



Data Protection Addendum

(Revision October 2023)

This Data Processing Addendum (collectively with all schedules, annexes, and exhibits, this “**Addendum**”) forms part of the agreement(s) (the “**Agreement**”) previously entered into by and between CodeLathe Technologies Inc. dba FileCloud and its subsidiaries (the “**Company**” or “**FileCloud**”) and the customer (the “**Customer**”) for the purchase of FileCloud Online services including associate mobile components, and reflects the parties’ agreement with regard to the Processing of Personal Data in accordance with the requirements of the Data Protection Laws as defined below.

Customer enters into this Addendum on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates. For the purposes of this Addendum only, and except where indicated otherwise, the term “Customer” shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In the course of providing the services to Customer pursuant to the Agreement, FileCloud may process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

HOW TO EXECUTE THIS ADDENDUM:

1. This Addendum has been pre-signed on behalf of FileCloud.
2. To complete this Addendum, Customer must: (a) Complete the information in the signature box and sign on page 11. (b) Send the signed DPA to FileCloud by email to dpo@filecloud.com indicating, if applicable, the Customer’s legal entity name as set out on the applicable FileCloud Order Form or invoice. Except as otherwise expressly provided in the Agreement, this Addendum will become legally binding upon receipt by FileCloud of the validly completed DPO email address. For the avoidance of doubt, signature of the Addendum on page 11 shall be deemed to constitute signature and acceptance.

HOW THIS ADDENDUM APPLIES:

- a. If the Customer entity signing this Addendum is a party to the Agreement, this Addendum is an addendum to and forms part of the Agreement, and the FileCloud entity that is a party to the Agreement is a party to this Addendum.



- b. If the Customer entity signing this Addendum has executed orders under the Agreement but is not a party to the Agreement, this Addendum will be incorporated in such order(s) and the Company entity that is a party to such order(s) will be a party to this Addendum.
- c. This Addendum will not be valid and legally binding if the signing Customer entity is not a party to the Agreement or order(s) or is an indirect customer through an authorized reseller. An indirect customer should contact the authorized reseller about its contract with that reseller.
- d. This Addendum shall apply only to the extent the Company processes Personal Data of Data Subjects on behalf of Customer or a Customer Affiliate as defined under the applicable Data Protection Law.

IT IS AGREED AS FOLLOWS:

1. Definitions

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 “**Affiliate**” means any legal entity directly or indirectly controlling, controlled by or under common control with a party, where control means the ownership of a majority share of the stock, equity or voting interests of such entity.

1.1.2 “**Customer Personal Data**” means any Personal Data Processed by the Company pursuant to or in connection with the Agreement;

1.1.3 “**Data Protection Laws**” means EU Data Protection Laws and the California Consumer Privacy Act of 2018, as amended, replaced or superseded;

1.1.4 “**EEA**” means the European Economic Area which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein, as well as, for the purposes of this Addendum, the United Kingdom and Switzerland;

1.1.5 “**EU Data Protection Laws**” means all data protection laws and regulations applicable to Europe, including (i) GDPR; (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); (iv) the GDPR as it forms part of UK law by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (together, “**UK Data Protection Laws**”); and (v) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance (“**Swiss DPA**”), all as amended, replaced or superseded;



1.1.6 “**GDPR**” means EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council 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, as amended, replaced or superseded;

1.1.7 “**Data Transfer**” means:

1.1.7.1 a transfer of Customer Personal Data from the Customer to the Company; or

1.1.7.2 an onward transfer of Customer Personal Data from the Company to a Sub-processor, or between two establishments of Sub-processors, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.8 “**Services**” means activities performed by the Company related to the Agreement.

1.1.9 “**Standard Contractual Clauses**” means: (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 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 (“**EU SCCs**”), (ii) where UK Data Protection Laws apply, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR (“**UK SCCs**”); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the “**Swiss SCCs**”).

1.1.10 “**Sub-processor**” means any Processor engaged by the Company to process Personal Data on behalf of the Customer in connection with the Agreement.

1.2 The terms, “**Commission**”, “**Controller**”, “**Data Subject**”, “**Data Exporter**”, “**Data Importer**”, “**Member State**”, “**Personal Data**”, “**Personal Data Breach**”, “**Processing**”, “**Processor**” and “**Supervisory Authority**” shall have the same meaning as in the Data Protection Laws, and their cognate terms shall be construed accordingly.

2. Processing of Personal Data



2.1 Parties' Roles. Customer appoints FileCloud to process the Personal Data on Customer's behalf, and the Company agrees to process the Personal Data as a data Processor on behalf of the Customer in accordance with this Addendum.

2.2 Purpose Limitation. The Company shall:

2.2.1 Process Personal Data in furtherance of the Company's provision of Services to Customer and comply with all applicable Data Protection Laws in the Processing of Personal Data; and

2.2.2 Process Personal Data only in accordance with the Customer's documented instructions, provided this Addendum shall be considered Customer's documented instructions for the Company to perform such Processing and any other changes to these instructions (inclusive of the rights and obligations set forth under the Agreement) will require written agreement of the parties hereto.

2.3 Compliance. Customer, as Controller, shall be responsible for ensuring that, in connection with Customer data, including Customer Personal Data, and the Services: (i) it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection; and (ii) it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to the Company for processing in accordance with the terms of the Agreement as supplemented by this Addendum. Customer agrees to indemnify, defend, and hold harmless the Company from and against any loss, cost, or damage of any kind, including attorney's fees and the cost of enforcement of indemnification, to the extent arising out of Customer's breach of this Section 2.3.

3. Processor Personnel

The Company shall ensure that its relevant employees, agents, and subcontractors ("**Company Personnel**") receive appropriate training regarding their responsibilities and obligations with respect to the processing, protection and confidentiality of Personal Data. Any access to Personal Data is strictly limited to those Company Personnel that have a need to know such information for purposes of providing the Services on behalf of Customer pursuant to the Agreement and the Company shall ensure that any applicable Company Personnel are subject to a duty of confidentiality (whether a contractual or a statutory duty) that shall survive the termination of their employment and/or contractual relationship.

4. Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Company shall in relation to the Customer's Personal Data



implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5. Sub-processing

Customer agrees that the Company may engage Company Affiliates and third party sub-processors as Sub-processors to process Customer Personal Data on the Company's behalf. As required under applicable EU Data Protection Laws, the Company agrees to inform the Customer of any material changes concerning the addition or replacement of such Sub-processors, thereby giving Customer the opportunity to object to such changes. Where the Company engages a new Sub-processor, the Company shall inform Customer of the engagement by sending an email notification along with any reasonably requested additional information about the new Sub-processor to Customer's email address on file with the Company. Customer must promptly notify the Company if it objects to any nominated Sub-processor, and the Company will take such steps as are reasonably necessary to address any reasonable Customer concerns. The Company shall impose on such Sub-processors data protection terms that protect the Customer Personal Data to the same standard provided for by this Addendum and shall remain liable for any breach of this Addendum caused by a Sub-processor. For the avoidance of any doubt, ancillary services that are provided to and on behalf of the Company by third party service providers and that are determined to be support services to the Company to execute the Services, shall not be regarded as "Sub-processors" within the meaning of this Addendum.

6. Data Subject Rights

Considering the nature of the Processing, the Company shall provide commercially reasonable assistance, including by appropriate technical and organizational measures as reasonably practicable, to enable Customer to respond to any inquiry, communication or request from a Data Subject seeking to exercise his or her rights under Data Protection Laws, including rights of access, correction, restriction, objection, erasure, or data portability, as applicable. In the event such inquiry, communication or request is made directly to the Company, the Company shall as soon as reasonably practicable inform Customer by providing the full details of the request. For the avoidance of doubt, Customer is responsible for responding to Data Subject requests for access, correction, restriction, objection, erasure or data portability of that Data Subject's Personal Data.

7. Personal Data Breach

7.1 Data Breach. The Company shall notify the Customer without undue delay and pursuant to the terms of the Agreement, but within no more than seventy two (72) hours, upon the Company becoming aware of a Personal Data Breach affecting Customer's Personal Data and shall provide timely information as Customer may reasonably require



to enable the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Cooperation. The Company shall co-operate with the Customer and take commercially reasonable steps as are directed by the customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

The Company shall, to the extent required by EU Data Protection Laws, provide Customer with reasonable assistance, at Customer's expense, with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out under EU Data Protection Laws.

9. Deletion or Return of Company Personal Data

Upon expiration or termination of the Agreement, the Company agrees to delete or return the Customer's Personal Data from the Company's Services, in accordance with the terms and conditions of the Agreement, but in any event within 10 business days.

10. Audit Rights

10.1 Information. Solely to the extent required by applicable Data Protection Laws, the Company shall make available to Customer all information reasonably necessary to demonstrate compliance with its obligations under this Addendum and allow for (and contribute to) audits, including inspections conducted by Customer or another auditor under the instruction of the Customer for the same purposes of demonstrating compliance with obligations set out in this Addendum.

10.2 Audit Conditions. Customer's right under Section 10.1 is subject to the following:

10.2.1 If the Company can demonstrate compliance with its obligations set out in this Addendum by adhering to an approved code of conduct, by obtaining an approved certification or by providing Customer with an audit report issued by an independent third party auditor (provided that Customer will comply with appropriate confidentiality obligations as set forth in an agreement covering the same, and shall not use such audit report for any other purpose), Customer agrees that it will not conduct an audit or inspection under this section 10; and

10.2.2 In acknowledgement of the time, expense and disruption to business associated with performing audits and inspections involving interviews and onsite visits, Customer agrees to only conduct such audits and inspections on condition



that Customer can demonstrate such audit or inspection is necessary beyond the information made available by the Company under this Section 10. Such audits and inspections shall be at reasonable intervals (but not more than once per year) upon not less than 60 days' notice and at a date mutually agreed by the parties, provided that the audit will (i) not disrupt the Company's business; (ii) be conducted during business hours and at the Customer's expense; (iii) not interfere with the interests of the Company's other customers; and (iv) not exceed a period of two successive business days.

11. International Data Transfer

11.1 International Data Transfer. To the extent the Company Processes Personal Data subject to the EU Data Protection Laws on behalf of Customer in the course of the performance under the Agreement, the terms of this Addendum and the Standard Contractual Clauses, which Standard Contractual Clauses are hereby incorporated by reference, shall both apply. Unless agreed to otherwise, the parties shall rely on Module 2: *Transfer from Controller to Processor Abroad* of the EU SCCs for the transfer of Personal Data outside the EEA to the Company and any of its Affiliates. It is agreed that in the event there is conflict between the terms and conditions of this Addendum and the Standard Contractual Clauses, that the Standard Contractual Clauses shall prevail as it pertains to such terms in conflict.

11.2 Restriction on Transfer. The Company shall not transfer or authorize the transfer of Customer Personal Data to countries outside the EEA without the prior written consent of the Customer. Customer agrees and acknowledges that the Company may store certain Customer Personal Data (including relating to individuals located in the EEA) in the United States and execution of this Addendum is deemed consent to the transfer and storage thereof.

11.3 Module Two Terms. The parties are deemed to have accepted and signed the Standard Contractual Clauses where necessary in their entirety, including the annexures thereto, and such Module 2 of the EU SCCs are hereby incorporated by reference, and:

11.3.1 Customer, on behalf of its applicable Data Subjects, shall be deemed to be the "data exporter" and the Company and its Affiliates shall be the "data importer";

11.3.2 Clause 7 "Docking clause" shall apply;

11.3.3 Clause 9 "Use of subprocessors" Option 2 shall apply and the "time period" shall be 10 business days;

11.3.4 Clause 11(a) "Redress", the optional language shall not apply;



11.3.5 Clause 13(a) “Supervision”:

- I. Where the Data Exporter is established in an EU Member State the following shall apply: “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.”
- II. 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 the GDPR the following shall apply: “*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.*”
- III. Where the Data Exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR, the following shall apply: “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.”
- IV. The Information in Exhibit A of this Addendum is incorporated into Annexes 1, 2, and 3 of the Standard Contractual Clauses.

11.4. UK SCCs. Unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Personal Data in compliance with the UK Data Protection Laws in which case the UK SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the UK SCCs shall be populated using the information contained in Exhibit A of this DPA (as applicable).

11.5. Swiss DPA. In relation to transfers of Personal Data protected by the Swiss DPA, the EU SCCs will also apply in accordance with Section 11.1 and 11.3, with the following modifications: (i) any references in the EU SCCs to “Directive 95/46/EC” or “Regulation (EU) 2016/679” shall be interpreted as references to the Swiss DPA; (ii) references to “EU”, “Union”, “Member State” and “Member State law” shall be interpreted as references to Switzerland and Swiss law, as the case may be; and (iii) references to the “competent supervisory authority” and “competent courts” shall be interpreted as references to the



Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland. Unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Personal Data in compliance with the Swiss DPA in which case the Swiss SCC's shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the Swiss SCCs shall be populated using the information contained in Exhibit A to this DPA (as applicable).

11.6. Alternate Mechanism. To the extent that a party relies on a basis for international Data Transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the parties agree to cooperate in good faith to terminate promptly the transfer and to pursue an alternate mechanism that can lawfully support the transfer.

12. General Terms

12.1 Confidentiality. Each party must keep information it receives about the other party and its business and operations in connection with the Agreement, as modified by this Addendum (“**Confidential Information**”) confidential. All Confidential Information provided by a party hereto shall be used by any other party hereto solely for the purpose of rendering or obtaining services pursuant to the Agreement and Addendum and, except as may be required in carrying out the Agreement and/or Addendum, shall not be disclosed to any third party without the prior consent of such providing party. The foregoing shall not be applicable to any information that is publicly available when provided or thereafter becomes publicly available other than through a breach of this Addendum and/or the Agreement, or that is required to be disclosed by or to any governmental authority, or by judicial or administrative process or otherwise by applicable law.

12.2 Notices. All notices and communications given under this Addendum must be in writing and will be delivered personally, sent by post or sent by email, to the address set out in the heading of this Addendum as it pertains to Company, or as it pertains to Customer, the address or email on file with the Company, or at such other address or email as notified from time to time by the parties changing address.

12.3 Main Agreement. Except as amended by this Addendum, the Agreement will remain in full force and effect. To the extent there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.

12.4 Limitation of Liability. The Company's and its Affiliates' liability taken together in the aggregate arising out of or related to this Addendum (including the Standard Contractual Clauses) shall be subject to the exclusions and limitations of liability set forth in the Agreement. Any claims made against the Company or its Affiliates under or in connection with this Addendum (including, where applicable, the Standard Contractual



Clauses) shall be brought solely by the Customer entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this Addendum or otherwise.

13. Governing Law and Jurisdiction

13.1 Governing Law. The governing law for the purposes of this Addendum shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of the Republic of Ireland; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of England and Wales.

Any legal suit, action, or proceeding arising out of or related to this Addendum or the matters contemplated hereunder shall be instituted exclusively in the courts of the Republic of Ireland and each party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action, or proceeding and waives any objection based on improper venue or forum non conveniens. Service of process, summons, notice, or other document by mail to such party's address set out herein shall be effective service of process for any suit, action, or other proceeding brought in any such court.

13.2 Standard Contractual Clauses. To the extent the Standard Contractual Clauses are utilized as detailed in Section 11, such clauses shall be governed by the law of the EU Member State in which the Data Exporter is established, or as otherwise required under the Swiss SCCs or UK SCC's, as applicable. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The parties agree that this shall be the law of, and courts located in, the Republic of Ireland in accordance with Clause 17 and Clause 18 of the EU SCC's.

[SIGNATURE PAGE FOLLOWS]



IN WITNESS WHEREOF, this Addendum is entered into with effect as of the date of the last signature below.

CUSTOMER:

Signature: _____

Customer Legal Entity Name: _____

Signatory Print Name: _____

Title: _____

Date: _____

COMPANY:

CodeLathe Technologies Inc. dba FileCloud

FileCloud Technologies Limited

Signature:  _____
037F0FCFD1E3488...

Signature:  _____
E94F829AB9644B2...

Print Name: George Lo

Print Name: Brian Cahill

Title: CFO & Corporate Secretary

Title: Director

Date: 10/10/2023

Date: 10/10/2023



EXHIBIT A INFORMATION TO BE INCORPORATED INTO THE STANDARD CONTRACTUAL CLAUSES	
ANNEX I A. List of Parties	
Data EXPORTER identity and contact details	
<i>Name</i>	The Customer as defined in the Addendum
<i>Address</i>	To be provided on request
<i>Contact person's name, position and contact details:</i>	To be provided on request
<i>Activities relevant to the data transferred under these Clauses:</i>	The scope and purposes of processing the Data Exporter's personal data is described in the Addendum to which these Clauses are annexed as well as the Agreement between Data Exporter and Data Importer.
<i>Role (controller/processor):</i>	Controller
Data IMPORTER identity and contact details	
<i>Name</i>	CodeLathe Technologies Inc. dba FileCloud
<i>Address</i>	13785 Research Blvd Suite 125 Austin TX, 78750, USA
<i>Contact person's name, position and contact details:</i>	support@filecloud.com
<i>Activities relevant to the data transferred under these Clauses:</i>	The scope and purposes of processing the Data Exporter's personal data is described in the Addendum to which these Clauses are annexed as well as the Agreement between Data Exporter and Data Importer.
<i>Role (controller/processor):</i>	Module 2: Processor



ANNEX I B. Description of Transfer	
<i>Categories of data subjects whose personal data is transferred</i>	The personal data transferred concern the Data Exporter's and Data Exporter's affiliates' end users including employees, consultants and contractors of the Data Exporter, as well as any individuals collaborating or sharing with these end users using the services provided by Data Importer.
<i>Categories of personal data transferred</i>	The personal data transferred concern end users identifying information and organization data (both on-line and offline) as well as documents, images and other content or data in electronic form stored or transmitted by end users via Data Importer's Services.
<i>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.</i>	Not Applicable
<i>The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).</i>	Continuous
<i>Nature and Purpose of the processing and data transfer</i>	The scope and purposes of processing the Data Exporter's personal data is described in the Addendum to which these Clauses are annexed as well as the Agreement between Data Exporter and Data Importer.
<i>Access to Data</i>	Data Exporter may designate an administrator who will have the ability to access Data Exporter's personal data in accordance with the Agreement. In addition, an individual end user of Data Exporter will have the ability to access any of such end user's personal data associated with the specific account through which such end user accesses and uses the



	service in accordance with the functionality of the service, the Agreement and the agreement between the Company and the individual Data Exporter end user.
<i>The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period</i>	Personal data will be retained in accordance with the Company's retention policies, generally for up to 30 days from the effective date of termination or expiration of relevant FileCloud services and no longer than what is required to meet the Company's legal, regulatory and operational requirements and as necessary to perform services.
<i>For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing</i>	Data Importer may engage other companies to provide parts of the service on Data Importer's behalf. Data Importer will ensure that any such Sub-Processors will only access and use any personal data of Data Exporter to provide the service in accordance with the Agreement.
Annex I C. Competent Supervisory Authority	
<i>Competent supervisory authority/ies</i>	To be provided by the data exporter on request.
ANNEX II Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data	
<i>Description of the technical and organizational 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.</i>	<u>Architecture</u> . Data Importer's Services are designed with multiple layers of protection, covering data transfer, encryption, network configuration and application-level controls that are distributed across a scalable, secure infrastructure. End users of Data Importer's service can access files and folders at any time from the desktop, web and mobile clients. All of these clients connect to secure services to provide access to files, allow file sharing with others, and update linked devices when files are added, changed or deleted. The service can be utilized and accessed through a number of interfaces. Each has security settings and features that process and protect Customer Data while ensuring ease of access.



	<p><u>Redundancy.</u> Data Importer's Services are developed with multiple layers of redundancy to guard against data loss and ensure availability.</p> <p><u>Encryption.</u> To protect Customer Data in transit between the Customer and Data Importer, Data Importer uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. Stored Data at rest is encrypted using 256-bit AES encryption. Data Importer's encryption key management infrastructure is designed with operational, technical and procedural security controls with very limited direct access to keys. Encryption key generation, exchange and storage are distributed for decentralized processing.</p> <p><u>Features.</u> End users of Data Importer's Service have the ability to restore lost files and recover previous versions of files, ensuring changes to those files can be tracked and retrieved. Data Importer's service allows for the use of a two-step authentication procedure which adds an extra layer of protection.</p> <p><u>Policies.</u> Data Importer has established a thorough set of security policies covering areas of information security, physical security, incident response, logical access, physical production access, change management and support.</p> <p><u>Security.</u> Data Importer maintains network security and monitoring techniques that are designed to provide multiple layers of protection and defense. Data Importer employs industry-standard protection techniques, including firewalls, network security monitoring, and intrusion detection systems to ensure only eligible traffic is able to reach Data Importer's infrastructure.</p>
<p><i>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</i></p>	



assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III LIST OF SUB-PROCESSORS

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

AWS datacenters in the respective regions. The data back-ups are encrypted and performed daily within the Availability Zones in the same region of AWS datacenters. For how AWS ensures processing your data in compliance with GDPR: : <https://aws.amazon.com/compliance/gdpr-center/>