# Data Processing Addendum

This Data Processing Addendum ("**Addendum**") amends the current version of the Master Cloud Agreement or other written or electronic terms of service or subscription agreement between Customer and Crossbeam, Inc. or the Crossbeam Affiliate indicated in the applicable Order ("**Crossbeam**"), each a "Party" and collectively the "**Parties**." This Addendum applies to and takes precedence over that document and any associated contractual document between the Parties, such as a master services agreement, an order form, statement of work or data protection addendum thereunder (collectively, the "**Agreement**"), to the extent of any conflict. All capitalized terms not defined in this Addendum shall have the meanings set forth in the Agreement.

Customer and Crossbeam agree as follows:

## 1 Definitions.

For purposes of this Addendum:

**1.1** "**Data Protection Laws**" means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of Personal Data, including without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. and any associated regulations and amendments, including, the California Privacy Rights Act amendments ("CCPA"), the General Data Protection Regulation, Regulation (EU) 2016/679 ("GDPR"), and the United Kingdom Data Protection Act of 2018, as such laws may be amended from time to time. For the avoidance of doubt, if Crossbeam's Processing activities involving Personal Data are not within the scope of a given Data Protection Law, such law is not applicable for purposes of this Addendum.

**1.2** "**Data Subject**" means an identified or identifiable natural person about whom Personal Data relates.

**1.3** "**Personal Data**" includes "personal data," "personal information," "personally identifiable information," and similar terms, which is included within Customer Data, and such terms shall have the same meaning as defined by applicable Data Protection Law.

**1.4** "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

**1.5** "**Security Incident**" means any confirmed unauthorized or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data being Processed by Crossbeam. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

**1.6** "**Subprocessor**" means any third party authorized by Crossbeam or its affiliates to Process any Personal Data.

## 2 Scope.

**2.1** This Addendum applies to the Personal Data that Crossbeam receives from Customer, or otherwise Processes on Customer's behalf, in connection with the Service provided by Crossbeam to Customer pursuant to the Agreement, except that Annex A (EU Annex) to this Addendum applies only to such Processing of Personal Data governed by GDPR and the United Kingdom Data Protection Act of 2018 and Annex B (US Annex) to this Addendum applies only to such Processing of Personal Data governed by the relevant state privacy laws.

## 3 Purposes of Processing.

**3.1** Subject Matter and Details of Processing. The Parties acknowledge and agree that (a) the subject matter of the Processing under the Agreement is Crossbeam's provision of the Service; (b) the duration of the Processing is from Crossbeam's receipt of Personal Data until deletion of all Personal Data by Crossbeam in accordance with the Agreement; (c) the nature and purpose of the Processing is to provide the Service; (d) the Data Subjects to whom the Processing pertains are Customer's customers, end users or other individuals to whom Personal Data pertains; and (e) the categories of Personal Data are such categories as Customer is authorized to ingest into the Service under the Agreement.

**3.2** Crossbeam will Process Personal Data: (1) to fulfill its obligations to Customer under the Agreement and this Addendum, including to share data provided by Customer with Partners (as defined in the Agreement) as instructed by Customer; (2) on Customer's behalf; (3) in compliance with Data Protection Laws; and (4) to perform its legal obligations and to establish, exercise, or defend legal claims in respect of the Agreement.

**3.3** If a Data Protection Law to which Crossbeam is subject requires Crossbeam to Process Personal Data in a manner that conflicts with the terms of the Agreement or this Addendum, Crossbeam will inform Customer of that legal requirement before Processing, unless that law prohibits Crossbeam from providing such information on important grounds of public interest within the meaning of the Data Protection Law.

**3.4** Crossbeam will immediately inform Customer if, in Crossbeam's opinion, an instruction from Customer infringes a Data Protection Law.

## 4 Personal Data Processing Requirements.

Crossbeam will:

**4.1** Ensure that the persons it authorizes to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

**4.2** Assist Customer in the fulfilment of Customer's obligations to respond to verifiable requests by Data Subjects (or their lawful representatives) for exercising their rights under Data Protection Laws (such as rights to access or delete Personal Data), by notifying Crossbeam by email to privacy@crossbeam.com.

**4.3** Promptly notify Customer by email of (i) any third-party or Data Subject complaints regarding the Processing of Personal Data; or (ii) any requests by Data Subjects (or their lawful representatives) for exercising their rights under Data Protection Laws; or (iii) any government request for access to or information about Crossbeam's Processing of Personal Data on Customer's behalf, unless prohibited by Data Protection Laws. If prohibited by law from disclosing the details of a government request to Customer, Crossbeam shall notify Customer that it can no longer process Personal Data in accordance with Customer's instructions or pursuant to applicable law, without providing the details thereof, until applicable law permits it to provide such details.

**4.4** Provide reasonable assistance to and cooperation with Customer for Customer's performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by applicable Data Protection Laws.

**4.5** Provide reasonable assistance to and cooperation with Customer for Customer's consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to Crossbeam under Data Protection Laws to consult with a regulatory authority in relation to Crossbeam's Processing or proposed Processing of Personal Data.

## 5 Security.

**5.1** Crossbeam shall implement and maintain technical and organizational security measures designed to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Personal Data, in accordance with Crossbeam's Security Policy which can be found here https://www.crossbeam.com/legal/security-policy/ ("**Security Measures**"). Crossbeam may update the Security Measures, provided, however, that such modifications shall not diminish the overall level of security.

**5.2** Upon becoming aware of a confirmed Security Incident, Crossbeam shall notify Customer without undue delay unless prohibited by applicable law. A delay in giving such notice requested by law enforcement and/or in light of Crossbeam's legitimate needs to investigate or remediate the matter before providing notice shall not constitute an undue delay. Such notices will describe, to the extent possible, details of the Security Incident, including steps taken to mitigate the potential risks and steps Crossbeam recommends Customer take to address the Security Incident. Without prejudice to Crossbeam's obligations under this Section 5, Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Security Incidents. Crossbeam's notification of or response to a Security Incident under this Section 5 will not be construed as an acknowledgement by Crossbeam of any fault or liability with respect to the Security Incident.

**6 Subprocessors.**

**6.1** Customer specifically authorizes Crossbeam to use its affiliates (including without limitation Reveal SAS) as Subprocessors, and generally authorizes Crossbeam to engage Subprocessors to Process Personal Data.

**6.2** Crossbeam shall enter into a written agreement with each Subprocessor, imposing data protection obligations substantially similar to those set out in this Addendum; and

**6.3** Crossbeam remains liable for compliance with the obligations of this Addendum and for any acts or omissions of the Subprocessor that cause Crossbeam to breach any of its obligations under this Addendum.

**6.4** A list of Crossbeam's Subprocessors is available at https://www.crossbeam.com/subprocessors/ or such other website as Crossbeam may designate In addition, if the Customer is using the Reveal Nearbound Platform or related services, the applicable list of Subprocessors is available at https://www.reveal.co/legals/sub-processors (each a "**Subprocessor Page**"), and each Subprocessor Page may be updated by Crossbeam from time to time in accordance with this Addendum.

**6.5** When any new subprocessor is engaged, Crossbeam will notify Customer of the engagement, which notice may be given by updating the Subprocessor Page. Crossbeam will give such notice at least ten (10) calendar days before the new Subprocessor Processes any Personal Data, except that if Crossbeam reasonably believes engaging a new Subprocessor on an expedited basis is necessary to protect the confidentiality, integrity or availability of the Personal Data or avoid material disruption to the Service, Crossbeam will give such notice as soon as reasonably practicable. If, within five (5) calendar days after such notice, Customer notifies Crossbeam in writing that Customer objects to Crossbeam's appointment of a new Subprocessor based on reasonable data protection concerns, the Parties will discuss such concerns in good faith and whether they can be resolved. If the Parties are not able to mutually agree to a resolution of such concerns, Customer, as its sole and exclusive remedy, may terminate the Agreement for convenience.

**7 Audits and Reviews of Compliance.**

To the extent applicable Data Protection Laws include a right for Customer to audit Crossbeam's Processing of Personal Data, Customer will exercise such audit right, and Crossbeam will fulfill its corresponding obligations, as follows:

**7.1** Crossbeam shall make available to Customer relevant information regarding Crossbeam's Processing of Personal Data under this Addendum in the form of Crossbeam's most recent SOC 2 Type II certifications or similar audit reports ("**Third Party Reports**").

**7.2** Not more than once per calendar year and at Customer's expense, Customer may audit Crossbeam's Processing of Personal Data for compliance with its obligations under this Addendum by submitting reasonable requests for information, including security and audit questionnaires. Crossbeam will provide written responses to the extent the requested information is necessary to confirm Crossbeam's compliance with this Addendum. However, if the requested information is addressed in a Third Party Report issued within the 12-month period prior to Customer's request and Crossbeam confirms there have been no material changes in the interim relevant to Customer's request, Customer agrees to accept such Third Party Report in lieu of a written response. Any information provided by Crossbeam under this Section 7 constitutes Crossbeam's Confidential Information under the Agreement.

**7.3** If a third party is to conduct an audit under this Section 7.3., Crossbeam may object to the auditor if the auditor is, in Crossbeam's reasonable opinion, not independent, a competitor of Crossbeam or otherwise unqualified. Such objection by Crossbeam will require Customer to appoint another auditor.

**7.4** Customer will promptly notify Crossbeam of any non-compliance discovered during the course of an audit and provide Crossbeam any audit reports generated in connection with any audit under this Section 7.2, unless prohibited by GDPR or otherwise instructed by a supervisory authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and confirming that Crossbeam's Processing of Personal Data complies with this Addendum.

**7.5** Customer shall reimburse Crossbeam for any time expended by Crossbeam or its Subprocessors in connection with any audits under this Section 7 at Crossbeam's then-current professional services rates, which shall be made available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit. Nothing in this Addendum shall be construed to require Crossbeam to furnish more information about Subprocessors in connection with such audits than such Subprocessors make generally available to their customers. Nothing in this Section 7 shall require Crossbeam to breach any duties of confidentiality.

## 8 Return or Destruction of Personal Data.

Except to the extent required otherwise by Data Protection Law, Crossbeam will within sixty (60) days after written request by Customer following the termination or expiration of the Agreement, return to Customer and/or securely destroy all Personal Data. Except to the extent prohibited by Addendum, Crossbeam will inform Customer if it is not able to return or delete the Personal Data.

## 9 General.

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

**9.2** Notwithstanding any provision to the contrary of the Agreement or this Addendum, Crossbeam may cooperate with law enforcement agencies concerning conduct or activity that it reasonably and in good faith believes may violate federal, state, or local law.

**9.3** Any liabilities arising under this Addendum are subject to the limitations of liability in the Agreement.

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

## Annex A - EU Annex

### 1 Definitions; Processing of Data.

**1.1** Definitions. For purposes of this Annex A, the terms “controller”, “processor” and “supervisory authority” have the meanings given in GDPR; “Standard Contractual Clauses” means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, completed as set forth in Schedule A to this DPA; and “data importer” and “data exporter” have the meanings given in the Standard Contractual Clauses.

**1.2** Roles and Regulatory Compliance; Authorization. The Parties acknowledge and agree that (a) Crossbeam is a processor of the Personal Data under GDPR; (b) Customer is a controller of the Personal Data under GDPR; and (c) each party will comply with the obligations applicable to it in such role under GDPR with respect to the Processing of Personal Data. To the extent that any Usage Data (as defined in the Agreement) is considered Personal Data, Crossbeam is the controller with respect to such data and shall Process such data in accordance with its Privacy Policy, which can be found at https://crossbeam.com/privacy/ (the “Privacy Policy”).

**1.3** Crossbeam’s Compliance with Instructions. Crossbeam will only Process Personal Data in accordance with Customer’s instructions (as set forth in this Addendum or the Agreement or as directed by Customer through the Service) unless GDPR requires otherwise, in which case Crossbeam will notify Customer (unless that law prohibits Crossbeam from doing so).

### 2 Data Security.

**2.1** Crossbeam Security Measures, Controls and Assistance.

(a) Crossbeam will (taking into account the nature of the Processing of Personal Data and the information available to Crossbeam) provide Customer with reasonable assistance necessary for Customer to comply with its obligations in respect of Personal Data under GDPR, including Articles 32 to 34 (inclusive) of the GDPR, by (a) implementing and maintaining the Security Measures; (b) complying with the terms of Section 5 of this Addendum; and (c) complying with this Annex A.

(b) Crossbeam will grant access to Personal Data only to personnel who need such access for the scope of their job duties, and are subject to appropriate confidentiality obligations. Should an employee of a Customer seek to exercise their rights under EU Data Protection Laws (e.g., rights of data access, rectification, erasure, restriction, portability and objection) in respect of any Usage Data that constitutes Personal Data then the Customer undertakes to inform Crossbeam without delay and instruct their employee to contact Crossbeam directly via privacy@crossbeam.com such other email address as directed at the time.

### 3 Data Transfers.

**3.1** Standard Contractual Clauses. To the extent that Crossbeam Processes Personal Data of Data Subjects located in or subject to the applicable Data Privacy Laws of the EEA and/or Switzerland, by signing this Addendum, Crossbeam agrees to be bound by the Standard Contractual Clauses contained in Schedule A. With respect to Personal Data transfers for which Swiss law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, references to the GDPR in Clause 4 of the Standard Contractual Clauses are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority shall include the Swiss Federal Data Protection and Information Commissioner.

**3.2** With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction or Switzerland) governs the international nature of the transfer, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the Effective Date at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) (“UK SCCs”) forms part of this Addendum and takes precedence over the rest of this Addendum as set forth in the UK SCCs. Undefined capitalized terms used in this provision shall mean the definitions in the UK SCCs. For purposes of the UK SCCs, they shall be deemed completed as follows: (1) table 1 of the UK SCCs: (a) the Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer; and (b) the Key Contacts shall be the contacts set forth in the Agreement; (2) table 2 of the UK SCCs: the Approved Standard Contractual Clauses referenced in Table 2 shall be the Standard Contractual Clauses included herein in Schedule A; (3) table 3 of the UK SCCs: Annex 1A, 1B, II, and III shall be set forth in the Annex to the Standard Contractual Clauses in Schedule A below; (4) table 4 of the UK SCCs: either Party may end this Addendum as set out in Section 19 of the UK SCCs; and (5) by entering into this Addendum, the Parties are deemed to be signing the UK SCCs, the Mandatory Clauses in Part 2, and its applicable Tables and Appendix Information.

**3.3** In case of conflict between the Standard Contractual Clauses or the UK SCCs, as applicable, and this Addendum, the Standard Contractual Clauses or UK SCCs, as applicable, will prevail.

**3.4** Additional Safeguards for the Transfer and Processing of Personal Data from the EEA, Switzerland, and the United Kingdom. To the extent that Crossbeam Processes Personal Data of Data Subjects located in or subject to the applicable Data Protection Laws of the European Economic Area, Switzerland, or the United Kingdom, Crossbeam agrees to the following safeguards to protect such data to an equivalent level as applicable Data Protection Laws:

(a) Crossbeam shall encrypt all transfers of the Personal Data between Crossbeam and Customer to prevent the acquisition of such data by third parties.

(b) Crossbeam represents and warrants that: (1) as of the date of this contract, it has not received any directive under Section 702 of the U.S. Foreign Intelligence Surveillance Act, codified at 50 U.S.C. § 1881a ("FISA Section 702"); and (2) no court has found Crossbeam to be the type of entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition; and (3) it is not the type of provider that is eligible to be subject to Upstream collection ("bulk" collection) pursuant to FISA Section 702.

(c) Crossbeam will challenge any request under FISA Section 702 for bulk or upstream surveillance.

(d) Crossbeam will use all reasonably available legal mechanisms to challenge any demands for data access through the national security process it receives, if any, as well as any non-disclosure provisions attached thereto.

(e) Crossbeam will challenge any action pursuant to U.S. Executive Order 12333.

(f) At regular intervals as may be required by law, Crossbeam shall create a transparency report that will be made available to Customer upon request, indicating the types of binding legal demands for the personal data it has received, including national security orders and directives, which shall encompass any process issued under FISA Section 702.

(g) Crossbeam will promptly notify Customer if Crossbeam can no longer comply with the Standard Contractual Clauses or the clauses in this Section. Crossbeam shall not be required to provide Customer with specific information about why it can no longer comply, if providing such information is prohibited by applicable law. Such notice shall entitle Customer to terminate the Agreement (or, at Customer's option, affected statements of work, order forms, and like documents thereunder) and receive a prompt pro-rata refund of any prepaid amounts thereunder. This is without prejudice to Customer's other rights and remedies with respect to a breach of the Agreement.

**Annex B – US Annex**

(a) For purposes of this Annex B, the terms “business”, “commercial purpose”, “service provider”, “sell” and “personal information” have the meanings given in the CCPA. This Annex B solely applies to the processing of “Covered Data” under applicable US privacy and data protection laws, including the CCPA, the Virginia Consumer Data Protection Act, the Colorado Privacy Act and related regulations, the Utah Consumer Privacy Act, and Connecticut’s Act Concerning Personal Data Privacy and Online Monitoring ("Applicable Data Protection Law") .

(b)

(c) With respect to Personal Data, Crossbeam is a "service provider" or "processor" under Applicable Data Protection Law.

**1** Crossbeam will not “sell” Personal Data (as such term in quotation marks is defined in "Applicable Data Protection Law"), “share” or Process Personal Data for purposes of “cross-context behavioral advertising” or “targeted advertising” (as such terms in quotation marks are defined in applicable Data Protection Law), or otherwise Process Personal Data for any purpose other than for the specific purposes set forth herein or outside of the direct business relationship with Customer..

**2** Crossbeam will not attempt to link, identify, or otherwise create a relationship between Personal Data and non-Personal Data or any other data without the express authorization of Consumer.

**3** Crossbeam will not retain, use, or disclose the Personal Data outside of the direct business relationship between Crossbeam and Customer.

**4** Crossbeam will not attempt to re-identify any pseudonymized, anonymized, aggregate, or de-identified Personal Data without Customer's express written permission.

**5** Crossbeam shall implement appropriate technical and organizational measures relating to its processing activities in a manner which enables processor to comply with applicable laws and regulations and maintain appropriate security, protection, deletion and backup of personal data. Crossbeam’s Security Policy https://www.crossbeam.com/legal/security-policy/ and Security Measures https://security.crossbeam.com/ describe Crossbeam’s technical and organizational measures designed to secure the Personal Data Crossbeam processes.

**6** The Parties acknowledge and agree that the Processing of Personal Data authorized by Customer’s instructions described in Section 3 of this Addendum is integral to and encompassed by Crossbeam’s provision of the Service and the direct business relationship between the Parties.

**7** Notwithstanding anything in the Agreement or any order form entered in connection therewith, the Parties acknowledge and agree that Crossbeam’s access to Personal Data does not constitute part of the consideration exchanged by the Parties in respect of the Agreement.

**8** Customer represents and warrants that it has provided notice that Personal Data is being used or shared consistent with Cal. Civ. Code 1798.140(t)(2)(C)(i).

**9** To the extent that any Usage Data (as defined in the Agreement) is considered Personal Data, Crossbeam is the "business" or "controller" with respect to such data and shall Process such data in accordance with its Privacy Policy

**10** Crossbeam certifies that it understands its obligations under this Addendum, including under this Annex B, and that it will comply with them.

## Schedule A

## STANDARD CONTRACTUAL CLAUSES

## SECTION 1

*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)[1] for the transfer of personal 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')

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

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

v. 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.

(c) 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*

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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) 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 the 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[2] (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;

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(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***

(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 10 business 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[3]. 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.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(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***

(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.

(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***

(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***

(a) 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.

## <u>SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES</u>

*Clause 14*

***Local laws and practices affecting compliance with the Clauses***

(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[4];

(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

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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***

#### **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. The Parties agree that this shall be the law of the Netherlands.

*Clause 18*

### ***Choice of forum and jurisdiction***

(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 Netherlands.
(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.

## APPENDIX

EXPLANATORY NOTE:
It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

## ANNEX I

### A. LIST OF PARTIES

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

**Data exporter(s)**: [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name set forth on the applicable Order Form or account registration

Address: … Address set forth on the applicable Order Form or account registration

Contact person's name, position and contact details: Contact details set forth on the applicable Order Form or account registration

Activities relevant to the data transferred under these Clauses: Provision of the Subscription Services

Signature and date: Signature and date set forth on the applicable Order Form or account registration.

Role (controller/processor): Controller

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: Crossbeam, Inc.

Address: 1315 Walnut Street, Suite 300, Philadelphia, PA 19107

Contact person's name, position and contact details: … Amy Rose, Head of Legal, legal@crossbeam.com

Activities relevant to the data transferred under these Clauses: Provision of the Subscription Services

Signature and date: August, 2021

Role (controller/processor): Processor

**B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

Customer business contacts and customer employees

*Categories of personal data transferred*

Business contact information, IP addresses and log data

*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*

For Crossbeam to provide services in accordance with the Agreement.

*Purpose(s) of the data transfer and further processing*

Personal Data is transferred for the purpose of provision of the services by the Crossbeam to Customer.

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

Personal Data will be retained for the length of the Agreement or in accordance with applicable Data Privacy Laws.

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

Subprocessors shall process Personal Data for purposes of assisting Crossbeam in providing the services to Customer under the Agreement and shall continue to process Personal Data for the length of the applicable agreement governing provision of the services or as otherwise required under applicable Data Privacy laws.

**C. COMPETENT SUPERVISORY AUTHORITY**

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

Same as Clause 13 above, and where possible, the Irish Data Protection Authority.

## **ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

Crossbeam's Security Measures https://security.crossbeam.com/ describe Crossbeam's technical and organizational measures designed to secure the Personal Data Crossbeam processes.