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 Master 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 the 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.

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

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 transmitted, stored or otherwise processed.

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

1.5. "**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**"), the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**") and California Consumer Privacy Act of 2018 Cal. Civil Code § 1798.100 et seq. ("**CCPA**").

1.6. "**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.

1.7. "**Third Country**" is a country outside the European Economic Area or the UK which was not acknowledged by the EU Commission or a UK Secretary of State as providing an adequate level of protection in accordance with Article 45(3) of the GDPR or Article 45 of the UK GDPR.

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 and the UK 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 Services 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. Cloudinary will notify the Customer of the intended engagement with the New Processor ten (10) days prior to such engagement. 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 GDPR governed Customer's Personal Data ("**EEA Transferred Data**") to a Third Country is made in accordance with the EU Standard Contractual Clauses ("**EU SCCs**"), pursuant to EU Commission Decision C(2021)3972, in the module specified in **Exhibit A** which is attached and incorporated by reference to this DPA, or, as required, in accordance with any successor thereof or an alternative lawful data transfer mechanism, and as follows:

6.1.1. In Clause 7, the optional docking clause will apply;

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

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

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

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

6.2. In accordance with Article 46 of the GDPR and the EU SCCs, and without prejudice to any provisions of this DPA, Cloudinary undertakes to implement the following organizational and technical safeguards, in addition to the safeguards mandated by the EU SCCs to ensure the required adequate level of protection to the EEA Transferred Data:

6.2.1. Cloudinary will implement and maintain the technical and organizational measures, as specified in Annex II of Exhibit A, which is attached and incorporated by reference to this DPA, with a purpose to protect Customer Personal Data against any processing for national security or other government purposes that goes beyond what is necessary and proportionate in a democratic society, considering the type of processing activities under the Subscription Agreement and relevant circumstances;

6.2.2. For the purposes of safeguarding EEA Transferred Data when any Third Country's government or regulatory authority requests access to such data ("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 Transferred Data, or where the access is requested in the event of imminent threat to lives, Cloudinary will:

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

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

6.2.2.3. 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.

6.2.3. If Cloudinary receives a request by a government agency to access Customer Personal Data, Cloudinary will notify Customer of such 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 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.

6.3. Transfer of UK GDPR-governed Customer's Personal Data ("**UK Transferred Data**") to a Third Country, is either:

6.3.1. made in accordance with the EU Standard Contractual Clauses ("**Previous EU SCCs**"), pursuant to EU Commission Decision 2010/87/EU of 5 February 2010, as officially published at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=EN, or other official publications of the European Union, *mutatis mutandis*, for as long as it is lawfully permitted to rely on in accordance with the UK GDPR, and on the following basis:

6.3.1.1. Appendix 1 to the Previous EU SCCs will be completed with the relevant information set out in Annex I to this DPA;

6.3.1.2. Appendix 2 will be completed with the relevant information set out in Annex II to this DPA;

6.3.1.3. The optional illustrative indemnification Clause under Appendix 2 of the Previous EU SCCs will not apply; and

or -

6.3.2. where Section 6.3.1 above does not apply, however the parties are lawfully permitted to rely on the EU SCCs in relation to the UK Transferred Data subject to completion of a "UK Addendum to the EU Standard Contractual Clauses ("**UK Addendum**") issued by the UK Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 (officially published at: draft-ico-addendum-to-com-scc-20210805.pdf, as a draft), and officially published by the Information Commissioner's Office, then:

6.3.2.1. the EU SCCs giving effect to the module specified in Exhibit A which is attached and incorporated by reference to this DPA, will also apply to UK Transferred Data, subject to Sections 6.1 and 6.2 above;

6.3.2.2. the UK Addendum will be deemed executed between the parties, and the EU SCCs will be deemed amended as specified by the UK Addendum in relation to the UK Transferred Data.

or –

6.3.3. If neither Section 6.3.1 and 6.3.2 apply, then the parties will cooperate in good faith to implement appropriate safeguards for transfers of UK Transferred Data, as required or permitted by the UK GDPR without undue delay.

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, as further specified under Annex II of **Exhibit A**. 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 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 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. 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

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.

Exhibit A

Standard Contractual Clauses

ANNEX to the COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as officially published at: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf or other official publications of the European Union as updated from time to time:

MODULE TWO: Transfer controller to processor

OR

MODULE THREE: Transfer processor to processor

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Customer whose name, address and contact details are further set out in the Subscription Agreement. The Customer (in its role as a controller or processor) will provide certain personal data in order to receive the Services pursuant to the Subscription Agreement.

Data importer(s)*:* Cloudinary whose name, address and contact details are further set out in the Subscription Agreement. Cloudinary (in its role as a processor) will process personal data in order to provide the Services pursuant to the Subscription Agreement.

B. DESCRIPTION OF TRANSFER

- Categories of data subjects whose personal data is transferred:

  Cloudinary has no control over the categories of data subjects whose personal data is transferred.

- Categories of personal data transferred:

  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, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

  Cloudinary has no control over the categories of personal data that is transferred.

- 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 that is 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 the terms therein.

- 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

Where the data exporter is established in an EU Member State - the supervisory authority of such EU Member State shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) - the supervisory authority of the Member State in which the representative is established shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) - the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses, shall act as competent supervisory authority.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE 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 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 – 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 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 – 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 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 – 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. **Data Access – Measures for the protection of data during storage**

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 – Measures for the protection of data during 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 – 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 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. 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 data retention

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.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.