San Francisco, USA
- Data Location: USA

Google LLC
- Headquarters: Dublin, Ireland
- Data Storage: Global