

COPY NOT FOR EXECUTION
FOR SIGNED DOCUMENT PLEASE
CONTACT:
ACCOUNTS@JUMPCLOUD.COM

DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) is effective as of _____ and is incorporated by reference into and made a part of the Directory-as-a-Service Agreement entered into between JumpCloud, Inc. (“**Service Provider**”) and _____ (“**Customer**”) dated _____ (“**Agreement**”). This DPA sets forth certain duties and obligations of the parties with respect to the protection, security, processing, and privacy of personal data provided or made available to Service Provider by Customer as part of the Service provided by Service Provider for Customer under the Agreement. This DPA shall supplement (and not supersede) the Agreement, and shall take precedence solely to the extent of any conflict between this DPA and the Agreement. All capitalized terms used and not expressly defined in this Addendum shall have the meanings given to them in the Agreement. This Agreement shall only be considered effective during the term that Customer is actively paying for Services.

In the course of providing the Service to Customer pursuant to the Agreement, Service Provider may Process certain Personal Data provided or made available to Service Provider by Customer on behalf of Customer and the parties agree to comply with the following provisions with respect to any such Personal Data, each acting reasonably and in good faith.

1. DEFINITIONS

- 1.1** “**Controller**” and “**Processor**” each have the meaning given to it in the GDPR.
- 1.2** “**Customer Data**” is defined in the Agreement as “Customer Content.”
- 1.3** “**Data Protection Laws and Regulations**” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.
- 1.4** “**Data Subject**” means the identified or identifiable person to whom Personal Data relates.
- 1.5** “**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).
- 1.6** “**Personal Data**” means personal data (as defined in the GDPR) that is uploaded or submitted to the Service by Customer.
- 1.7** “**Processing**” has the meaning given in the GDPR.
- 1.8** “**Security Documentation**” means Service Provider’s security processes and procedures applicable to the Service that are described at www.jumpcloud.com/security, as updated from time to time, or as otherwise made reasonably available by Service Provider.
- 1.9** “**Standard Contractual Clauses**” means the agreement executed by and between Customer and Service Provider, and attached hereto as Schedule 2 pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010 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.
- 1.10** “**Sub-processor**” means any Processor engaged by Service Provider.

1.11 “Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 Roles. Customer is the Controller and Service Provider is the Processor with regard to the Processing of Personal Data under the Agreement.

2.2 Customer’s Processing of Personal Data. Customer shall (a) collect and Process Personal Data, (b) use the Service, and (c) give Service Provider instructions regarding the Processing of Personal Data for Customer, in all cases, in accordance with all applicable laws, rules, and regulations, including the Data Protection Laws and Regulations. Customer is solely liable and responsible for the accuracy, quality, and legality of Personal Data. Customer is responsible for configuring the Service to meet its security and backup needs and requirements, including by choosing strong passwords and using multi-factor authorization when available.

2.3 Service Provider’s Processing of Personal Data. Effective as of 25 May 2018, Service Provider shall process Personal Data in accordance with the GDPR requirements directly applicable to Service Provider’s provision of its Service. Personal Data shall be considered Customer’s Confidential Information under the Agreement. Service Provider shall only Process Personal Data on behalf of and in accordance with Customer’s instructions set forth in this DPA and the Agreement for the following purposes: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by Users in their use of the Service; and (c) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. The subject-matter, nature, and purpose of Processing of Personal Data by Service Provider is solely so Service Provider can provide the Service to Customer pursuant to the Agreement. The duration of the Processing shall be for the duration of the Agreement. Schedule 1 to his DPA identifies the nature of the Processing, the types of Personal Data Processed, and categories of Data Subjects for which data is Processed under this DPA.

2.4 Personnel. Service Provider shall 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 on their responsibilities and have executed written, industry standard confidentiality agreements. Service Provider shall ensure that Service Provider’s access to Personal Data is limited to those personnel performing Service in accordance with the Agreement.

3. RIGHTS OF DATA SUBJECTS. Service Provider shall, to the extent legally permitted, promptly notify Customer if Service Provider receives a request from a Data Subject to exercise the Data Subject’s rights under the GDPR (“Data Subject Request”). Taking into account the nature of the Processing, Service Provider shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Service, does not have the ability to address a Data Subject Request, Service Provider shall upon Customer’s request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Service Provider is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Service Provider’s provision of such assistance.

4. SUB-PROCESSORS

4.1 Appointment of Sub-processors. Customer acknowledges and agrees that Service Provider may engage third-party Sub-processors in connection with the provision of the Service. Service Provider has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Service provided by such Sub-processor.

4.2 List of Current Sub-processors and Notification of New Sub-processors. Service Provider’s current list of Sub-processors for the Service is located at www.jumpcloud.com/gdpr . Such Sub-processor lists shall include the identities of those Sub-processors and their country of location (“Sub- processor Lists”). Service Provider shall

provide Customer notification of potential new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data.

4.3 Objection Right for New Sub-processors. Customer may object to Service Provider's use of a new Sub-processor by notifying Service Provider promptly in writing within ten (10) business days after receipt of Service Provider's notice. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Service Provider will use reasonable efforts to make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration or use of the Service to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Service Provider is unable to make available such change within a reasonable period of time, which shall not exceed fifteen (15) days, Customer may terminate the applicable Order Form(s) with respect only to those Service which cannot be provided by Service Provider without the use of the objected-to new Sub-processor by providing written notice to Service Provider. Service Provider will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Service, without imposing a penalty for such termination on Customer.

4.4 Liability. Service Provider shall be liable for the acts and omissions of its Sub-processors to the same extent Service Provider would be liable if performing the Service of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5. SECURITY

5.1 Controls for the Protection of Customer Data. Service Provider shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed by the Processing. Service Provider's measures will include those set forth in the Security Documentation. Service Provider regularly monitors compliance with these measures. Service Provider will not materially decrease the overall security of the Service during a subscription term.

5.2 Third-Party Certifications and Audits. Service Provider has obtained the third-party certifications and audits set forth in the Security Documentation. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Service Provider shall make available to Customer that is not a competitor of Service Provider (or Customer's independent, third-party auditor that is not a competitor of Service Provider) a copy of Service Provider's then most recent third-party audits or certifications, as applicable.

6. CUSTOMER DATA INCIDENT NOTIFICATION. Service Provider shall, notify Customer without undue delay, but in no event in less than 72 hours, after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Service Provider or its Sub-processors of which Service Provider (a "**Customer Data Incident**"). Service Provider shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Service Provider deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Service Provider's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

7. RETURN AND DELETION OF CUSTOMER DATA. Service Provider shall return Customer Data to Customer or, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Security Documentation, or as requested by Customer.

8. GDPR AND ONWARD TRANSFER

8.1 Assistance. As required by the GDPR, Service Provider shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under the GDPR.

8.2 Standard Contractual Clauses. The Standard Contractual Clauses set forth in Schedule 2 to this DPA apply to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to Service Provider's facilities in countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations, to the extent such transfers are subject to such Data Protection Laws and Regulations.

(a) Instructions. For the purposes of Section 2 of the DPA and Clause 5(a) of the Standard Contractual Clauses, the following acts are deemed an instruction by the Customer to process Personal Data: (a) Customer's entering into the Agreement and applicable Order Form(s) are deemed instructions to Process Personal Data as is necessary to perform Service under the Agreement; (b) Users actions that initiate Processing while using the Service; and (c) Customer's other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

(b) Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Service Provider may engage new Sub-processors as described in the DPA.

(c) Copies of Sub-processor Agreements. The parties agree that Service Provider may redact the copies of the Sub-processor agreements that must be provided by Service Provider to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses to remove commercial information, confidential information, and clauses unrelated to the Standard Contractual Clauses or their equivalent. Service provider will provide copies of the Sub-processor agreements, only upon written request by Customer.

(d) Audits and Certifications. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications. Customer requests an on-site audit of the procedures relevant to the protection of Personal Data, and Customer and Service Provider shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. Customer shall promptly notify Service Provider with information regarding any non-compliance discovered during the course of an audit.

8.3 Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Service Provider to Customer only upon Customer's written request.

8.4 Conflict. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

List of Schedules

Schedule 1: Details of the Processing

Schedule 2: Standard Contractual Clauses

The parties' authorized signatories have duly executed this Agreement:

SCHEDULE 1 - DETAILS OF THE PROCESSING

Categories of Data Subjects

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

- Customer's Users authorized by Customer to use the Service

Type of Personal Data

Customer may submit Personal Data to the Service, 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:

- First and last name
- Title
- Contact information (company, email, phone, physical business address)
- IP Address

SCHEDULE 2 - STANDARD CONTRACTUAL CLAUSES

**Commission Decision C(2010)593
Standard Contractual Clauses (processors)**

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

Name of the data exporting organisation:

Address:

Tel.: _____ ; fax: _____ ; e-mail: _____

Other information needed to identify the organisation:

.....
(the data **exporter**)

And

Name of the data importing organisation: JumpCloud, Inc.

Address: 2040 14th St STE 200 Boulder, CO 80302

Tel.: ___720.240.5001; fax: ___720.240.5005; e-mail: finance@jumpcloud.com

Other information needed to identify the organisation:

.....n/a.....
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *'personal data'*, *'special categories of data'*, *'process/processing'*, *'controller'*, *'processor'*, *'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure

a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by

a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

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

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

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

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely [insert country]

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or

destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

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

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Larry Middle

Position: CFO

Address: 2040 14th St STE 200 Boulder, CO 80302

Other information necessary in order for the contract to be binding (if any): none

(stamp of organisation)

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer): The data exporter is the entity that executed these Standard Contractual Clauses.

Data importer

The data importer is (please specify briefly activities relevant to the transfer): Jumpcloud, Inc., which offers a hosted directory as a service and processes personal data in accordance with the terms of the Agreement.

Data subjects

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

Data exporter may submit Personal Data to the Service. The Data exporter determines what Personal Data and how much Personal Data is submitted in its sole discretion. The Personal Data provided may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Data exporter's Users authorized by data exporter to use the Service

Categories of data

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

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

- First and last name
- Title
- Contact information (company, email, phone, physical business address)
- IP Address

Special categories of data (if appropriate)

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

not applicable

Processing operations

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

The objective of Processing of Personal Data by data importer is the performance of the Service pursuant to the Agreement.

DATA EXPORTER

Name:

DATA IMPORTER

Name: Larry Middle

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Service, that are described at www.jumpcloud.com/security, or otherwise made reasonably available by data importer. Data Importer will not materially decrease the overall security of the Service during a subscription term.

DATA EXPORTER

DATA IMPORTER