CLOUDINARY DATA PROCESSING ADDENDUM

With effect as of its execution by Cloudinary and Customer, this Data Processing Addendum ("**DPA**") forms part of the Cloudinary Subscription Agreement ("**Subscription Agreement**") between Cloudinary Ltd., or the Cloudinary Ltd. subsidiary from which Customer is acquiring (directly or through an authorized distributor or reseller) the Service, as applicable (collectively, "**Cloudinary**") and the person or entity who acquires the Service under the Subscription Agreement ("**Customer**"). This DPA reflects the parties' agreement with regard to the Processing of Personal Data. All capitalized terms not defined herein will have the meaning set forth in the Subscription Agreement or under the Privacy Laws and Regulations.

DATA PROCESSING TERMS

In the course of providing the Cloudinary's image and video management service ("**Service**") to Customer pursuant to the Subscription Agreement, Cloudinary may Process Personal Data on behalf of Customer. The parties agree to comply with the following provisions with respect to Personal Data Processed by Cloudinary as part of the Service for Customer.

1. **DEFINITIONS**

1.1. "**Cloudinary Information Security Documentation**" means the information security documentation applicable to the specific Service purchased by Customer, as updated from time to time, and made available by Cloudinary upon request and subject to adequate confidentiality arrangements.

1.2. "**Data Subject**" means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Data Subject includes Consumer as such term is defined under the CCPA.

1.3. "**Personal Data**" means any information relating to a Data Subject. Personal Data includes Personal Information as such term is defined under the CCPA.

1.4. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.5. "**Personnel**" means persons authorized by Cloudinary to Process Customer's Personal Data.

1.6. "**Privacy Laws and Regulations"** means 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 and repealing Directive 95/46/EC ("**GDPR**") and California Consumer Privacy Act of 2018 Cal. Civil Code § 1798.100 et seq. ("**CCPA**").

1.7. "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, organization,

storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, blocking, erasure or destruction.

2. DATA PROCESSING

2.1. **Scope and Roles.** This DPA applies when Personal Data is Processed by Cloudinary as part of Cloudinary's provision of the Service. In this context, for the purposes of the GDPR, Customer is the Data Controller and Cloudinary is the Data Processor and for the purposes of the CCPA, Customer is a Business and Cloudinary is the Service Provider.

2.2. **Subject Matter, Duration, Nature and Purpose of Processing.** Cloudinary processes Customer's Personal Data as part of providing Customer with the Service, pursuant to the specifications and for the duration under the terms of the Subscription Agreement._

2.3. **Type of Personal Data and Categories of Data Subjects**. Cloudinary has no control over the type of Personal Data that Customer and users authorized by Customer upload to the Service. Accordingly, Cloudinary has no control over the categories of Data Subjects that Customer's Personal Data relates to.

2.4. **Instructions for Cloudinary's Processing of Personal Data**. Cloudinary will only Process Personal Data on behalf of and in accordance with Customer's instructions. Customer instructs Cloudinary to Process Personal Data for the following purposes: (i) Processing related to the Service in accordance with the terms of the Subscription Agreement; and (ii) Processing to comply with other reasonable instructions provided by Customer where such instructions are consistent with the terms of the Subscription Agreement. Customer undertakes to provide Cloudinary with lawful instructions only.

2.5. As required under applicable Privacy Laws and Regulations, Cloudinary will inform Customer immediately, if in Cloudinary's opinion an instruction infringes any provision under the GDPR and will be under no obligation to follow such instruction, until the matter is resolved in good-faith between the parties.

2.6. Cloudinary will not (1) Sell Personal Data, or (2) retain, use or disclose Personal Data (i) for any purpose other than for the specific purpose of performing the Service, or (ii) outside of the direct business relationship between Customer and Cloudinary, except as permitted under the applicable Privacy Laws and Regulations. Cloudinary acknowledges and will comply with the restrictions set forth in this Section 2.5.

2.7. The parties acknowledge and agree that the Personal Data that Customer discloses to Cloudinary is provided to Cloudinary for a Business Purpose, and Customer does not Sell Personal Data to Cloudinary in connection with the Subscription Agreement.

2.8. Customer undertakes to provide all necessary notices to Data Subject and receive all necessary permissions and consents, or otherwise secure the required lawful ground of Processing, as necessary for Cloudinary to process Personal Data on Customer's behalf under the terms of the Subscription Agreement and this DPA, pursuant to the applicable Privacy Laws and Regulations.

2.9. To the extent required under the applicable Privacy laws and regulations, Customer will appropriately document Data Subjects' notices and consents, or necessary assessment with other applicable lawful grounds of Processing.

3. **ASSISTANCE**

3.1. Taking into account the nature of the Processing, Cloudinary will assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising the Data Subjects' rights under the GDPR. Cloudinary will further assist Customer in ensuring compliance with Customer's obligations in connection with the security of Processing, notification of a Personal Data Breach to supervisory authorities and affected Data Subjects, Customer's data protection impact assessments and Customer's prior consultation with supervisory authorities, in relation to Cloudinary's Processing of Personal Data under this DPA. Except for negligible costs, Customer will reimburse Cloudinary with costs and expenses incurred by Cloudinary in connection with the provision of assistance Customer under this DPA.

4. **PERSONNEL**

4.1. **Limitation of Access**. Cloudinary will ensure that Cloudinary's access to Personal Data is limited to those personnel who require such access to perform the Subscription Agreement.

4.2. Confidentiality. Cloudinary will impose appropriate contractual obligations upon its personnel engaged in the Processing of Personal Data, including relevant obligations regarding confidentiality, data protection, and data security. Cloudinary will ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training in their responsibilities, and have executed written confidentiality agreements. Cloudinary will ensure that such confidentiality agreements survive the termination of the employment or engagement of its personnel.

5. **OTHER PROCESSORS**

5.1. Cloudinary may engage third-party service providers to process Personal Data on behalf of Customer ("**Other Processors**"). Customer hereby provides Cloudinary with a general authorization to engage the Other Processors listed in the Other Processors List available at: https://cloudinary.com/subprocessors.

5.2. All Other Processors have entered into written agreements with Cloudinary that bind them by substantially the same material obligations under this DPA.

5.3. Where an Other Processor fails to fulfil its data protection obligations in connection with the Processing of Personal Data under this DPA, Cloudinary will remain fully liable to Customer for the performance of that Other Processor's obligations.

5.4. Cloudinary may engage with a new Other Processor ("**New Processor**") to Process Customer Personal Data on Customer's behalf. Customer may object to the Processing of Customer's Personal Data by the New Processor, for reasonable and explained grounds, within five (5) business days following Cloudinary's written notice to Customer of the intended engagement with the New Processor. If Customer timely sends Cloudinary a written objection notice, the parties will make a good-faith effort to resolve Customer's

objection. In the absence of a resolution, Cloudinary will make commercially reasonable efforts to provide Customer with the same level of Service, without using the New Processor to Process Customer's Personal Data.

6. ONWARD AND TRANS-BORDER DATA TRANSFER

6.1. Transfer of Personal Data related to Data Subjects within the EU to Cloudianry's data hosting services in the US and other Third Countries, which are covered by the GDPR, is made in accordance with the EU Controller-Processor standard contractual clauses, pursuant to EU Commission Decision C(2010)593, in the form attached and incorporated by reference to this DPA as **Exhibit A**, or, as required, in accordance with any successor thereof or an alternative lawful data transfer mechanism.

7. INFORMATION SECURITY

7.1. Cloudinary will maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Customer's Personal Data, pursuant to the Cloudinary Information Security Documentation and the ISO 27001 standard. Cloudinary regularly monitors compliance with these safeguards. Cloudinary will not materially decrease the overall security of the Service during the term of providing the Service to the Customer under the Subscription Agreement.

8. PERSONAL DATA BREACH MANAGEMENT AND NOTIFICATION

8.1. Cloudinary will maintain security incident management policies and procedures and will notify Customer without undue delay after becoming aware of a Personal Data Breach related to Customer's Personal Data which Cloudinary, or any of Cloudinary's Other Processors, Process. Cloudinary's notice will at least: (a) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (b) communicate the name and contact details of the Cloudinary's data protection team, which will be available to provide any additional available information about the Personal Data Breach; (c) describe the likely consequences of the Personal Data Breach; (d) describe the measures taken or proposed to be taken by Cloudinary to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

8.2. Cloudinary will work diligently, pursuant to its incident management policies and procedures to promptly identify and remediate the cause of the Personal Data Breach and will inform Customer accordingly.

8.3. Cloudinary's liability for a Personal Data Breach toward Customer and any third party is subject to the following limitations: (a) the Personal Data Breach is a result of a breach of Cloudinary's information security obligations under this DPA; and (b) the Personal Data Breach is not caused by: (i) acts or omissions of Customer, or any person acting on behalf of or jointly with Customer (collectively "Customer Representatives"); (ii) Customer Representatives' instructions to Cloudinary; (iii) a willful, deliberate or malicious conduct by a third party; or (iv) acts of God or force major, including, without limitation, acts of war, terror, state-supported attacks, acts of state or governmental action prohibiting or impeding Cloudinary from performing its information security obligations under the Subscription Agreement and natural and man-made disasters.

9. AUDIT AND DEMONSTRATION OF COMPLIANCE

9.1. Cloudinary will make available to Customer all information necessary for Customer to demonstrate compliance with the obligations laid down under Article 28 to the GDPR in relation to the Processing of Personal Data under this DPA by Cloudinary and its Other Processors.

9.2. To the extent required under applicable Privacy Laws and Regulations, Cloudinary will allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, in relation to Cloudinary's obligations under this DPA. Cloudinary may satisfy the audit obligation under this section by providing Customer with attestations, certifications and summaries of audit reports conducted by accredited third party auditors. Audits by Customer are subject to the following terms: (i) the audit will be pre-scheduled in writing with Cloudinary, at least forty-five (45) days in advance and will be performed not more than once a year (except for an audit following a Personal Data Breach); (ii) the auditor will execute a non-disclosure and non-competition undertaking toward Cloudinary; (iii) the auditor will not have access to non-Customer data (iv) Customer will make sure that the audit will not interfere with or damage Cloudinary's business activities and information and network systems; (v) Customer will bear all costs and assume responsibility and liability for the audit; (vi) the auditor will first deliver a draft report to Cloudianry and allow Cloudinary reasonable time and no less than ten (10) business days, to review and respond to the auditor’s findings, before submitting the report to the Customer; (vii) Customer will receive only the auditor's report, without any Cloudinary 'raw data' materials, will keep the audit results in strict confidentiality and will use them solely for the specific purposes of the audit under this section; and (viii) as soon as the purpose of the audit is completed, Customer will permanently dispose of the audit report.

10. DELETION OF PERSONAL DATA

10.1. **Data Deletion**. Within reasonable time after the end of the provision of the Service, Cloudinary will return Customer's Personal Data to Customer or delete such data, including by de-identifying thereof.

10.2. **Data Retention**. Notwithstanding, Customer acknowledges and agrees that Cloudinary may retain copies of Customer Personal Data as necessary in connection with its routine backup and archiving procedures and to ensure compliance with its legal obligations and its continuing obligations under applicable law, including to retain data pursuant to legal requirements and to use such data to protect Cloudinary, its affiliates, agents, and any person on their behalf in court and administrative proceedings.

11. DISCLOSURE TO COMPETENT AUTHORITIES

11.1. Cloudinary may disclose Personal Data (a) if required by a subpoena or other judicial or administrative order, or if otherwise required by law; or (b) if Cloudinary deems the disclosure necessary to protect the safety and rights of any person, or the general public.

12. ANONYMIZED AND AGGREGATED DATA

12.1. Cloudinary may process data based on extracts of Personal Data on an aggregated and non-identifiable forms, for Cloudinary's legitimate business purposes, including for testing, development, controls, and operations of the Service, and may share and retain such data at Cloudinary's discretion.

13. DISPUTE RESOLUTION

13.1. The parties agree to communicate regularly about any open issues or process problems that require resolution. The parties will attempt in good faith to resolve any dispute related to this DPA as a precondition to commence legal proceedings, first by direct communications between the persons responsible for administering this DPA and next by negotiation between executives with authority to settle the controversy. Either party may give the other party a written notice of any dispute not resolved in the normal course of business. Within two (2) business days after delivery of the notice, the receiving party will submit to the other party a written response. The notice and the response will include a statement of each party's position and a summary of arguments supporting that position and the name and title of the executive who will represent that party. Within five (5) business days after delivery of the disputing party's notice, the executives of both parties will meet at a mutually acceptable time and place, including by phone, and thereafter as often as they reasonably deem necessary, to resolve the dispute. All reasonable requests for information made by one party to the other will be honored. All negotiations pursuant to this clause are confidential and will be treated as compromise and settlement negotiations for purposes of applicable rules of evidence.

14. LIMITATION OF LIABILITY

14.1. Each party's liability arising out of or related to this DPA (whether in contract, tort, or under any other theory of liability) is subject to the section 'Limitation of Liability' of the Subscription Agreement, and any reference in such section to the liability of a party means that party and its Affiliates in the aggregate.

15. TERM

15.1. This DPA will commence on the later of the date of its execution or the effective date of the Subscription Agreement to which it relates and will continue until the Subscription Agreement expires or is terminated.

16. COMPLIANCE

16.1. Cloudinary is responsible to make sure that all relevant Cloudinary's personnel adhere to this DPA.

16.2. Cloudinary's compliance team can be reached at: **support@cloudinary.com**.

17. MISCELLANEOUS

1. Any alteration or modification of this DPA is not valid unless made in writing and executed by duly authorized personnel of both parties.

2. Invalidation of one or more of the provisions under this DPA will not affect the remaining provisions. Invalid provisions will be replaced to the extent possible by those valid provisions which achieve essentially the same objectives.

Exhibit A
Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the exporting organization (Customer): _____

Address (Customer): _____

("**Data exporter**")

and

Name of the importing organisation: the relevant Cloudinary entity as specified under the Agreement

("**Data importer**")

(individually referred to as a "Party" and jointly referred to as the "**Parties**")

HAVE AGREED on the following contractual clauses (the "**Clauses**") in order to provide adequate safeguards for the protection of privacy rights and fundamental rights and freedoms of individuals for the transfer of personal data specified in Appendix 1 from the Data Exporter to the Data Importer.

Clause 1 – Definitions

For the purposes of the Clauses:

"personal data", "special categories of data", "process/processing", "controller", "processor", "data subject" and "supervisory authority" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

"the data exporter" means the controller who transfers the personal data;

"the data importer" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

"the sub-processor" means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

"the applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

"technical and organisational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 - Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3 - Third-party beneficiary clause

The data subject can enforce against the data exporter this Clause, Clause 4 (b) to (i), Clause 5 (a) to (e), and (g) to (j), Clause 6 (1) and (2), Clause 7, Clause 8 (2), and Clauses 9 to 12 as third-party beneficiary.

The data subject can enforce against the data importer this Clause, Clause 5 (a) to (e) and (g), Clause 6, Clause 7, Clause 8 (2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

The data subject can enforce against the sub-processor this Clause, Clause 5 (a) to (e) and (g), Clause 6, Clause 7, Clause 8 (2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 - Obligations of the data exporter

The data exporter agrees and warrants:

that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the EU member state where the data exporter is established) and does not violate the relevant provisions of that state;

that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

that it will ensure compliance with the security measures;

that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

to forward any notification received from the data importer or any sub-processor pursuant to Clause 5 (b) and Clause 8 (3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

that it will ensure compliance with Clause 4 (a) to (i).

Clause 5 - Obligations of the data importer

The data importer agrees and warrants:

to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

that it will promptly notify the data exporter about:

any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

any accidental or unauthorised access; and

any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

that the processing services by the sub-processor will be carried out in accordance with Clause 11;

to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6 - Liability

The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7 - Mediation and jurisdiction

The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

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

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

The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 - Cooperation with supervisory authorities

The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 - Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 - Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 - Sub-processing

The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 - Obligation after the termination of personal data-processing services

The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Annex forms part of the Clauses and must be completed and signed by the Parties.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The Data Controller as per the Agreement, who is a Party to the Clauses.

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):

The Data Processor as per the Agreement, who is a Party to the Clauses.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

The data importer has no control over the type of Personal Data that the data exporter and users authorized by the data exporter. Accordingly, the data importer has no control over the categories of data subjects that the data exporter's personal data relates to.

Categories of data

The personal data transferred concern the following categories of data (please specify):

The data importer has no control over the type of Personal Data that the data exporter and users authorized by the data exporter. Accordingly, the data importer has no control over the categories of data that the data exporter's personal data relates to.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify, tick the applicable):

The data importer has no control over the type of Personal Data that the data exporter and users authorized by the data exporter. Accordingly, the data importer has no control over the special categories of data that the data exporter's personal data relates to.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify, tick the applicable):

Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and describes the technical and organisational security measures implemented by the data importer.

CLOUDINARY'S TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

These Technical and Organizational Data Security Measures articulate the security measures and controls implemented by Cloudinary in support of its security program that leverages the ISO/IEC 27000-series of control standards as its baseline.

In the course of processing customer, Cloudinary will implement and maintain commercially reasonable, industry standard technical and organizational measures to protect customer data, consistent with applicable laws, that meet the measures described below, or an equivalent standard of protection appropriate to the risk of processing customer data in the course of providing Cloudinary's services, and regularly carry out, test, review, and update all such measures:

1. Information Security Management System

Cloudinary has an ISMS (Information Security Management System) in place to evaluate risks to the security of data, to manage the assessment and treatment of these risks and to continually improve its information security. It includes all aspects of the company – people, processes, and systems – by applying a risk-based approach. Cloudinary ISMS has been inspired and based upon industry best practices, frameworks and standards such as ISO/IEC 27001:2013.

2. Personnel – Screening Personnel Authorized to Process Customer Data

Cloudinary conducts background checks (subject to local restrictions) on all personnel who may interact with customer data as part of their duties, regardless of specific client requirements. As part of the onboarding processes, Cloudinary provides the necessary trainings about protecting and securing customer data to such authorized personnel.

3. Physical Access – Implementation of Controls Designed to Prevent Unauthorized Access to Premises Where Customer Data is Processed

Cloudinary's platform is hosted on AWS cloud infrastructure, and as part of the organizational policies, customer data is not stored at Cloudinary's offices or in any location except for Cloudinary's cloud-based production environment.

Customer data will only be stored and processed on Cloudinary's cloud-based production environment. The production infrastructure is hosted by AWS and as such is not physically accessible to Cloudinary personnel or anyone but AWS. Information about AWS' physical access processes is available at: https://aws.amazon.com/security/.

AWS's security whitepaper (including information about their physical premises security) is available at: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

4. System Security – Implementation of Controls Designed to Prevent Unauthorized Access and Limit Vulnerabilities of Systems Processing Customer Data

Cloudinary's workstation controls include the following: (i) unique user authentication (utilizing complex, regularly-rotated passwords); (ii) password-protected screen locking that activates after a specified period of inactivity; (iii) anti-malware utility that is regularly updated; (iv) disk encryption; and, (v) OS and application patching.

Cloudinary's corporate and production networks are segregated by multiple security measures, such as separate accounts, multi-factor authentication and strict enforcement of access patterns; Cloudinary monitors its systems and networks for security related events and runs, at least once a year, penetration test by a third party on its production applications. Identified vulnerabilities are remediated in a timely manner.

User lifecycle management procedures have been implemented to assign and deploy user rights in alignment with the specific assign function and revocation of user rights upon termination and deactivation of the user's account. Access is granted according to the principle of least privilege and is fully monitored, from the VPN access to database queries, end-to-end.

5. Data Access – Implementation of Controls Designed to Detect and Prevent Unauthorized Activities in Systems Processing Customer Data

Role-based user and administrator access to customer data, limited to the least number of administrators necessary, and granting physical, system, and network access only to the extent necessary for users to accomplish their job function (i.e., on a "need to know") basis, amended for role changes and revoked for terminated personnel on date of termination; Multi-factor authentication on all privileged accounts and accounts with access to sensitive data; Logging of privileged account use and access to sensitive data; Effective control operation verified at least annually by a qualified third party auditor.

Passwords must adhere to Cloudinary's password policy, which includes minimum length requirements, enforcing complexity and set periodic resets, all according to market standard and relevant best practices. As part of Cloudinary's compliance processes user privileges reviews are being conducted for all organizational systems on a quarterly basis. By policy, shared credentials are not allowed.

In regard to Cloudinary's platform, on an Enterprise plan, Cloudinary will support SSO, allowing customers to enforce their own password policies for their employees. Cloudinary's platform does not store users' passwords, but rather a secure hash.

6. Data Transfer – Implementation of Controls Designed to Prevent Unauthorized Access to Customer Data During Storage and Transmission

All data is encrypted in transit, at rest, and when stored in AWS backups.

Remote access (including during remote maintenance or service procedures) is allowed only via VPN tunnels or other secure, encrypted connections that require multi-factor authentication; Cloudinary implements secure communication sessions across applications/services through strong encryption protocols and ciphers (e.g. HTTPS with Transport Layer Security (TLS); Encryption of customer data does not employ vulnerable protocols or weak ciphers. For data at rest, industry-standard AES-256 encryption is being used.

7. Instructions – Implementation of Controls Designed to Ensure Customer Data is Only Processed in Accordance with Customer's Instructions

Cloudinary has in place internal policies containing formal instructions for data processing procedures; Contractors are being carefully vetted with regard to data security; Cloudinary personnel is being trained periodically to maintain awareness regarding data protection and security requirements.

8. Vulnerability Management and Secure Development Life Cycle (SDLC)

Cloudinary's development processes follow secure software development best practices, which include formal design reviews, threat modeling, and completion of a risk assessment.

Cloudinary employs automated tools that monitor CVEs in dependent libraries. Cloudinary also maintains relationships with the open-source maintainers of cardinal libraries such as Imagemagick, to receive advance notifications and patch instructions for yet unpublished vulnerabilities, similar to the advance notifications Linux distribution maintainers receive to be prepared with patches when the vulnerability is made public.

Cloudinary conducts third-party penetration tests on Cloudinary's systems (at least once a year) by carefully selected industry experts and manage a security bug bounty program managed by BugCrowd (https://bugcrowd.com/cloudinary), to improve Cloudinary's security posture on an ongoing basis.

As part of its ongoing maintenance, Cloudinary's production systems are patched periodically after sufficient testing, or in an ad-hoc manner when a specific critical vulnerability that affects the systems is announced. Low-level infrastructure updates are handled by AWS. Cloudinary is a SaaS service that works on an agile development cycle with weekly releases. Releases include feature enhancements, bug requests, security patches, etc. There is no down time associated with releases.

Cloudinary puts an emphasis on writing secure, clear, highly maintainable, and well-documented code. All codes are reviewed as part of the organizational SDLC processes, to identify possible security vulnerabilities. In general, development follows security best-practices, features are considered with security in mind and all new code is carefully code-reviewed before being merged into the main codebase. Cloudinary's developers are trained to follow OWASP principles and keep them in mind during code reviews. Every change is documented in an internal release notes document and every deployment is versioned and labelled. In addition to tests of specific changes, Cloudinary also conducts acceptance tests to identify regressions. Depending on the type and magnitude of a change, Cloudinary may initiate a full regression test before deploying a new version on production.

9. Incident Management, Disaster Recovery and Business Continuity

Cloudinary has designed its systems to tolerate system failures with minimal customer impact.

Cloudinary's internal procedures provide guidance on how to plan and execute operations addressing potential business interruptions caused by emergency events in a manner minimizing any kind of loss. Cloudinary's business continuity management process is designed and implemented to reduce the disruption caused by disasters and security failures to an acceptable level.

Cloudinary conducts ongoing technical DR sessions to review its related technical operations and to conduct 'fire drills' to test it in real time. As part of a holistic approach, all production related DR aspects (compute, storage, databases, site-is-down, etc.) are being covered during such drills.

Cloudinary has datacenters in multiple locations (US, EU and APAC), that will be used according to clients' specific requirements. Cloudinary's default datacenter is based in the US. Cloudinary has Disaster Recovery (DR) sites that are within the same regulatory region (EU, US), except for APAC in which the primary site is Singapore and the DR site is in Japan.

Backups are performed to a separate cloud account protected by MFA, to a separate region. Backups are performed online in close time proximity to the data ingestion. Backups are tested regularly as part of Cloudinary's internal compliance processes.

Cloudinary's DevOps team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents and

to manage the impact and resolution.

An incident would receive immediate attention from all relevant personnel, every day of the week, any time of the day. Once identified and validated, incidents will be reported according to Cloudinary's security and privacy policies.

Cloudinary's Incident Management, Disaster Recovery and Business Continuity processes are approved by Cloudinary's management, audited by a non-dependent 3rd party on an annual basis and are practiced on an ongoing basis.

10. Separation – Processing of Customer Data Separately From Other Data in a Multi-Tenant Environment

Cloudinary's platform is hosted on a multi-tenant logically-separated AWS cloud infrastructure. As a multi-tenant SaaS with 75,000+ active customers, no single customer can affect capacity, which is designed with embedded rate limits and throttling.

Customer (tenant) user account credentials are restricted, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures.

Separation of at-rest storage to dedicated storage infrastructure is available to Enterprise customers to comply with different regulations.

11. Security Event Logs – Secure Logging, Monitoring, and Reporting of Security Events

All systems generate logs (from the VPN access to database queries, end-to-end) and alert in case of logging capabilities failure. All system logs are recorded and stored online for 90 days and in cold storage for 1 year.

Running native on AWS Cloud, Cloudinary uses a set of Cloud-native tools that monitor activity and mitigate risks and configuration mistakes. Audit logs are kept in highly privileged, dedicated, S3 buckets and log file access is granted according to the principle of 'need to have' and is fully monitored.

Cloudinary employs 24x7 system monitoring and ops personnel on call. When a service issue is identified, Cloudinary updates the system status at http://status.cloudinary.com. Cloudinary measures multiple metrics to scale and accommodate changes in incoming load. The system has an automatic pre-emptive scale up events feature, based on known usage patterns which are unique to each data center.

Cloudinary employs intrusion detection systems and uses commercial and customized tools to collect and examine Cloudinary's application and system logs, to detect anomalies.

12. Data Deletion – Secure Data Destruction

Upon request and pursuant to contractual obligations, Cloudinary is able to completely and permanently delete specific or all customer personal information from its production environment.

Cloudinary follows GDPR requirements.