Data Processing Agreement

PROVIDER: **WeVideo, Inc.**
25422 Trabuco Road, Suite 105-544
Lake Forest, CA 92630
USA

CONTACT: **Jonathan Huang**
Data Protection Officer
jonathan@wevideo.com

CUSTOMER: **[Customer Name]**
[Customer's Registered Address]

CONTACT: **[Customer Contact Name]**
[Customer Contact Job Title]
[Customer Contact Email Address]

Document Control: March 20, 2025 v3.2 WeVideo DPA

DATA PROCESSING ADDENDUM

The undersigned customer ("Customer") and WeVideo, Inc. ("Provider") enter into this Data Processing Addendum (including the annexes attached hereto, this "DPA") as of the date signed by both parties and forms part of that certain WeVideo Subscription Agreement (as amended, the "Agreement") between the parties.

1. Definitions

For purposes of this DPA, the terms below have the meanings set forth below. Capitalized terms that are used but not defined in this DPA have the meanings given in the Agreement.

(a) Affiliate means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

(b) Applicable Data Protection Laws means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Personal Data under the Agreement, including, without limitation, European Data Protection Laws and the CCPA.

(c) CCPA means the California Consumer Privacy Act of 2018 and any binding regulations promulgated thereunder.

(d) Customer Data means information provided or made available to Provider for Processing on Customer's behalf to perform the Services.

(e) EEA means the European Economic Area.

(f) EU means the European Union.

(g) EU GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

(h) EU Restricted Transfer means a transfer of Personal Data to any person, which would be prohibited without a legal basis therefor under Chapter V of the EU GDPR.

(i) EU Standard Contractual Clauses means the standard contractual clauses issued by the European Commission for the transfer of Personal Data from Customer in the EEA to Provider in the United States, a copy of which is attached hereto as Part B of Annex 1.

(j) European Data Protection Laws means the GDPR and other data protection laws of the European Union, its Member States, Switzerland, Iceland, Liechtenstein, Norway and the United Kingdom, in each case, to the extent applicable to the Processing of Personal Data under the Agreement.

(k) GDPR means the UK GDPR and/or EU GDPR (as applicable), together with any applicable implementing or supplementary legislation in any member state of the EEA or the UK (including the UK Data Protection Act 2018). References to "Articles" and "Chapters" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

(l) Information Security Incident means a breach of Provider's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Provider's possession, custody or control. Information 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.

(m) Personal Data means Customer Data that constitutes "personal data," "personal information," or "personally identifiable information" defined in Applicable Data Protection Laws or information of a similar character regulated thereby, except that Personal Data does not include such information pertaining to Customer's business contacts who are Customer personnel where Provider acts as a controller of such information.

(n) Processing means any operation or set of operations which is performed by (or on behalf of Provider) on behalf of Customer under this Agreement, on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(o) Relevant Body (i) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office and/or UK Government (as and where applicable); and/or (ii) in the context of the EEA and EU GDPR, means the European Commission.

(p) Restricted Country (i) in the context of the UK, means a country or territory outside the UK; and (ii) in the context of the EEA, means a country or territory outside the EEA (which shall, as and where applicable, be interpreted in line with Article FINPROV.10A(1) of the Trade and Cooperation Agreement between the EU and the UK), that the Relevant Body has not deemed to provide an 'adequate' level of protection for Personal Data pursuant to a decision made in accordance with Article 45(1) of the GDPR.

(q) Restricted Transfer means an EU Restricted Transfer and/or a UK Restricted Transfer, as the context requires.

(r) Security Measures has the meaning given in Section 4(a) (Provider Security Measures).

(s) Standard Contractual Clauses means the EU Standard Contractual Clauses and/or UK Standard Contractual Clauses (as applicable).

(t) Subprocessors means third parties that Provider engages to Process Personal Data in relation to the Service.

(u) Supervisory Authority (i) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office; and (ii) in the context of the EEA and EU GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR.

(v) UK GDPR means the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019).

(w) UK Restricted Transfer means a transfer of Personal Data to any person, which would be prohibited without a legal basis therefor under Chapter V of the UK GDPR.

(x) UK Standard Contractual Clauses means the standard contractual clauses issued or approved by the UK Information Commissioner's Office from time to time for the transfer of Personal Data from Customer in the UK to Provider in the United States which, as at the date hereof, are as shown at https://ico.org.uk/media/for-organisations/documents/2620100/uk-sccs-c-p-202107.docx.

(y) The terms controller, data subject, and processor as used in this DPA have the meanings given in the GDPR.

1. Duration and Scope of DPA

(a) This DPA will remain in effect so long as Provider Processes Personal Data, notwithstanding the expiration or termination of the Agreement.

(b) Processing of Personal Data subject to European Data Protection Laws shall be subject to the terms of Annex 1 (EU Annex) to this DPA. Processing of Personal Data subject to the CCPA with respect to which Customer is a Business or Service Provider (as defined in CCPA) shall be subject to Annex 2 (California Annex) to this DPA.

2. Customer Instructions

Provider will Process Personal Data only in accordance with Customer's instructions to Provider. This DPA is a complete expression of such instructions, and Customer's additional instructions will be binding on Provider only pursuant to an amendment to this DPA signed by both parties. By entering into this DPA, Customer instructs Provider to Process Personal Data to provide the Service and to perform its other obligations and exercise its rights under the Agreement.

3. Security

(a) Provider Security Measures. Provider will implement and maintain technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data (the "Security Measures") as described in Annex 3 (Security Measures). Provider may update the Security Measures from time to time, so long as the updated measures do not decrease the overall protection of Personal Data.

(b) Information Security Incidents. Provider will notify Customer without undue delay of any Information Security Incident of which it becomes aware. Such notifications will describe available details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Provider recommends Customer take to address the Information Security Incident. Provider's notification of or response to an Information Security Incident will not be construed as Provider's acknowledgement of any fault or liability with respect to the Information Security Incident.

(c) Customer's Security Responsibilities and Assessment

(i) Customer's Security Responsibilities. Customer agrees that, without limitation of Provider's obligations under Section 4 (Security), Customer is solely responsible for its use of the Service, including (a) making appropriate use of the Service to ensure a level of security appropriate to the risk in respect of the Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Service; (c) securing Customer's systems and devices that Provider uses to provide the Service; and (d) backing up Personal Data.

(ii) Customer's Security Assessment. Customer agrees that the Service, the Security Measures and Provider's commitments under this DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Personal Data.

4. Data Subject Rights

(a) Provider's Data Subject Request Assistance. Provider will (taking into account the nature of the Processing of Personal Data) provide Customer with assistance reasonably necessary for Customer to perform its obligations under Applicable Data Protection Laws to fulfill requests by data subjects to exercise their rights under Applicable Data Protection Laws ("Data Subject Requests") with respect to Personal Data in Provider's possession or control. Customer shall compensate Provider for any such assistance at Provider's then-current professional services rates, which shall be made available to Customer upon request.

(b) Customer's Responsibility for Requests. If Provider receives a Data Subject Request, Provider will (i) notify Customer; and (ii) advise the data subject to submit the request to Customer, and Customer will be responsible for responding to any such request.

5. Customer Responsibilities

(a) Customer shall ensure (and is solely responsible for ensuring) that it has given such notices to and obtained such consents and permissions from third parties (including, without limitation, data subjects), and has reserved all rights, in each case, as may be required under applicable law or otherwise for Provider to Process Personal Data as contemplated by the Agreement.

(b) Customer represents and warrants to Provider that Customer Data does not and will not contain any social security numbers or other government-issued identification numbers, protected health information subject to the Health Insurance

Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health insurance information; biometric information; passwords for online accounts; credentials to any financial accounts; tax return data; any payment card information subject to the Payment Card Industry Data Security Standard; personal data of children under 13 years of age; or any other information that falls within any special categories of data (as defined in GDPR).

6. Miscellaneous

Except as expressly modified by the DPA, the terms of the Agreement remain in full force and effect. To the extent of any conflict or inconsistency between this DPA and the other terms of the Agreement, this DPA will govern. Notwithstanding anything in the Agreement or any order form entered in connection therewith to the contrary, the parties acknowledge and agree that Provider's access to Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement. Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Provider to Customer under this DPA may be given (a) in accordance with any notice clause of the Agreement; (b) to Provider's primary points of contact with Customer; or (c) to any email provided by Customer for the purpose of providing it with Service-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

IN WITNESS WHEREOF, the undersigned have executed this Agreement by their duly authorized representatives, with the intention to be legally bound.

[CUSTOMER NAME]

By:____________________________

Name:__________________________

Title:___________________________

Date:___________________________

WEVIDEO, INC.

By:____________________________

Name:__________________________

Title:___________________________

Date:___________________________

ANNEX 1 TO DPA

EU ANNEX

Part A

1. **Processing of Data**

(a) Subject Matter and Details of Processing. The parties acknowledge and agree that (i) the subject matter of the Processing under the Agreement is Provider's provision of the Service; (ii) the duration of the Processing is from Provider's receipt of Personal Data until deletion of all Personal Data by Provider in accordance with the Agreement; (iii) the nature and purpose of the Processing is to provide the Service; (iv) the data subjects to whom the Personal Data pertains are Customer's personnel; and (v) the categories of personal data are the data subjects' account credentials for the Service platform.

(b) Roles and Regulatory Compliance; Authorization. The parties acknowledge and agree that (i) Provider is a Processor of that Personal Data under European Data Protection Laws; (ii) Customer is a controller of that Personal Data under European Data Protection Laws; and (iii) each party will comply with the obligations applicable to it in such role under the European Data Protection Laws with respect to the Processing of that Personal Data. If Customer is a processor, Customer represents and warrants to Provider that Customer's instructions and actions with respect to Personal Data, including its appointment of Provider as another processor, have been authorized by the relevant controller.

(c) Provider's Compliance with Instructions. Provider will Process Personal Data only in accordance with Customer's instructions stated in this DPA unless applicable European Data Protection Laws require otherwise, in which case Provider will notify Customer (unless that law prohibits Provider from doing so on important grounds of public interest).

(d) Data Deletion. Provider shall delete all the Personal Data on Provider's systems after the end of the provision of Services, unless local laws applicable to Provider require storage of the Personal Data. Provider will comply with such instruction as soon as reasonably practicable and no later than 180 days after such expiration or termination, unless local laws applicable to Provider require storage. Customer may choose to request a copy of such Personal Data from Provider for an additional charge by requesting it in writing at least 30 days prior to expiration or termination of the Agreement. Upon the parties' agreement to such charge pursuant to a work order or other amendment to the Agreement, Provider will provide such copy of such Personal Data before it is deleted in accordance with this clause.

2. **Data Security**

(a) Provider Security Measures, Controls and Assistance

(i) Provider Security Assistance. Provider will (taking into account the nature of the Processing of Personal Data and the information available to Provider) provide Customer with reasonable assistance necessary for Customer to comply with its obligations in respect of Personal Data under European Data Protection Laws, including Articles 32 to 34 (inclusive) of the GDPR, by (a) implementing and maintaining the Security Measures; (b) complying with the terms of Section 4(b) (Information Security Incidents) of the DPA; and (c) complying with this Annex 1.

(ii) Security Compliance by Provider Staff. Provider ensure that its personnel who are authorized to access Personal Data are subject to appropriate confidentiality obligations.

(b) Reviews and Audits of Compliance

Customer may audit Provider's compliance with its obligations under this DPA up to once per year and on such other occasions as may be required by European Data Protection Laws, including where mandated by any supervisory authority with competent jurisdiction. Provider will contribute to such audits by providing Customer or such supervisory authority with the information and assistance reasonably necessary to conduct the audit. If a third party is to conduct the audit, Provider may object to the auditor if the auditor is, in Provider's reasonable opinion, not independent, a competitor of Provider, or otherwise manifestly unsuitable. Such objection by Provider will require Customer to appoint another auditor or conduct the audit itself. To request an audit, Customer must submit a proposed audit plan to Provider at least two weeks in advance of the proposed audit date and any third party auditor must sign a customary non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Provider will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Provider security, privacy, employment or other relevant policies). Provider will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 2(b) shall require Provider to breach any duties of confidentiality. If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of Customer's audit request and Provider has confirmed there have been no known material changes in the controls audited since the date of such report, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures. The audit must be conducted during regular business hours, subject to the agreed final audit plan and Provider's safety, security or other relevant policies, and may not unreasonably interfere with Provider business activities. Customer will promptly notify Provider of any non-compliance discovered during the course of an audit and provide Provider any audit reports generated in connection with any audit under this Section 2(b), unless prohibited by European Data Protection Laws 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/or confirming compliance with the requirements of this DPA. Any audits are at Customer's sole expense. Customer shall reimburse Provider for any time expended by Provider and any third parties in connection with any audits or inspections under this Section 2(b) at Provider'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.

3. Impact Assessments and Consultations

Provider will (taking into account the nature of the Processing and the information available to Provider) reasonably assist Customer in complying with its obligations under Articles 35 and 36 of the GDPR, by (a) making available documentation describing relevant aspects of Provider's information security program and the security measures applied in connection therewith and (b) providing the other information contained in the Agreement, including this DPA.

4. Data Transfers

(a) Data Processing Facilities. Provider may, subject to Section 4(b) (Transfers out of the EEA) and Section 4(d), store and Process Personal Data in the United States or anywhere Provider or its Subprocessors maintains facilities.

(b) Transfers out of the EEA. In relation to any EU Restricted Transfer associated with the Processing by Provider in the United States, the Parties shall comply with their respective obligations set out in the EU Standard Contractual Clauses, which are deemed to be entered into with effect from the first date of any such EU Restricted Transfer.

(c) Transfers out of the UK. In relation to any UK Restricted Transfer associated with the Processing by Provider in the United States, the Parties shall comply with their respective obligations set out in the UK Standard Contractual Clauses, which are deemed to be entered into with effect from the first date of any such UK Restricted Transfer. In respect of any UK Standard Contractual Clauses entered into pursuant to this Section:

(i) Customer shall act as the data exporter and Provider shall act as the data importer and the details on pages 1 to 3 of such UK Standard Contractual Clauses shall be populated with the corresponding information set out on page 1 hereto;

(ii) Clause 9 of such UK Standard Contractual Clauses shall be populated as follows: "*The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established*";

(iii) Clause 11(3) of such UK Standard Contractual Clauses shall be populated as follows: "*The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established*";

(iv) for purposes of Appendix 1 to the UK Standard Contractual Clauses, the categories of data subjects, data, special categories of data (if appropriate), and the Processing operations shall be populated with the corresponding information set out in Annex 5 (Customer Instructions) to this DPA; and

(v) Appendix 2 to the UK Standard Contractual Clauses shall be populated by selecting Option 2 and populating it as follows: "*The following is the description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c): those security measures established and maintained under Section 5 of the DPA*".

(b) Order of Precedence. In the event of any conflict or inconsistency between any provision in this DPA and any provision in the Standard Contractual Clauses, the relevant provision in the Standard Contractual Clauses shall prevail and govern in preference to the relevant provision in this DPA to the extent of such conflict or inconsistency; provided that, it is agreed that the following shall apply:

(i) upon Customer's request under Clause 5(j) of the UK Standard Contractual Clauses that Provider provide copies of the Subprocessor agreements to Customer, Provider may remove or redact all commercial information and/or any clauses unrelated the UK Standard Contractual Clauses or their equivalent beforehand;

(ii) the audits described in Clauses 5(f) and 12(2) of the UK Standard Contractual Clauses and in Clauses 8.9(c) and 8.9(d) of the EU Standard Contractual Clauses shall be performed in accordance with Section 2(b) of this Annex 1 (Reviews and Audits of Compliance);

(iii) Section 5 (Subprocessors) of this Annex 1 constitutes Customer's prior written consent to the subcontracting by Provider of the Processing of Personal Data if such consent is required under Clause 5(h) of the UK Standard Contractual Clauses and Clause 9(a) of the EU Standard Contractual Clauses, in respect of which the Parties are deemed to have selected Option 2; and

(iv) certification of deletion of Personal Data as described in Clause 12(1) of the UK Standard Contractual Clauses and Clauses 8.5 and 16(d), of the EU Standard Contractual Clauses shall be provided upon Customer's request.

(c) Notwithstanding the foregoing, (i) the EU Standard Contractual Clauses will not apply to the extent an alternative recognized compliance standard under Chapter V of the EU GDPR for the lawful transfer of Personal Data outside the EEA applies to the relevant EU Restricted Transfer; and (ii) the UK Standard Contractual Clauses will not apply to the extent an alternative recognized compliance standard under Chapter V of the UK GDPR for the lawful transfer of Personal Data outside the UK applies to the relevant UK Restricted Transfer.

2. Subprocessors

(a) General Authorization to Subprocessor Engagement. Customer hereby provides its general authorization to the engagement by Provider of Subprocessors from time to time. Provider may continue to use those Subprocessors already engaged by Provider as at the date of this DPA (as show in the Subprocessor List). Provider shall notify Customer of any addition or replacement of any Subprocessors at least seven (7) days prior to any such proposed addition or replacement.

(b) Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available in Annex 4 of this DPA (as Annex 4 may be updated from time to time in accordance with this Section 5) ("Subprocessor List").

(c) Requirements for Subprocessor Engagement. When engaging any Subprocessor, Provider will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this DPA with respect to Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. Provider shall be liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

(d) Opportunity to Object to Subprocessor Changes. If within 15 days of receipt of the notice pursuant to Section 5(a) Customer notifies Provider in writing of any objections to the proposed appointment of any Subprocessor on reasonable grounds relating to the protection of Personal Data, Customer and Provider will work together in good faith to find a mutually acceptable resolution to address such objection or withholding. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Service by providing written notice to Provider and pay Provider for all amounts due and owing under the Agreement as of the date of such termination.

Part B

EU STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (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')

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

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

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e);

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules Two and Three: 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.

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.

MODULE TWO: Transfer controller to processor

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 (4) (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 2: 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 seven (7) 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. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

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

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

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

Clause 11

Redress

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

MODULE TWO: Transfer controller to processor

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

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

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

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

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

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

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

Clause 12

Liability

MODULE TWO: Transfer controller to processor

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

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

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

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

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

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

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

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(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.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

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

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

> (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
>
> (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards [12];
>
> (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

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

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

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

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

Clause 15

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

MODULE TWO: Transfer controller to processor

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the EU Member State in which the data exporter is established.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

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

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

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

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

[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, 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.

[4] 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.

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

[6] 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 purposes of these Clauses.

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

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

[11] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[12] 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.

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

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: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

2. …

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

1. Name: WeVideo, Inc.

Address: WeVideo, Inc., 25422 Trabuco Road, Suite 105-544, Lake Forest, CA 92630, USA

Contact person’s name, position and contact details: Jonathan Huang, Data Protection Officer, jonathan@wevideo.com

Activities relevant to the data transferred under these Clauses: Provision of the Services as described in the Agreement and DPA into which these Clauses are incorporated.

Signature and date: …

Role (controller/processor): Processor

2. …

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

As described in Annex 5 to the DPA into which these Clauses are incorporated.

Categories of personal data transferred

As described in Annex 5 to the DPA into which these Clauses are incorporated.

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.

Not applicable.

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

As initiated by the Customer in using the Services.

Nature of the processing

Processing in the course of the provision of the Services as described in the Agreement and the DPA into which these Clauses are incorporated.

Purpose(s) of the data transfer and further processing

For the purpose of the provision of the Services as described in the Agreement and the DPA into which these Clauses are incorporated.

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

For the period determined in accordance with the Agreement and the DPA into which these Clauses are incorporated.

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

Onward transfers to subprocessors as described in Annex 4 to the DPA into which these Clauses are incorporated.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13 (Customer to confirm on a case-by-case basis):

…

ANNEX II

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

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Please refer to Annex 3 to the DPA into which these Clauses are incorporated.

For the purposes of Clause 10, the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance in respect of data subject requests shall be provided, as well as the scope and the extent of the assistance required, is: provided via self-service functionality within the Services, which enables Customers’ users to (i) change certain Personal Data, such as name, username, email address and password; and (ii) to download an archive of certain Personal Data. The user can also contact Customer Support in the event that assistance is required in making use of this functionality.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorized the use of the following sub-processors:

1. Name:

Address:

Contact person's name, position and contact details:

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

2.

…

Annex 2 to DPA

California Annex

1. For purposes of this Annex 2, the terms “business,” “commercial purpose,” “sell” and “service provider” shall have the respective meanings given thereto in the CCPA, and “personal information” shall mean Personal Data that constitutes personal information governed by the CCPA.

2. It is the parties’ intent that with respect to any personal information, Provider is a service provider. Provider shall not (a) sell any personal information; (b) retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Service, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the Service; or (c) retain, use or disclose the personal information outside of the direct business relationship between Provider and Customer. Provider hereby certifies that it understands its obligations under this Section 2 and will comply with them.

3. The parties acknowledge that Provider’s retention, use and disclosure of personal information authorized by Customer’s instructions documented in the DPA are integral to Vendor’s provision of the Services and the business relationship between the parties.

Annex 3 to DPA
Security Measures

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of the Provider's information security program. WeVideo follows the NIST Cyber Security Framework.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Provider's organization, monitoring and maintaining compliance with the Provider's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include, at a minimum, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available industry standard encryption technologies for Personal Data that is transmitted over public networks (i.e. the Internet) or when transmitted wirelessly or at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes). All web traffic is transmitted through HTTPS TLS 1.2. Server to server calls are signed with an HMAC based protocol. Databases are encrypted with AES-256 with daily offsite backups. User passwords hashed with bcrypt with a user specific salt. Encryption of devices where possible, and endpoint protection systems are active. Production database keys are rotated every 30 days.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur). Only employees who should have access to admin privileges will have access, such as system administrators and support agents. Access rights are reviewed upon certain employee events and on a monthly basis. System administrators are on call across time zones via a pager system to provide 24/7 overwatch.
   All admin activity is auditable and logs are kept indefinitely.

5. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that the Provider's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on the Provider's computer systems; (iii) must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity. Various system monitors, firewalls and alerts are active, including Amazon Guard Duty and WAF.
   Systems are accessible only through VPN enforced with 2fa in combination with SSH key access where applicable.
   No on premise cloud services are hosted. Amazon Web Services hosts WeVideo's platform and is ISO 27001 and SOC2-compliant.

7. Physical and environmental security of data centers, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of the Provider's facilities, and (iii) guard against environmental hazards such as heat, fire and water damage. Offices have 24/7 keycard access with building security.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Provider's possession. Deleted items follow a grace period for recovery and then are securely deleted.

9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to the Provider's technology and information assets. Secure software development lifecycle process is established and development follows 2 week sprints that includes testing, staging, and incremental deployment to live servers without any user downtime.
   Production environment data is not used in testing/staging environments.

10. Incident management procedures designed to allow Provider to investigate, respond to, mitigate and notify of events related to the Provider's technology and information assets. Documented incident response plan and disaster recovery tested annually at a minimum.

11. Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
    Threat modeling documents are maintained, as well as incident and event histories.
    Third party penetration tests are performed at least once per year, vulnerability scanning is performed weekly.

13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergencies or disasters.

14. All employees undergo background checks prior to hire. Upon being hired, an internal privacy pledge is signed and cyber awareness training is mandatory on an annual basis. Phishing training is performed every 2 weeks with remedial training for clickers.

Annex 4 to DPA
List of Subprocessors

Subprocessor	Function	Country
Amazon Web Services Inc.	Hosting services	United States
Google	Analytics services	United States
Hubspot	Marketing and analytics services	United States
Mixpanel	Analytics services	United States
Zendesk	Customer Support	United States
Salesforce	Marketing and analytics services	United States
TrackJS	Error Tracking	United States
sentry.io	Error Tracking	United States
Power BI (Microsoft Azure)	Data Visualization	United States
Baremetrics	Payment analysis, credit card notification	United States
Datadog	Cloud monitoring	United States
WeVideo AS	WeVideo subsidiary in Norway	Norway
WeVideo Inc. Menlo Park Sucursala Timisoara, RO	WeVideo subsidiary in Romania	Romania

Annex 5 to DPA
CUSTOMER'S INSTRUCTIONS

Data exporter	Customer, whose particulars are set out in the execution block of the DPA to which these Standard Contractual Clauses are attached.
Data importer	WeVideo, Inc., whose particulars are set out in the pre-amble to the DPA to which these Standard Contractual Clauses are attached.
Data Subjects	Those categories of Data Subject as are set out in the DPA (including in any *Data Processing Details* Annex or similar thereto) – which may include: ● Customer's personnel (eg. Teachers, Administrators, IT-personnel) ● Students in Customer's Municipality / School district
Categories of Data	Those categories of Personal Data as are set out in the DPA (including in any *Data Processing Details* Annex or similar thereto) – which may include: ● The data subjects' account credentials for the Service platform. ● Information about the data subjects' use of the Service platform.
Special categories of data	None
Processing Operations	Any Processing carried out by WeVideo on behalf of the Customer, which is part of WeVideo's provision of the relevant WeVideo Service to the Customer subject to and in accordance with the Agreement.
Types of information processed	WeVideo processes the following personal data on behalf of the data controller: Information about browsers and devices users use to access WeVideo services, which helps WeVideo troubleshoot the Services. ● User's name, email address and password ● User's media content (images, music and video clips) ● User's potential comments added to shared videos WeVideo collect this information when a service on a user's device contacts WeVideo's servers — for example, when a user installs a WeVideo app on a mobile device or when a user connects to WeVideo services through your browser. Activity data that WeVideo collect may include: ● Terms users search for ● Features that users use ● Published videos users watch ● People with whom a user communicates or share content when using WeVideo ● Information that users provide to WeVideo to connect external services of users' choice with the WeVideo services ● What third party sites users publish to (such as Google Drive, Facebook, Twitter) ● Users' responses to surveys