CLOUDINARY DATA PROCESSING AGREEMENT

With effect as of execution by Customer of an Order Form with Cloudinary, this Data Processing Agreement ("**DPA**") forms part of the Cloudinary Main 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 Services, as applicable (collectively, "**Cloudinary**") and the person or entity who acquires the Services 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 Cloudinary's image and video management service ("**Services**") 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 Services for Customer.

1. **DEFINITIONS**

1.1. "**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 or similar terms under other Privacy Laws and Regulations.

1.2. "**Data Privacy Framework**" means the EU-US and/or Swiss-US Data Privacy Framework (DPF) self certification program operated by the US Department of Commerce; "**Data Privacy Principles**" means the Data Privacy Framework principles (as supplemented by the Supplemental Principles).

1.3. "**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.

1.4. "**Personal Data**" means any information relating to a Data Subject which Cloudinary may Process on behalf of Customer in performance of the Services. Personal Data includes "Personal Information" as such term is defined under the CCPA.

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 ("**EU GDPR**"), the GDPR as transformed into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the Data Protection Act 2018 ("**UK GDPR**") (collectively referred to herein as "**GDPR**"),California Consumer Privacy Act of 2018 Cal. Civil Code § 1798.100 et seq. ("**CCPA**"), as amended by the California Privacy Rights Act of 2020 ("**CPRA**", both CCPA and CPRA collectively referred to herein as "**CCPA**").

1.7. "**Process**" or "**Processing**", "**Controller**", "**Processor**" and "**Supervisory Authority**" shall have the meanings given to them in the EU GDPR or equivalent terms under applicable Privacy Laws and Regulations.

1.8. "**Services**" means Cloudinary's image and video management service as more fully described in the Subscription Agreement.

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 Services. In this context, for the purposes of the GDPR, Customer is the Controller or the Processor of the Personal Data and Cloudinary is the Processor and for the purposes of the CCPA, Customer is a Business and Cloudinary is the Service Provider.

2.2. **Details of Processing.** The details of the Processing of Customer's Personal Data are set forth in **Annex I** of this DPA.

2.3. **Instructions for Cloudinary's Processing of Personal Data**. Cloudinary will only Process Personal Data on behalf of and in accordance with Customer's instructions, described in this DPA. Customer instructs Cloudinary to Process Personal Data for the following purposes: (i) Processing related to the Services in accordance with the terms of the Subscription Agreement, including processing Personal Data into aggregated and de-identified form, as inherently required for the provision of the Services; 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. Cloudinary will inform Customer immediately, if in Cloudinary's opinion an instruction infringes any provision under Privacy Laws and Regulations.

2.4. Cloudinary will not (1) "Sell" or "Share" Personal Data as those terms are defined under the CCPA, (2) retain, use or disclose Personal Data (i) for any purpose other than for the specific purpose of performing the Services, or (ii) outside of the direct business relationship between Customer and Cloudinary, except as permitted under the applicable Privacy Laws and Regulations, and (3) combine Personal Data that Cloudinary receives from, or on behalf of a Data Subject, or which Cloudinary collects from its own interaction with a Data Subject with that of another person, except as permitted under the applicable Privacy Laws and Regulations.

2.5. Customer will not transfer and/or disclose "Sensitive Personal Information" (as defined under the CCPA) to Cloudinary, unless (i) it has expressly notified Cloudinary in writing; (ii) provided Cloudinary specific instructions regarding such Sensitive Personal Information, and in such a case, Cloudinary will not retain or use such Sensitive Personal Information other than in accordance with such instructions.

2.6. Customer will document and provide all necessary notices to Data Subject and receive all necessary permissions and consents, to the extent required under applicable Privacy Laws and Regulations or otherwise secure the required lawful ground of Processing, as necessary for Cloudinary to Process Personal Data, pursuant to the applicable Privacy Laws and Regulations.

3. **ASSISTANCE.** Taking into account the nature of the Processing, Cloudinary will assist Customer by reasonable technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligations to: (i) respond to requests for exercising the Data Subjects' rights under Privacy Laws and Regulations, (ii) Customer's obligations to notify a Personal Data Breach to the relevant Supervisory Authorities and affected Data Subjects, and (iii) Customer's data protection impact assessments and Customer's prior consultation with supervisory authorities, all in relation to Cloudinary's Processing of Personal Data under this DPA. Except for negligible costs, Customer will reimburse Cloudinary for costs and expenses incurred by Cloudinary in connection with the provision of assistance to Customer under this DPA, which costs and expenses the parties shall agree in advance.

4. **PERSONNEL.** Cloudinary will ensure that (i) access to Personal Data by its Personnel is limited to need to know and/or access basis to perform the Subscription Agreement, (ii) such Personnel are subject to written confidentiality undertakings or statutory obligations of confidentiality, and (iii) such Personnel receives appropriate training.

5. **SUBPROCESSORS**

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

5.2. All Cloudinary's Sub-Processors have entered into written agreements with Cloudinary that bind them by substantially similar material obligations under this DPA.

5.3. Where a Cloudinary's Sub-Processor fails to fulfil its data protection obligations in connection with the Processing of Personal Data, Cloudinary will remain fully liable to Customer for the performance of that Cloudinary Sub-Processor's obligations.

5.4. Cloudinary may replace or engage with a new Sub-Processor ("**New Sub-Processor**") to Process Personal Data on Customer's behalf. Cloudinary will notify the Customer of the intended engagement with the New Sub-Processor ten (10) days prior to such engagement. Customer may object to the Processing of Customer's Personal Data by the New Sub-Processor, for reasonable and explained grounds relating to data protection, within ten (10) days following Cloudinary's written notice to Customer of the intended engagement with the New Sub-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 Services, without using the New Sub-Processor to Process Customer's Personal Data, to the extent feasible.

6. **ONWARD AND TRANS-BORDER DATA TRANSFER**

6.1. General; Data Privacy Framework. Cloudinary will comply with the rules on onward and trans-border data transfers specified in Privacy Laws and Regulations. To the extent Cloudinary, Inc. Processes any Personal Data originating from the European Economic Area ("**EEA**") or Switzerland, Cloudinary represents that Cloudinary Inc. is self certified under the Data Privacy Framework and complies with the Data Privacy Principles when Processing any such Personal Data. To the extent that Customer is (a) located in the United States of America and is self-certified under the Data Privacy Framework or (b) located in the EEA or Switzerland, Cloudinary further agrees (i) to provide at least the same level of protection to any Personal Data as required by the Data Privacy Principles; (ii) to notify Customer in writing, without undue delay, if its self certification to the Data Privacy Framework is withdrawn, terminated, revoked, or otherwise invalidated (in which case, an alternative transfer mechanism will apply in accordance with the remainder of this Section 6); and (iii) upon written notice, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized Processing of Personal Data.

6.2. Customer agrees that Cloudinary may Processes Personal Data governed by the EU GDPR in a country that has been recognized by the European Commission as providing an adequate level of protection for Personal Data. To the extent Cloudinary Processes any Personal Data governed by the EU GDPR in a country that has not been recognized by the European Commission, as providing an adequate level of protection for Personal Data, the Personal Data shall be transferred by virtue of the following lawful transfer mechanism:

6.2.1. For the purpose of this DPA, the parties agree that the standard contractual clauses as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, including all Annexes thereto, as may be amended or replaced from time to time ("**EU SCCs**") are incorporated herein by reference and the parties are deemed to have accepted and signed the EU SCCs where necessary in their entirety. For all intents and purposes, Annexes I and II of this DPA, shall be deemed to be Annexes I and

II of the EU SCCs and Annex III of the EU SCCs is the list of Cloudinary's Sub-Processors available at: https://cloudinary.com/subprocessors. If and

to the extent the EU SCCs conflict with any provision of this DPA, the EU SCCs will prevail to the extent of such conflict.

6.2.2. For the purpose of this DPA, the parties agree that Module Two (Controller to Processor) of the EU SCCs or Module Three (Processor to Processor), as the case may be, will apply.

6.3. The parties agree that with respect to the election of specific terms and/or optional clauses required by the EU SCCs, the following shall apply and any optional clauses not expressly selected are not included:

6.3.1. Between the parties, Customer will be deemed the "data exporter" and Cloudinary will be deemed the "data importer";

6.3.2. In Clause 7, the optional docking clause will not apply;

6.3.3. If applicable - in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes will be as set out in Section 5 of this DPA;

6.3.4. In Clause 11, the optional language will not apply;

6.3.5. In Clause 17, Option 1 will apply, and the EU SCCs will be governed by the Irish law;

6.3.6. In clause 18(b), disputes will be resolved before the courts of Ireland.

6.4. In the event Cloudinary receives any subpoena, warrant or other judicial, regulatory, governmental or administrative order by a government or quasi-governmental or other regulatory authority (including law enforcement or intelligence agencies) seeking or requiring access to or disclosure of Customer's Personal Data ("Government Authority Request"), and unless required by a valid court order or if otherwise Cloudinary may face criminal charges for failing to comply with orders or demands to disclose or otherwise provide access to EEA Personal Data, or where the access is requested in the event of imminent threat to lives, Cloudinary will:

6.4.1. not purposefully create back doors or similar programming that could be used to access EEA Personal Data;

6.4.2. not provide the source code or encryption keys to any government agency for the purpose of accessing EEA Personal Data; and

6.4.3. upon Customer's written request, provide reasonable available information about the requests of access to Personal Data by government agencies Cloudinary has received in the 6 months preceding to Customer's request.

6.4.4. notify Customer of such Government Authority Request to enable the Customer to take necessary actions, to communicate directly with the relevant authority and to respond to the request. If Cloudinary is prohibited by law to notify the Customer of such Government Authority Request, Cloudinary will make reasonable efforts to challenge such prohibition through judicial action or other means at Customer's expense and, to the extent possible, will provide only the minimum amount of information necessary.

6.5. Customer agrees that Cloudinary may Processes Personal Data governed by the UK GDPR in a country that has been recognized pursuant to the UK GDPR as providing an adequate level of protection for Personal Data. To the extent Cloudinary Processes any Personal Data governed by the UK GDPR, either directly or via onward transfer, in a country that has not been recognized pursuant to the UK GDPR, as providing an adequate level of protection for Personal Data, the Personal Data shall be transferred by virtue of the following lawful transfer mechanism:

6.5.1. For the purpose of this DPA, the parties agree that International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as approved by the Information Commissioner's Office (ICO) under S119A(1) Data Protection Act 2018 and in force 21 March 2022 ("**UK Addendum**") is incorporated herein by reference and the parties are deemed to have accepted and signed the UK Addendum where necessary in their entirety.

6.5.2. The parties agree that with respect to the election of specific terms and/or optional clauses required by the UK Addendum the following shall apply and any optional clauses not expressly selected are not included:

6.5.2.1. In Part 1: Tables – (i) Table 1: Parties – Start date is the start date of the Subscription Agreement between Cloudinary and the Customer; as between the parties, Customer will be deemed the "data exporter" and Cloudinary will be deemed the "data importer"; (ii) Table 2: Selected SCCs, Modules and Selected Clauses: the box "the version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information" is checked and the date is the Subscription Agreement date; (iii) Table 3: Appendix Information - Annex 1A: List of Parties: Cloudinary and the Customer as set out in the Subscription Agreement; Annex 1B: Description of Transfer: as set out in Annex I; Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: as set out in Annex II; Annex III: List of Sub-Processors (Modules 2): the sub processor(s) list

available at: https://cloudinary.com/subprocessors; (iv) Table 4: Ending this Addendum when the Approved Addendum Changes – the boxes "Importer" is checked;

6.5.2.2. In Part 2: Mandatory Clauses is applicable.

7. **INFORMATION SECURITY**. Cloudinary will implement and maintain appropriate administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data, as further specified under Annex II of this DPA. Cloudinary regularly monitors compliance with these safeguards. Cloudinary will not materially decrease the overall security of the Services during the term of the Subscription Agreement.

8. **PERSONAL DATA BREACH MANAGEMENT AND NOTIFICATION**

8.1. Cloudinary will notify Customer without undue delay, and in any event within 72 hours, after becoming aware of a Personal Data Breach related to Customer's Personal Data. 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 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 insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without further delay.

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

8.3. In the event of a Personal Data Breach, any notification to the relevant Supervisory Authorities or Data Subjects, if required, will be the responsibility of the Customer, unless otherwise specified in Privacy Laws and Regulations, and Cloudinary shall reasonably assist Customer upon request.

8.4. 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 majeure, 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. Following Customer's reasonable request, Cloudinary will make available to Customer available information necessary for Customer to demonstrate compliance with the Privacy Laws and Regulations.

9.2. To the extent required under applicable Privacy Laws and Regulations, upon Customer's written request (not more frequently than annually), and subject to reasonable confidentiality obligations, Cloudinary will make available to Customer a copy of Cloudinary's most recent audit report, certifications and summaries of audit reports conducted by accredited third party auditors.

9.3. To the extent that Cloudinary's provision of an audit report does not provide sufficient information or Customer is required to respond to a regulatory authority audit, Customer may conduct an audit of Cloudinary's processing, 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's 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 Cloudinary 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. **DATA RETENTION**

10.1. **Personal Data Deletion**. Unless otherwise required by applicable law or agreed in writing between the parties, Cloudinary will delete the Customer's Personal Data within 30 days following termination or expiration of the Services.

10.2. **Data Retention**. Customer acknowledges and agrees that Cloudinary may retain copies of Customer's 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 Customer's

Personal Data pursuant to legal requirements and to use such Customer's Personal Data to protect Cloudinary, its affiliates, agents, and any person on their behalf in court and administrative proceedings.

11. **DISPUTE RESOLUTION**. 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 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.

12. **LIMITATION OF LIABILITY**. 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.

13. **TERM**. 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.

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

ANNEX I

A. LIST OF PARTIES

1. **Data exporter(s):** Customer

   Name: as detailed in the Order Form (as defined in the Subscription Agreement).

   Address: as detailed in the Order Form.

   Contact person's name, position and contact details: as detailed in the Order Form.

   Activities relevant to the data transferred under these Clauses: receipt of Services pursuant to the Subscription Agreement.

   Signature and date: By entering into the Order Form, data exporter is deemed to have signed these EU SCCs incorporated herein, including their Annexes, as of the effective date of the Order Form. **Role**: Controller

2. **Data importer(s)**:

   Name: Cloudinary Ltd. or its subsidiary from which Customer is acquiring (directly or through an authorized distributor or reseller) the Services listed in the Order Form

   Address: as detailed in the Order Form

   Contact person's name, position and contact details: Data Protection Officer, at privacy@cloudinary.com and support@cloudinary.com

   Activities relevant to the data transferred under these Clauses: provide the Services pursuant to the Subscription Agreement.

   Signature and date: By entering into the Order Form, data importer is deemed to have signed these EU SCCs incorporated herein, including their Annexes, as of the effective date of the Order Form. **Role**: Processor

B. DESCRIPTION OF TRANSFER

- ***Categories of data subjects whose Personal Data is transferred***:

  Customer Data Subjects as determined by the Customer (Cloudinary has no control over the categories of Data Subjects).

- ***Categories of personal data transferred***:

  Personal Data as determined by the Customer (Cloudinary has no control over the categories of Personal Data that is transferred).

- ***Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved***: N/A

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

  Continuous basis.

- ***Nature of the processing***:

  All operations 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 of data (whether or not by automated means), etc.

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

  The provision of the Services in accordance with the Subscription Agreement.

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

  Personal Data will be retained during the term of the Subscription Agreement and will be deleted in accordance with Section 10 of the DPA.

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

  The subject matter of the Processing is Customer's Personal Data, the nature of the Processing is the performance of the Services under the Subscription Agreement and as detailed above and the duration of the Processing is the term of the Subscription Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

- ***Identify the competent supervisory authority in accordance with Clause 13:*** Irish DPC

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF DATA

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, which Cloudinary is certified to, as its baseline.

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

1. **Information Security Management System – Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing**

   Cloudinary has an ISMS (Information Security Management System) in place to evaluate risks to the security of Personal 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's Personal Data**

   Cloudinary conducts background checks (subject to local restrictions) on all Personnel who may interact with Customer's Personal Data as part of their duties, regardless of specific Customer requirements. As part of the onboarding processes, Cloudinary provides the necessary trainings about protecting and securing Customer's Personal Data to such authorized Personnel.

3. **Physical Access – Measures for ensuring physical security of locations at which Personal Data are Processed**

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

   Customer's Personal 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's 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://aws.amazon.com/compliance/data-center/controls/.

4. **System Security – Measures for user identification and authorization**

   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. **Personal Data Access – Measures for the protection of Personal Data during storage**

   Role-based user and administrator access to Customer's Personal 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 Personal Data; Logging of privileged account use and access to sensitive Personal 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. **Personal Data Transfer – Measures for the protection of Personal Data during transmission**

All Personal 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's Personal Data does not employ vulnerable protocols or weak ciphers. For Personal Data at rest, industry-standard AES-256 encryption is being used.

7. **Instructions – Implementation of controls designed to ensure Customer's Personal Data is only Processed in accordance with Customer's instructions**

Cloudinary has in place internal policies containing formal instructions for Personal Data processing procedures; Contractors are being carefully vetted with regard to Personal Data security; Cloudinary's 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 – Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident**

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 Customers' 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's 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. **Measures for ensuring events logging**

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. **Measures for ensuring limited Personal Data retention**

Upon request and pursuant to contractual obligations, Cloudinary is able to completely and permanently delete specific or all Customer's Personal Data from its production environment.