Notes on this Pre-signed DPA

The CloudFiles Data Processing forms part of the CloudFiles Customer Terms of Service available at https://www.cloudfiles.io/terms-of-service. We have made this pre-signed copy of the CloudFiles Data Processing Agreement available for you. You do not need to sign and return to CloudFiles. This copy includes signatures on the DPA version last modified June 02, 2022, followed by a complete copy of the Standard Contractual Clauses and UK Addendum, which are incorporated by reference within the DPA.

Any changes made to this copy are not agreed to by CloudFiles Technologies Inc or its affiliates. Please note that we update the Data Processing Agreement as we describe in the 'Amendments' section below. Current Data Processing Agreement terms are available at https://cloudfiles.io/legal/dpa and archived Data Processing Agreement terms are available at https://cloudfiles.io/legal/dpa/archive.

If you have any questions, please contact us at privacy@cloudfiles.io.

CloudFiles

w: https://cloudfiles.io

Data Processing Addendum

Customer Name(**"Customer"**): _____

THIS DATA PROCESSING ADDENDUM ("DPA") forms part of the Terms of Use (or other similarly titled written or electronic agreement addressing the same subject matter) ("**Agreement**") between Customer (the **"Controller"),** and **CloudFiles** (the **"Processor")** under which the Processor provides the Controller the software and services (the **"Services")** The Controller and the Processor are individually referred to as a **"Party"** and collectively as the **"Parties".**

The Parties seek to implement this DPA to comply with the requirements of GDPR (defined hereunder) in relation to Processor's processing of Personal Data (as defined under the GDPR) as part of its obligations under the Agreement.

This DPA shall apply to Processor's processing of Personal Data, provided by the Controller as part of Processor's obligations under the Agreement.

Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. **Definitions.**

Capitalized terms not otherwise defined herein shall have the meaning given to them in the GDPR or the Agreement. The following terms shall have the corresponding meanings assigned to them below:

1.1. **"Data Transfer"** means (1) a transfer of the Personal Data from the Controller to the Processor, or between two establishments of the Processor, or with a Sub-processor by the Processor.

1.2. "**GDPR**" means the 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 (General Data Protection Regulation).

1.3. "**Standard Contractual Clauses**" means the contractual clauses attached hereto as Schedule I pursuant to the European Commission's IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection.

1.4. "**Sub-processor**" means a processor/ sub-contractor appointed by the Processor for the provision of all or parts of the Services and Processes the Personal Data as provided by the Controller.

2. Purpose of this Addendum:

This DPA sets out various obligations of the Processor in relation to the Processing of Personal Data and shall be limited to the Processor's obligations under the Agreement. If there is a conflict between the provisions of the Agreement and this DPA, the provisions of this DPA shall prevail.

3. **Categories of Personal Data and Data Subjects**. The Controller authorizes the Processor to Process such Personal Data the extent of which is determined and controlled by the Controller. The current nature of the Personal Data is specified in Annex 1 of Schedule 1 to this DPA.

4. **Purpose of Processing.** The objective of Processing of Personal Data by the Processor shall be limited to the Processor's provision of the Services to the Controller and or its Client, pursuant to the Agreement.

5. **Duration of Processing.** The Processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing by the Controller.

6. **The Processor's obligations.**

   a. The Processor will follow written and documented instructions received, including by email, from the Controller, its affiliate, agents or personnel, with respect to the Processing of Personal Data (each, an "**Instruction**").

   b. The Processing described in the Agreement and the relating documentation shall be considered as Instruction from the Controller.

c. The Processor will notify Controller if an Instruction, in Processor's opinion, infringes the GDPR and further reserves its right not to provide any further assistance on such reported Instruction.

d. At the Controller's request, the Processor will provide reasonable assistance to the Controller in responding to/ complying with requests / directions by Data Subject in exercising their rights or of the applicable regulatory authorities regarding Processor's Processing of Personal Data.

7. Data Secrecy.

To Process the Personal Data, the Processor will use personnel who are (i) informed of the confidential nature of the Personal Data, (ii) actually performing the Services in accordance with the Agreement. The Processor will regularly train individuals having access to Personal Data in data security and data privacy in accordance with accepted industry practice and shall ensure that all the Personal Data is kept as strictly confidential. Further, the Processor will maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of the Personal Data as per the specifications as per the standards mutually agreed in writing by the Parties.

8. Audit Rights.

a. Upon the Controller's reasonable request, the Processor will make available to the Controller, information as is reasonably necessary to demonstrate Processor's compliance with its obligations under the GDPR or other applicable laws in respect of its Processing of the Personal Data. When the Controller wishes to conduct the audit (by itself or through a representative) at Processor's site, it shall provide at least fifteen (15) days' prior written notice to the Processor; the Processor will provide reasonable cooperation and assistance in relation to audits, including inspections, conducted by the Controller or its representative.

b. The Controller shall bear the expense of such an audit.

9. Mechanism of Data Transfers.

Any Data Transfer for the purpose of Processing by the Processor in a country outside the European Economic Area (the "***EEA***") shall only take place in compliance with the Standard Contractual Clauses as detailed in Schedule 1 to the DPA. Where such model clauses have not been executed at the same time as this DPA, the Processor shall not unduly withhold the execution of such template model clauses, where the transfer of Personal Data outside of the EEA is required for the performance of the Agreement.

10. Sub-processors.

a. The Controller acknowledges and agrees that the Processor, may engage a third-party Sub-processor(s) in connection with the performance of the Services, provided such Sub-processor(s) take technical and organizational measures to ensure confidentiality of Personal Data shared with them; The current Sub-processors engaged by the Processors and approved by the Controller are listed in Annex 3 of Schedule 1 hereto. In accordance with Article 28(4) of the GDPR, the Processor shall remain liable to the Controller for any

failure on behalf of a Sub-processor to fulfil its data protection obligations under the DPA in connection with the performance of the Services.

b. If the Controller has a concern that the Sub-processor(s) Processing of Personal Data is reasonably likely to cause the Controller to breach its data protection obligations under the GDPR, the Controller may object to Processor's use of such Sub-processor and the Processor and Controller shall confer in good faith to address such concern.

11. Personal Data Breach Notification.

a. The Processor shall maintain defined procedures in case of a Personal Data Breach (as defined under the GDPR) and shall without undue delay notify Controller if it becomes aware of any Personal Data Breach, unless such Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.

b. The Processor shall provide the Controller with all reasonable assistance to comply with the notification of Personal Data Breach to the Supervisory Authority and/or the Data Subject, to identify the cause of such Data Breach and take such commercially reasonable steps as reasonably required to mitigate and remedy such Data Breach.

c. No Acknowledgement of Fault by Processor. Processor's notification of or response to a Personal Data Breach under this DPA will not be construed as an acknowledgement by Processor of any fault or liability with respect to the data incident.

12. Return and Deletion of Personal Data.

a. The Processor shall at least thirty (30) days from the end of the Agreement or cessation of the Processor's Services under the Agreement, whichever occurs earlier, shall return to the Controller all the Personal Data, or if the Controller so instructs, the Processor shall have the Personal Data deleted. The Processor shall return such Personal Data in a commonly used format or in the then current format in which it was stored at discretion of the Controller, soon as reasonably practicable following receipt of Controller's notification.

b. In any case, the Processor shall delete Personal Data including all the copies of it as soon as reasonably practicable following the end of the Agreement.

13. Technical and Organizational Measures.

Having regard to the state of technological development and the cost of implementing any measures, the Processor will take appropriate technical and organizational measures against the unauthorized or unlawful processing of Personal Data and against the accidental loss or destruction of, or damage to, Personal Data to ensure a level of security appropriate to: (a) the harm that might result from unauthorized or unlawful processing or accidental loss, destruction or damage; and (b) the nature of the data to be protected [including the measures stated in Annex 2 of Schedule 1].

14. Amendments

Notwithstanding anything else to the contrary in the Agreement and without prejudice to the 'Compliance with Instructions' or 'Security' sections of this DPA, we reserve the right to make any updates and changes to this DPA.

EXECUTED BY THE PARTIES AUTHORIZED REPRESENTATIVES:

Cloudfiles Technologies Inc.

38350 Fremont Blvd , Suite 203

Fremont CA 94536

United States

Signature:

Name: Ankit Gupta

Title: CTO

Customer Name

_____

Address:

Signature:

Name:

Title:

Date:

Schedule 1

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and Scope

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

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);

(b)Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a)Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b)These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c)These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a)The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b)The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union

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

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

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

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

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

8.9 **Documentation and compliance**

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

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

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

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

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

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 7 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

(a)Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

(i)the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii)the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards

(iii)any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

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

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

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

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

Clause 15

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

15.1 **Notification**

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

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to

these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

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

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

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

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

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

15.2 **Review of legality and data minimization**

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member States, provided such laws allow for third-party beneficiary rights. The Parties agree that this shall be the laws of Ireland.

Clause 18

Choice of forum and jurisdiction

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

(b)The Parties agree that those shall be the courts of the jurisdiction specified in Clause 17.

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

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

ANNEX I

Data exporter: The data exporter is the legal entity executing the Agreement as Customer, and who is engaging CloudFiles to provide the cloud-based file sharing services, defined in the Agreement as "Services."

Data importer: The data importer is CloudFiles, the provider of the Services, as defined in the Agreement. CloudFiles' entity and contact details are set forth in the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer may submit Personal Data in the course of using the Service, the extent of which is determined and controlled by Customer in its sole discretion, which may include the Personal Data of Customer's end users receiving CloudFiles links, as well as Customer's authorized users of the Services.

Categories of personal data transferred

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to the following categories of Personal Data:

a. information about your customer's users of the application and device information.

b. information about end users (e.g., names, email addresses, and telephone numbers) and their file browsing activity, location, and device information

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not Applicable

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

Continuous

Nature of the processing

Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

a. Storage and other Processing necessary to provide, maintain and improve the Services provided to Customer; and/or

b. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

Purpose(s) of the data transfer and further processing

CloudFiles will Process Personal Data as necessary to provide the Services pursuant to the Agreement, as further specified in the Order Form, and as further instructed by Customer in their use of the Services.

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

Deleted on Customer's request or 30 days after the termination of Agreement

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

The period for which Customer's Personal Data will be retained in the Services is determined by Customer during the term of the Agreement. Upon termination of the Agreement, Customer may retrieve or delete its Personal Data as set forth in the Agreement and this DPA and CloudFiles will destroy (including on all Subprocessor systems) Customer's Personal Data within the timeline described in this DPA.

C.COMPETENT SUPERVISORY AUTHORITY

For the purposes of the Standard Contractual Clauses, the supervisory authority that shall act as competent supervisory authority is either (i) where Customer is established in an EU Member State, the supervisory authority responsible for ensuring Customer's compliance with the GDPR; (ii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU Member State in which Customer's representative is established; or (iii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR without having to appoint a representative, the supervisory authority of the EU Member State in which the Data Subjects are predominantly located. In relation to Personal Data that is subject to the UK GDPR or Swiss DPA, the competent supervisory authority is the UK Information Commissioner or the Swiss Federal Data Protection and Information Commissioner (as applicable).

ANNEX II

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into

account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures of pseudonymisation and encryption of personal data	CloudFiles maintains Customer Data in an encrypted format at rest using Advanced Encryption Standard and in transit using TLS.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	CloudFiles' customer agreements contain strict confidentiality obligations. Additionally, CloudFiles requires every downstream Subprocessor to sign confidentiality provisions that are substantially similar to those contained in CloudFiles' customer agreements. The infrastructure for the CloudFiles Services spans multiple fault-independent AWS availability zones in geographic regions physically separated from one another, supported by various tools and processes to maintain high availability of services.
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	CloudFiles performs regular backups of Customer Data, which is hosted in AWS data centers. Backups are retained redundantly across multiple availability zones and encrypted in transit and at rest using Advanced Encryption Standard (AES-256).
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	CloudFiles maintains a risk-based assessment security program. The framework for CloudFiles' security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data. CloudFiles' security program is intended to be appropriate to the nature of the Services and the size and complexity of CloudFiles' business operations. CloudFiles facilitates and supports independent audits and assessments performed by third-parties to provide independent feedback on the operating effectiveness of the information security program.
Measures for user identification and authorization	CloudFiles personnel are required to use unique user access credentials and passwords for authorization. CloudFiles follows the principles of least privilege through role-based and time-based access models when provisioning system access. CloudFiles personnel are authorized to access Customer Data based on their job function, role and responsibilities, and such access requires approval prior to access provisioning. Access is promptly removed upon role change or termination.
Measures for the protection of data during transmission	Customer Data is encrypted when in transit between Customer and CloudFiles Services using TLS 1.2.
Measures for the protection of data during storage	Customer Data is stored encrypted using the Advanced Encryption Standard.

Measures for ensuring physical security of locations at which personal data are processed	The Services operate on Amazon Web Services ("AWS") and are protected by the security and environmental controls of Amazon. Detailed information about AWS security is available at https://aws.amazon.com/security/ and https://aws.amazon.com/security/sharing-the-security-responsibility/. For AWS SOC Reports, please see https://aws.amazon.com/compliance/soc-faqs/.
Measures for ensuring events logging	CloudFiles monitors access to applications, tools, and resources that process or store Customer Data, including cloud services. Log activities are investigated when necessary and escalated appropriately.
Measures for ensuring system configuration, including default configuration	CloudFiles applies Secure Software Development Lifecycle (Secure SDLC) standards to perform numerous security-related activities for the Services across different phases of the product creation lifecycle from requirements gathering and product design all the way through product deployment. These activities include, but are not limited to, the performance of (a) internal security reviews before new Services are deployed; (b) annual penetration testing by independent third parties; and (c) threat models for new Services to detect any potential security threats and vulnerabilities. CloudFiles adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. Monitors are in place to notify the security team of changes made to critical infrastructure and services that do not adhere to the change management processes.
Measures for internal IT and IT security governance and management	CloudFiles maintains a risk-based assessment security program. The framework for CloudFiles' security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data. CloudFiles' security program is intended to be appropriate to the nature of the Services and the size and complexity of CloudFiles' business operations. Security is managed at the highest levels of the company, with the Chief Security Officer meeting with executive management regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are reviewed and approved by management at least annually and are made available to all CloudFiles employees for their reference.
Measures for certification/assurance of processes and products	CloudFiles conducts third-party audits to attest to SOC 2 Type 2 and annual application penetration testing.

Measures for ensuring data minimization	CloudFiles Customers determine what Customer Data they collect through the CloudFiles Services. By default, CloudFiles collect minimum information required to distinguish between the unique viewers of the links.
Measures for ensuring data quality	CloudFiles performs validation checks to ensure that the input values match expected values during the collection.
Measures for ensuring limited data retention	CloudFiles deletes Customer Data upon the Customer's written request, within the timeframe specified in the Data Protection Addendum and in accordance with Applicable Data Protection Law.
Measures for ensuring accountability	CloudFiles has adopted measures for ensuring accountability, such as implementing data protection policies across the business, maintaining documentation of processing activities, recording and reporting Security Incidents involving Personal Data. Additionally, CloudFiles conducts regular third-party audits to ensure compliance with our privacy and security standards.
Measures for allowing data portability and ensuring erasure	CloudFiles' Customers have direct relationships with their end users and are responsible for responding to requests from their end users who wish to exercise their rights under Applicable Data Protection Laws. CloudFiles will provide assistance to Customer as may reasonably be require to comply with Customer's obligations under Applicable Data Protection Laws to respond to requests from individuals to exercise their rights under Applicable Data Protection Laws (e.g., rights of data access, rectification, erasure, restriction, portability and objection). If CloudFiles receives a request from a Data Subject in relation to their Customer Data, CloudFiles will advise the Data Subject to submit their request to Customer, and Customer will be responsible for responding to any such request.
For transfers to (sub-) processors, also describe the specific technical and organisational 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.	When CloudFiles engages a sub-processor under this Addendum, CloudFiles and the sub-processor enter into an agreement with data protection terms substantially similar to those contained herein. Each sub-processor agreement must ensure that CloudFiles is able to meet its obligations to Customer. In addition to implementing technical and organisational measures to protect personal data, sub-processors must a) notify CloudFiles in the event of a Security Incident so CloudFiles may notify Customer; b) delete data when instructed by CloudFiles in accordance with Customer's instructions to CloudFiles; c) not engage additional sub-processors without authorization; d) not change the location where data is processed; or e) process data in a manner which conflicts with Customer's instructions to CloudFiles.

ANNEX III

LIST OF SUB-PROCESSORS

SubProcessor	Purpose	Location	Transfer Mechanism
Amazon Web Services	Cloud hosting and infrastructure provider	United States	SCCs
Cloudflare	DNS, CDN, DDOS protection	United States	SCCs
HubSpot	Email marketing/Sales management/Customer support	United States	SCCs
GitHub	Source Code	United States	SCCs
Posthog	In-application analytics	United States	SCCs
Stripe	Payments	United States	SCCs