DATA PROCESSING ADDENDUM

PARTIES

This Data Processing Addendum (this "**DPA**") is between User (as defined in the Crossbeam Terms of Service set forth at getcrossbeam.com/terms), on behalf of itself, its Affiliates, and its current and future affiliated offices (the "**Customer**") and Crossbeam, Inc., a Delaware corporation (the "**Service Provider**") (each a "**Party**" and collectively the "**Parties**").

BACKGROUND

This DPA is supplemental to and subject to the terms and conditions of the Crossbeam Terms of Service set forth at getcrossbeam.com/terms (the "**Agreement**"). In the event of a conflict between any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail.

1. INTERPRETATION

1.1 Unless otherwise set out below, each capitalised term in this DPA shall have the meaning set out in the Agreement. In this DPA, unless the context requires otherwise:

"**Affiliates**" means the current and future respective affiliated offices of Customer;

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the effective date of this Data Processing Addendum;

"**CCPA Consumer**" means a "consumer" as such term is defined in the CCPA;

"**CCPA Personal Information**" means the "**personal information**" (as defined in the CCPA) that the Service Provider Processes on behalf of the Customer and/or the Customer's Affiliates in connection with the Service Provider's provision of the Services;

"**Controller**" has the meaning given in the GDPR;

"**Customer Personal Data**" means the CCPA Personal Information and the GDPR Personal Data;

"**Data Processing Services**" means the Processing of CCPA Personal Information for any purpose permitted by the CCPA, such as for a permitted "business purpose," as such term is defined in the CCPA, or for any other purpose expressly permitted by the CCPA;

"**Data Subject**" has the meaning given in the GDPR;

"**EU Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council (the "**GDPR**") and any applicable national legislation implementing or supplementing the GDPR, in each case as amended, replaced or superseded from time to time, and all applicable legislation protecting the fundamental

rights and freedoms of persons and their right to privacy with regard to the Processing of GDPR Personal Data;

"**European Economic Area**" or "**EEA**" means the Member States of the European Union together with Iceland, Norway, and Liechtenstein;

"**GDPR Personal Data**" means the "**personal data**" (as defined in the GDPR) that the Service Provider Processes on behalf of the Customer and/or the Customer's Affiliates in connection with the Service Provider's provision of the Services;

"**Privacy Shield**" means the EU-US Privacy Shield self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C (2016)4176 of July 12, 2016.

"**Privacy Shield Principles**" means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of July 12, 2016 (as may be amended, superseded or replaced).

"**Processing**" has the meaning given in the GDPR, and "**Process**" will be interpreted accordingly;

"**Processor**" has the meaning given in the GDPR;

"**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Customer Personal Data;

"**Sell**" and "**Sale**" have the meaning given in the CCPA;

"**Services**" means the service(s) provided by Service Provider to the Customer under the Agreement, including the Data Processing Services;

"**Subprocessor**" means any Processor engaged by the Service Provider who agrees to receive from the Service Provider any Customer Personal Data; and

"**Supervisory Authority**" has the meaning given in the GDPR.

1.2 **Applicability to Customer Personal Data**. Except as otherwise provided in this DPA, this DPA shall apply to all Processing of Customer Personal Data by or on behalf of the Service Provider.

REQUIREMENTS FOR GDPR PERSONAL DATA:

2. GDPR PERSONAL DATA PROCESSING

2.1 **Applicability to GDPR Personal Data.** Clauses 2 through 0 of this DPA shall only apply to the Processing of GDPR Personal Data by or on behalf of the Service Provider

2.2 **Role of the Parties.** For the purposes of the EU Data Protection Laws, the Parties acknowledge and agree that the Service Provider acts as Processor and the Customer and/or Customer's Affiliates act as Controllers. The Customer acts as a single point of contact for its Affiliates with respect to compliance with EU Data Protection Laws, such that where the Service Provider gives notice to the Customer, such information or notice is deemed received by the Customer's Affiliates. The Parties acknowledge and agree that any claims in connection with EU Data Protection Laws under this DPA will be brought by the Customer, whether acting for itself or on behalf of an Affiliate.

2.3 **Instructions for GDPR Personal Data Processing**

The Service Provider will only Process GDPR Personal Data in accordance with:

(a) the Agreement, to the extent necessary to provide the Services to the Customer, and

(b) the Customer's written instructions,

unless Processing is required by European Union or Member State law to which Service Provider is subject, in which case the Service Provider shall, to the extent permitted by European Union or Member State law, inform the Customer of that legal requirement before Processing that GDPR Personal Data.

2.4 Processing GDPR Personal Data outside the scope of this DPA or the Agreement will require prior written agreement between the Customer and the Service Provider on additional instructions for Processing.

2.5 **Required consents and notices**

Where required by applicable EU Data Protection Laws, the Customer will ensure that it has obtained/will obtain all necessary consents, and has given/will give all necessary notices, for the Processing of GDPR Personal Data by the Service Provider in accordance with the Agreement.

3. TRANSFER OF GDPR PERSONAL DATA

3.1 The Service Provider shall not permit, allow or otherwise facilitate any Subprocessor to Process GDPR Personal Data without the prior written consent of the Customer and unless the Service Provider enters into a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor with regard to their Processing of GDPR Personal Data, as are imposed on the Service Provider under this DPA and the Agreement.

3.2 **Liability of Subprocessors of GDPR Personal Data**

The Service Provider shall at all times remain responsible for compliance with its obligations under this DPA with respect to the EU Data Protection Laws and will be liable to the Customer for the acts and omissions of any Subprocessor approved by the Customer

that Processes GDPR Personal Data as if they were the acts and omissions of the Service Provider.

3.3 **Prohibition on Transfers of GDPR Personal Data**

GDPR Personal Data from a Customer's establishments in the EEA or Switzerland may only be exported or accessed by the Service Provider or its Subprocessors outside the EEA or Switzerland (the "**International Transfer**"):

(a) if the recipient, or the country or territory in which it Processes GDPR Personal Data, ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of GDPR Personal Data as determined by the European Commission; or

(b) in accordance with clause **Error! Reference source not found.**.

3.4 **Privacy Shield**

The Service Provider represents and warrants that International Transfers shall be subject to, and that the Service Provider is and shall remain in compliance with the requirements of, self-certification to the Privacy Shield (and will maintain a current self-certification throughout the term of the Agreement) and agree to apply the Privacy Shield Principles to the Processing of any such GDPR Personal Data.

4. ACCESS REQUESTS AND DATA SUBJECT RIGHTS

4.1 **Data Subject Requests**

Unless otherwise required by applicable law, the Service Provider shall promptly notify the Customer of any request received by the Service Provider or any Subprocessor from a Data Subject in respect of the GDPR Personal Data of the Data Subject, and shall not respond to the Data Subject.

4.2 The Service Provider shall, where possible, assist the Customer with ensuring its compliance under applicable EU Data Protection Laws, and in particular shall:

(a) provide the Customer with the ability to correct, delete, block, access or copy the GDPR Personal Data of a Data Subject, or

(b) promptly correct, delete, block, access or copy GDPR Personal Data within the Services at the Customer's request.

4.3 **Data Subject Rights**

Where applicable by virtue of Article 28(3)(e) of the GDPR, taking into account the nature of the Processing, the Service Provider shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising Data Subject rights laid down in the GDPR.

5. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

5.1 Where applicable by virtue of Article 28(3)(f) of the GDPR, the Service Provider shall provide reasonable assistance to the Customer with any data protection impact assessments which are referred to in Article 35 of the GDPR and with any prior consultations to any Supervisory Authority of the Customer which are referred to in Article 36 of the GDPR, in each case solely in relation to Processing of GDPR Personal Data and taking into account the nature of the Processing and information available to the Service Provider

REQUIREMENTS FOR CCPA PERSONAL INFORMATION:

6. CCPA PERSONAL INFORMATION PROCESSING

6.1 **Applicability to CCPA Personal Information.** Clauses 6 through 8 of this DPA shall only apply to the Processing of CCPA Personal Information by or on behalf of the Service Provider on or after the effective date of the CCPA; provided, however, that clause 9.3 shall apply prior to, on and after the effective date of the CCPA.

6.2 **Role of the Parties.** For the purposes of the CCPA, the Parties acknowledge and agree that the Service Provider will act as a "Service Provider" as such term is defined in the CCPA, in its performance of its obligations pursuant to the Agreement. The Customer will act as a single point of contact for its Affiliates with respect to CCPA compliance, such that if the Service Provider gives notice to the Customer, such information or notice will be deemed received by the Customer's Affiliates. The Parties acknowledge and agree that any claims in connection with the CCPA under this DPA will be brought by the Customer, whether acting for itself or on behalf of an Affiliate.

6.3 **Instructions for CCPA Personal Information Processing**

Service Provider shall not retain, use or disclose CCPA Personal Information for any purpose other than for the specific purpose of providing the Services, or as otherwise permitted by the CCPA. Service Provider acknowledges and agrees that it shall not retain, use or disclose CCPA Personal Information for a commercial purpose other than providing the Services.

Processing CCPA Personal Information outside the scope of this DPA or the Agreement will require prior written agreement between the Customer and the Service Provider on additional instructions for Processing.

6.4 **Required consents and notices**

Where required by applicable laws, the Customer will ensure that it has obtained/will obtain all necessary consents, and has given/will give all necessary notices, for the Processing of CCPA Personal Information by the Service Provider in accordance with the Agreement.

7. TRANSFER OF CCPA PERSONAL INFORMATION

7.1 No Disclosure of CCPA Personal Information

The Service Provider shall not disclose, release, transfer, make available or otherwise communicate any CCPA Personal Information to another business or third party without the prior written consent of the Customer unless and to the extent that such disclosure is made to a Subprocessor for a business purpose, provided that Service Provider has entered into a written agreement with Subprocessor which imposes the same obligations on the Subprocessor with regard to their Processing of CCPA Personal Information as are imposed on the Service Provider under this DPA and the Agreement. Notwithstanding the foregoing, nothing in this Agreement shall restrict the Service Provider's ability to disclose CCPA Personal Information to comply with applicable laws or as otherwise permitted by the CCPA.

7.2 No Sale of CCPA Personal Information

The Service Provider shall not Sell any Customer Personal Data to another business or third party without the prior written consent of the Customer.

7.3 Liability of Subprocessors of CCPA Personal Information

The Service Provider shall at all times remain responsible for compliance with its obligations under this DPA with respect to the CCPA and will be liable to the Customer for the acts and omissions of any Subprocessor or other third party to whom Service Provider has disclosed or permitted to Process CCPA Personal Information as if they were the acts and omissions of the Service Provider.

8. CONSUMER RIGHTS REQUESTS

8.1 CCPA Consumer Rights Requests

On and after the effective date of the CCPA, Service Provider shall comply with all applicable requirements of the CCPA, and shall, where possible and at Service Provider's expense, assist Customer with ensuring its compliance under applicable CCPA requirements, and in particular shall:

(a) provide the Customer with the ability to delete, block, access or copy the CCPA Personal Information of a CCPA Consumer, or

(b) promptly delete, block, access or copy CCPA Personal Information within the Services at the Customer's request.

8.2 Notice of Requests

The Service Provider shall promptly notify the Customer of any request received by the Service Provider or any Subprocessor from a CCPA Consumer in respect of the CCPA Personal Information of the CCPA Consumer, and shall not respond to the CCPA Consumer.

8.3 **CCPA Policies, Procedures, and Controls**

Prior to the effective date of the CCPA, Service Provider shall adopt policies, procedures, and controls that enable Service Provider to respond, and to cause its agents and employees to respond, promptly to any rights request pursuant to the CCPA, including any disclosure request, deletion request or opt-out request

REQUIREMENTS FOR ALL CUSTOMER PERSONAL DATA:

9. SECURITY

9.1 **Service Provider Security Obligations**

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Service Provider shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including, where applicable by virtue of Article 28(3)(c) of the GDPR, and as appropriate, the measures referred to in Article 32(1) of the GDPR. Without limiting the generality of the foregoing, the Service Provider shall put in place and maintain the technical and organisational measures as set out in Schedule 2 of this DPA to protect the Customer Personal Data against any Security Incident.

9.2 **Service Provider Audits**

The Customer may audit (by itself or using independent third-party auditors) the Service Provider's compliance with this DPA (including the technical and organisational measures as set out in Schedule 2), including by conducting audits of the Service Provider's (and its Subprocessors') data processing facilities, and such audits may be performed at least once annually.

9.3 Where applicable by virtue of Article 28(3)(h) of the GDPR, the Service Provider shall make available to the Customer on request all information necessary to demonstrate compliance with this DPA. The Service Provider shall immediately inform the Customer if, in its opinion, an instruction pursuant to this clause 9.3 infringes the GDPR or other EEA or Member State or UK data protection provisions.

9.4 **Security Incident Notification**

If the Service Provider or any Subprocessor discovers or becomes aware of a Security Incident, then the Service Provider shall promptly notify the Customer, take any additional steps that are reasonably necessary to remedy any non-compliance with this DPA, including complying with all applicable requirements of the Agreement, and reasonably cooperate in the investigation of the Security Incident.

9.5 **Service Provider Employees and Personnel**

The Service Provider shall limit access to Customer Personal Data to those employees or other personnel who have a business need to have access to such Customer Personal Data. Further, the Service Provider shall ensure that such employees or other personnel have agreed in writing to protect the confidentiality and security of such Customer Personal Data in accordance with the provisions of this DPA.

9.6 **Government Disclosure**

The Service Provider shall promptly notify the Customer of any request for the disclosure of any Customer Personal Data by a governmental or regulatory body or law enforcement authority (including any Supervisory Authority) unless otherwise prohibited by applicable law or a legally binding order of such body or agency.

10. TERMINATION

10.1 **Deletion of data**

Subject to clause 10.2 and 10.3 below, the Service Provider shall promptly and in any event within 90 (ninety) days of the date of termination of the Agreement (or within such shorter timeframe as may be required by the Agreement):

(a) return a complete copy of all Customer Personal Data by secure file transfer in such a format as notified by the Customer to the Service Provider; and

(b) delete and procure the deletion of all other copies of Customer Personal Data Processed by the Service Provider or any Subprocessors.

10.2 Subject to clause 10.3 below, the Customer may in its absolute discretion notify the Service Provider in writing within 30 (thirty) days after the date of termination of the Agreement to require the Service Provider to delete and procure the deletion of all copies of Customer Personal Data Processed by the Service Provider or any Subprocessors. The Service Provider shall comply with any such written request within 90 (ninety) days after the date of termination of the Agreement (or within such shorter timeframe as may be required by the Agreement), and for the avoidance of doubt where this clause 10.2 applies, the Service Provider shall not be required to provide a copy of such Customer Personal Data to the Customer.

10.3 The Service Provider 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 the Service Provider shall ensure the confidentiality of all such Customer Personal Data in accordance with this DPA and the Agreement 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.

10.4 The Service Provider shall provide written certification to Customer that it has fully complied with this clause 10 within 90 days (ninety) days after the date of termination of the Agreement (or within such shorter timeframe as may be required by the Agreement).

11. BENEFIT TO AFFILIATES

11.1 The Service Provider acknowledges and agrees that all rights granted to the Customer under this DPA are for the benefit of the Customer and for the additional purpose of conferring the same benefit on each of its Affiliates as if they were a party hereto.

11.2 Other than as stated in this DPA, no person shall have any rights under or in connection with this DPA under the Contracts (Rights of Third Parties) Act 1999.

12. INDEMNITY

12.1 The Service Provider agrees to indemnify, keep indemnified, and defend at its own expense the Customer and each of its Affiliates against all costs, claims, damages or expenses incurred by the Customer or its Affiliates, or for which the Customer or its Affiliates may become liable due to any failure by the Service Provider or its employees, Subprocessors, or agents to comply with any of its obligations under this DPA, the EU Data Protection Laws, or the CCPA.

12.2 For the avoidance of doubt, any limitation of liability set forth in the Agreement will not apply to this DPA.

13. LIABILITY

13.1 Neither party seeks to exclude its liability for death or personal injury caused by its negligence, or fraud or fraudulent misrepresentation on the part of that party.

13.2 The Customer shall not be liable to the Service Provider, whether in contract, tort (including negligence) or restitution, or for breach of statutory duty or misrepresentation, or otherwise, for any loss of profit, goodwill, business, business opportunity, revenue, turnover or reputation, or any loss of anticipated saving or wasted expenditure, in each case arising under or in connection with the DPA. The Customer's total liability in contract, tort (including negligence) or restitution, or for breach of statutory duty or misrepresentation, or otherwise, arising under or in connection with the DPA shall in all circumstances be limited to the amount set forth in Section 12.3 of the Crossbeam Terms of Service.

14. GENERAL

14.1 If any court or competent authority decides that any term of this DPA is held to be invalid, unlawful, or unenforceable to any extent, such term shall, to that extent only, be severed from the remaining terms, which shall continue to be valid to the fullest extent permitted by law.

14.2 Either Party's failure to enforce any provision of this DPA shall not constitute a waiver of that or any other provision and will not relieve the other Party from the obligation to comply with such provision.

14.3 Neither Party is permitted to assign, transfer, charge, sub-contract, or deal in any other manner with all or any of the rights or obligations under this DPA without the prior express written consent of the other Party.

14.4 This DPA sets forth the entire understanding and agreement between the Parties with respect to the subject matter hereof.

14.5 This DPA and any dispute or claim arising out of it or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the laws of the EU Member State in which the Customer is established; provided, however, that to the extent any such dispute or claim relates to the CCPA, such dispute shall be governed by and construed in accordance with the laws of California.

14.6 Any claim or dispute between the Parties arising out of, or in connection with, this DPA (a "**Dispute**") that cannot be resolved by direct discussions between the Parties shall be resolved in accordance with the procedure set out in the Agreement, if any.

SCHEDULE 1
DETAILS OF THE TRANSFER

Data Exporter

The Customer subscribed to the Services that include Processing of GDPR Personal Data.

Data Importer

Service Provider and its Subprocessors.

Data Subjects

Unless provided otherwise by the Data Exporter, transferred GDPR Personal Data relates to the following categories of data subjects: Customers.

Data Categories

The Customer determines the categories of data entered onto the Services. The transferred GDPR Personal Data typically relates to the following categories of data: Customer's employee names, titles, addresses.

Processing Operations

The transferred GDPR Personal Data is subject to the following basic processing activities:

- use of GDPR Personal Data to set up, operate, monitor and provide the Services (including operational and technical support)
- provision of services
- communication to authorized users
- storage of GDPR Personal Data in dedicated data centers
- upload any fixes or upgrades to the Services
- back up of GDPR Personal Data
- computer processing of GDPR Personal Data, including data transmission, data retrieval, data access
- network access to allow GDPR Personal Data transfer
- execution of instructions of the Customer in accordance with the Agreement

SCHEDULE 2
TECHNICAL AND ORGANISATIONAL MEASURES

1. Service Provider maintains internal policies and procedures, and procures that its Subprocessors also maintain internal policies and procedures, which are designed to:

   (a) secure any Customer Personal Data Processed by Service Provider against accidental or unlawful loss, access, or disclosure;

   (b) identify reasonably foreseeable and internal risks to security and unauthorised access to any Customer Personal Data Processed by Service Provider; and

   (c) minimise security risks, including through risk assessment and regular testing.

2. Service Provider will, and will also procure that its Subprocessors will, conduct periodic reviews to:

   (a) evaluate the security of its network and associated services and the adequacy of its information security program, as measured against industry security standards, Service Provider's policies and procedures, and all applicable information security requirements in the Agreement; and

   (b) determine whether additional or different security measures are required (i) for Service Provider's continued compliance with industry standards, its policies and procedures, and all applicable information security requirements in the Agreement, and (ii) to respond to new security risks or findings generated by the period reviews.

3. Without limiting the generality of the foregoing provisions of this Schedule 2, Service Provider will implement and maintain (for so long as Service Provider continues to Process any Customer Personal Data) all applicable information security requirements in the Agreement. In the event of a conflict between the provisions of the Information Security Requirements and a provision of this Data Processing Agreement, the provision that is more stringent will control.