DATA PROTECTION ADDENDUM

This BrainStorm, Inc. Data Protection Addendum ("DPA") is between the parties with respect to the terms governing the Processing of Customer's Personal Information under the BrainStorm Customer Terms of Service (the "Master Agreement"). This DPA sets out the additional terms, requirements and conditions on which BrainStorm, as Provider (defined below), will obtain, handle, process, disclose, transfer, or store Personal Information (defined below) when providing services under the Master Agreement. This DPA serves as an addendum to the Master Agreement and is effective upon its incorporation into the Master Agreement, which incorporation may be specified in the Master Agreement, the Order Form (as defined in the Master Agreement), or as otherwise agreed to between the parties.

BrainStorm will periodically update the terms and conditions of this DPA. You will be notified of any material updates or changes via email or through the Admin Portal.

Terms not otherwise defined in this DPA shall have the meaning as set forth in the Master Agreement.

1. **Definitions and Interpretation**.

    a. The following definitions and rules of interpretation apply in this DPA.

        i. **"Business Purpose"** means the services described in the Master Agreement or any other purpose specifically identified in Appendix A.

        ii. **"Data Subject"** means an individual who is the subject of Personal Information.

        iii. **"Personal Information"** means any information the Provider processes for the Customer that (a) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in the Provider's possession or control or that the Provider is likely to have access to, or (b) the relevant Privacy and Data Protection Requirements otherwise define as protected personal information.

        iv. **"Processing, processes, or process"** means any activity that involves the use of Personal Information or that the relevant Privacy and Data Protection Requirements may otherwise include in the definition of processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Information to third parties

        v. **"Privacy and Data Protection Requirements"** means all applicable federal, state, and international laws and regulations relating to the processing, protection, or privacy of Personal Information, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction.

        vi. **"Security Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise processed by Provider; or a security breach as defined by applicable Privacy and Data Protection Requirements.

    b. This DPA is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this DPA.

c. The Appendices form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Appendices

d. A reference to writing or written includes email but not messages sent via fax.

e. In the case of conflict or ambiguity between:

i. any provision contained in the body of this DPA and any provision contained in the Appendices, the provision in the body of this DPA will prevail;

ii. the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Appendices, the provision contained in the Appendices will prevail;

iii. any of the provisions of this DPA and the provisions of the Master Agreement, the provisions of this DPA will prevail; and

iv. any of the provisions of this agreement and any executed Standard Contractual Clauses, the provisions of the executed Standard Contractual Clauses will prevail.

2. **Personal Information Types and Processing Purposes.**

a. The Customer retains control of the Personal Information and remains responsible for its compliance obligations under the applicable Privacy and Data Protection Requirements, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Provider.

b. Appendix A describes the general Personal Information categories and Data Subject types the Provider may process to fulfill the Business Purposes of the Master Agreement.

3. **Provider's Obligations**

a. The Provider will only process the Personal Information to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's instructions. The Provider will not process the Personal Information for any other purpose or in a way that does not comply with this DPA or the Privacy and Data Protection Requirements. The Provider will promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with the Privacy and Data Protection Requirements.

b. The Provider shall promptly comply with any Customer request or instruction requiring the Provider to amend, transfer, or delete the Personal Information, or to stop, mitigate, or remedy any unauthorized processing.

c. The Provider will maintain the confidentiality of all Personal Information and will not disclose Personal Information to third parties unless the Customer or this DPA specifically authorizes the disclosure, or as required by law. If a law requires the Provider to process or disclose Personal Information, the Provider shall first inform the Customer of the legal requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

d. The Provider will reasonably assist the Customer with meeting the Customer's compliance obligations under the Privacy and Data Protection Requirements, taking into account the nature of the Provider's processing and the information available to the Provider.

e. The Provider will promptly notify the Customer of any changes to Privacy and Data Protection Requirements that may adversely affect the Provider's performance of the Master Agreement.

f. The Customer acknowledges that the Provider is under no duty to investigate the completeness, accuracy, or sufficiency of any specific Customer instructions from Authorized Persons or the Personal Information other than as required under the Privacy and Data Protection Requirements.

g. The Provider will only collect Personal Information for the Customer using the notice set forth at

info.brainstorminc.com/legal/#privacy-policy.

4. Provider's Employees

    a. The Provider will limit Personal Information access to:

        i. those employees who require Personal Information access to meet the Provider's obligations under this DPA and the Master Agreement; and

        ii. the part or parts of the Personal Information that those employees strictly require for the performance of their duties.

    b. The Provider will ensure that all employees:

        i. are informed of the Personal Information's confidential nature and use restrictions;

        ii. have undertaken training on the Privacy and Data Protection Requirements relating to handling Personal Information and how it applies to their particular duties; and

        iii. are aware both of the Provider's duties and their personal duties and obligations under the Privacy and Data Protection Requirements and this DPA.

    c. The Provider will take reasonable steps to ensure the reliability, integrity, and trustworthiness of all of the Provider's employees with access to the Personal Information.

5. **Security.**

    a. The Provider will maintain appropriate technical and organizational measures designed to safeguard Personal Information against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, destruction, or damage. These shall include any security measures set out in Appendix B. The Provider will periodically review these measures at least annually to ensure they remain current and complete.

    b. The Provider will immediately notify the Customer if it becomes aware of any advance in technology and methods of working, which indicate that the parties should adjust their security measures.

    c. The Provider will take reasonable precautions to preserve the integrity of any Personal Information it processes and to prevent any corruption or loss of the Personal Information, including but not limited to establishing effective back-up and data restoration procedures.

6. **Security Breaches.**

    a. The Provider will promptly notify the Customer of any Security Breach.

    b. Immediately following a Security Breach, the parties will co-ordinate with each other to investigate the matter. The Provider will reasonably co-operate with the Customer in the Customer's handling of the matter, including: making available all relevant records, logs, files, data reporting, and other materials required to comply with all Privacy and Data Protection Requirements or as otherwise reasonably required by the Customer.

    c. The Provider will not inform any third party of any Security Breach without first obtaining the Customer's prior written consent, except when law or regulation requires it.

    d. The Provider agrees that the Customer has the sole right to determine:

        i. whether to provide notice of the Security Breach to any Data Subjects, regulators, law enforcement agencies, or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

ii. whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

e. The Provider will cover all reasonable expenses associated with the performance of the obligations under clause Clause 2 and 6.c, unless the matter arose from the Customer's specific instructions, negligence, willful default, or breach of this DPA, in which case the Customer will cover all reasonable expenses.

f. The Provider will also reimburse the Customer for actual reasonable expenses the Customer incurs when responding to and mitigating damages, to the extent that the Provider caused a Security Breach, including all costs of notice and any remedy as set out in clause 4.

7. **Cross-Border Transfers of Personal Information.**

a. If the Privacy and Data Protection Requirements restrict cross-border Personal Information transfers, the Customer will only transfer that Personal Information to the Provider under the following conditions:

i. the Provider, either through its location or participation in a valid cross-border transfer mechanism under the Privacy and Data Protection Requirements, as identified in Appendix A, may legally receive that Personal Information; however the Provider will immediately inform the Customer of any change to that status;

ii. the Customer obtained valid Data Subject consent to the transfer under the Privacy and Data Protection Requirements; or

iii. the transfer otherwise complies with the Privacy and Data Protection Requirements for the reasons set forth in Appendix A.

b. The Provider will not transfer any Personal Information to another country unless the transfer complies with the Privacy and Data Protection Requirements. In Appendix A, the Provider shall identify the legal basis supporting any transfers it makes and will promptly inform the Customer of any change to that status.

8. **Subcontractors.**

a. The Provider may only authorize a third party (subcontractor) other than those set forth in Appendix A to process the Personal Information if:

i. the Customer is given an opportunity to object within 14 days after the Provider supplies the Customer with details regarding the subcontractor's proposed role and contact information;

ii. the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this DPA and, upon the Customer's written request, provides the Customer with copies of such contracts (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum);

iii. the Provider maintains control over all Personal Information it entrusts to the subcontractor; and

iv. the subcontractor shall return or delete the Personal Information after the end of the provision of Services relating to Provider upon such notice from Customer.

b. The Provider shall list all subcontractors that it anticipates using to carry out the Business Purposes in Appendix A and include each subcontractor's name and location and contact information for the person responsible for privacy and data protection compliance. The Customer's agreement to this DPA shall authorize the Provider to use the subcontractors as described in Appendix A.

c. If a subcontractor fails to fulfill its obligations under such written agreement, the Provider remains responsible to the Customer for the subcontractor's performance of its obligations.

d. Upon the Customer's written request, the Provider will audit a subcontractor's compliance with its obligations regarding the Customer's Personal Information and provide the Customer with a summary of the audit results.

9. **Complaints, Data Subject Requests, and Third-Party Rights.**

   a. The Provider shall notify the Customer promptly if it receives any complaint, notice, or communication that directly or indirectly relates to the Personal Information processing or to either party's compliance with the Privacy and Data Protection Requirements.

   b. The Provider will notify the Customer within 5 working days if it receives a request from a Data Subject regarding their Personal Information unless the Provider is able to fully handle and respond to such request.

   c. The Provider will give the Customer its full co-operation and assistance in responding to any complaint, notice, communication, or Data Subject request.

   d. The Provider shall not disclose the Personal Information to any Data Subject or to a third party unless the disclosure is either at the Customer's request or instruction, permitted by this DPA, or is otherwise required by law.

10. **Term and Termination.**

    a. This DPA will remain in full force and effect so long as:

       i. the Master Agreement remains in effect; or

       ii. the Provider retains any Personal Information related to the Master Agreement in its possession or control (the "**Term**").

    b. Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect Personal Information will remain in full force and effect.

    c. If a change in any Privacy and Data Protection Requirement prevents either party from fulfilling all or part of its Master Agreement obligations, the parties will suspend the processing of Personal Information until that processing complies with the new requirements. If the parties are unable to bring the Personal Information processing into compliance with the Privacy and Data Protection Requirement within a reasonable time, they may terminate the Master Agreement upon written notice to the other party.

11. **Data Return and Destruction.**

    a. At the Customer's request, the Provider will give the Customer a copy of or access to all or part of the Customer's Personal Information in its possession or control in the format and on the media reasonably specified by the Customer.

    b. On written notice from the Customer, the Provider will securely destroy or return and not retain all or any Personal Information related to this agreement in its possession or control, except for one copy that it may retain and use for audit purposes only.

    c. If any law, regulation, or government or regulatory body requires the Provider to retain any documents or materials that the Provider would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends. The Provider may only use this retained Personal Information for the required retention reason or audit purposes.

    d. If Customer requests, the Provider will certify in writing that it has destroyed the Personal Information within

30 days after receiving the Customer's request.

12. **Records.**

    a. The Provider will keep detailed, accurate, and up-to-date records regarding any processing of Personal Information it carries out for the Customer, including but not limited to, the access, control, and security of the Personal Information, approved subcontractors and affiliates, the processing purposes, and any other records required by the applicable Privacy and Data Protection Requirements (the "**Records**").

    b. The Provider will ensure that the Records are sufficient to enable the Customer to verify the Provider's compliance with its obligations under this DPA.

    c. The Customer and the Provider shall review the information listed in the Appendices to this DPA annually to confirm its current accuracy and update it if required to reflect current practices.

13. **Audit.**

    a. At least annually, the Provider will assess its Personal Information processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this DPA.

    b. Upon the Customer's written request, the Provider will make the relevant reports available to the Customer for review. The Customer will treat such audit reports as the Provider's confidential information under this Agreement.

    c. The Provider will promptly address any issues, concerns, or exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Provider's management.

14. **Warranties.**

    a. The Provider warrants and represents that:

        i. its employees, subcontractors, agents, and any other person or persons accessing Personal Information on its behalf are reliable and trustworthy and have received the required training on the Privacy and Data Protection Requirements relating to the Personal Information; and

        ii. it and anyone operating on its behalf will process the Personal Information in compliance with both the terms of this DPA and all applicable Privacy and Data Protection Requirements and other laws, enactments, regulations, orders, standards, and other similar instruments; and

        iii. it has no reason to believe that any Privacy and Data Protection Requirements prevent it from providing any of the Master Agreement's contracted services; and

        iv. considering the current technology environment and implementation costs, it will take appropriate technical and organizational measures to prevent the unauthorized or unlawful processing of Personal Information and the accidental loss or destruction of, or damage to, Personal Information, and ensure a level of security appropriate to:

            A. the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction, or damage; and

            B. the nature of the Personal Information protected; and

            C. comply with all applicable Privacy and Data Protection Requirement and its information and security policies, including the security measures required in clause 5.

    b. The Customer warrants and represents that the Provider's expected use of the Personal Information for the

Business Purpose and as specifically instructed by the Customer will comply with all Privacy and Data Protection Requirements.

15. **Indemnification.**

    a. The Provider agrees to indemnify the Customer against all costs, claims, damages, or expenses incurred by the Customer or for which the Customer may become liable due to any failure by the Provider or its employees, subcontractors, or agents to comply with any of its obligations under this DPA or applicable Privacy and Data Protection Requirements.

    b. The limitations on liability set forth in the Master Agreement shall apply to this DPA's indemnity or reimbursement obligations.

16. **Notice**

    a. Any notice or other communication given to a party under or in connection with this DPA shall be in writing and delivered to:

        i. For the Customer:

        ii. For the Provider: BrainStorm, Inc., Ten South Center Street, American Fork, Utah 84003, Attention: Legal Department

    b. Clause 16.a does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

Appendix A

Personal Information Processing Purposes and Details

Business Purposes: To provide Customer with the Service, as set forth in the Master Agreement.

Personal Information Categories: The personal data transferred includes the name, work email, title, department, IP address, and other data in an electronic form in the context of Provider's Service.

Data Subject Types: The data subjects include Customer's representatives and end-users, primarily Customer's employees, but also, potentially, contractors, affiliates and their affiliate's employees and contractors, and collaborators thereof.

Approved Subcontractors: Microsoft Azure (hosting services); Snowflake (data warehouse); SendGrid (email messaging tool with the Service); Freshdesk (support ticket management); HubSpot (email communications management platform); Aha! (customer feedback portal); SurveyMonkey (optional survey collection and analytics); Ironclad (contract management)

Provider's legal basis for receiving Personal Information with cross-border transfer restrictions: Standard Contractual Clauses

Appendix B

Security Measures

Provider will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of the data uploaded to the service, as described in the Master Agreement or in this DPA, or otherwise made reasonably available by Provider. The security practices described int his Appendix B are currently observed by Provider. Although it reserves the right to modify or update these practices, Provider will not materially decrease the overall security of the Service during a subscription term.

APPENDIX C

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a)The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of data to a third country.

(b)The Parties:

(i)the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii)the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c)These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d)The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a)These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b)These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a)Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i)Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii)Clause 8 – Module 2: Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii)Clause 9 - Module 2: Clause 9(a), (c), (d) and (e);

(iv)Clause 12 – Module 2: Clause 12(a), (d) and (f);

(v)Clause 13;

(vi)Clause 15.1(c), (d) and (e);

(vii)Clause 16(e);

(viii)Clause 18 – Module 2: Clause 18(a) and (b).

(b)Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a)Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b)These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c)These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a)An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b)Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c)The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b)The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b)The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i)the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii)the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii)the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv)the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a)The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b)The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c)The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d)The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e)The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODUEL TWO: Transfer controller to processor

(a)GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c)The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d)The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under

its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e)The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODUEL TWO: Transfer to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b)The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c)In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a)The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b)In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c)Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i)lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii)refer the dispute to the competent courts within the meaning of Clause 18.

(d)The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e)The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f)The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODUEL TWO: Transfer controller to processor

(a)Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b)The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c)Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d)The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e)Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f)The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g)The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

1. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b)The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODUEL TWO: Transfer controller to processor

(a)The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b)The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i)the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii)the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii)any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c)The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d)The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e)The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f)Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODUEL TWO: Transfer controller to processor

15.1 Notification

(a)The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the

data exporter) if it:

(i)receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii)becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b)If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d)The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a)The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c)The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these

Clauses, where:

(i)the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii)the data importer is in substantial or persistent breach of these Clauses; or

(iii)the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d)Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e)Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights.

Clause 18

Choice of forum and jurisdiction

MODUEL TWO: Transfer controller to processor

(a)Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b)The Parties agree that those shall be the courts of the Member State in which the data exporter is established.

(c)A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d)The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Customer as identified in the Agreement

Address: Address of Customer as listed in the Agreement

Contact person's name, position and contact details: Customer's contact information as listed in the Agreement

Activities relevant to the data transferred under these Clauses: Processing data in connection with the Agreement entered between the parties.

Signature and date: By executing the Agreement and using the Services (as defined in the Agreement) and transfer Personal Data outside of the EEA or the United Kingdom (UK), the data exporter will be deemed to have singed this Annex I.

Role (controller/processor): Controller

Data importer(s):

Name: BrainStorm, Inc.

Address: Ten South Center Street, American Fork, Utah 84003

Contact person's name, position and contact details: Andrew Wojciechowski, Associate Vice President, Legal; awojciechowski@brainstorminc.com

Activities relevant to the data transferred under these Clauses: Processing data in connection with the Agreement entered between the parties.

Signature and date: By transferring Persona Data outside of the EEA or the UK on Customer's instructions, the data importer will be deemed to have signed this Annex I.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Appendix A of the DPA

Categories of personal data transferred

See Appendix A of the DPA

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

See Appendix A of the DPA

Purpose(s) of the data transfer and further processing

See Appendix A of the DPA

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The personal data will be retained for as long as necessary to complete any processing necessary to provide the Services under the Agreement executed by the data exporter and the data importer.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Processing data in connection with the Processor's provision of the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority shall be determined in accordance with Clause 13 of the Standard Contractual Clauses.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Appendix B of the DPA

ANNEX III

LIST OF SUB-PROCESSORS

Subject to General Authorization. A current list of Sub-processors is found below:

Name	Location	Contact (if available)	Description of Processing
Microsoft Azure	USA		Hosting services provider
SendGrid	USA		In-application email messaging
Aha!	USA		Customer feedback portal
HubSpot	USA		Email campaign management
Snowflake	USA		Data warehouse
Ironclad	USA		Clickwrap management
Freshdesk	USA		Support desk solution

END OF ADDENDUM