JUMPCLOUD INC.

Data Processing Addendum for JumpCloud Customers

This Data Processing Addendum (this "**DPA**") is between JumpCloud Inc. ("**JumpCloud**") and the customer identified on the Order Form to which this DPA is incorporated ("**Customer**"), and is incorporated into the Terms of Use located at: https://jumpcloud.com/legal (the "**Agreement**") between JumpCloud and Customer. Any undefined capitalized term shall have the meaning given to it in the Agreement. The parties agree as follows:

1. DEFINITIONS

1.1 "**Applicable Data Protection Laws**" means the data protection laws and regulations that are applicable to JumpCloud and include the General Data Protection Regulation (the "**GDPR**") (Regulation (EU) 2016/679), and any implementing and supplementing law; (ii) the GDPR as transposed into the law of England and Wales, Scotland and Northern Ireland and the UK Data Protection Act 2018 United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, together with the Data Protection Act 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019; (iii) the Swiss Federal Act on Data Protection; (iv) the California Consumer Privacy Act of 2018 and its implementing regulations (the "**CCPA**") (Cal. Civ. Code §§ 1798.100-1798.199), any other applicable law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule, or other binding instrument implementing any of the foregoing (in each case as amended, consolidated, re-enacted, or replaced from time to time).

1.2 "**Customer Personal Data**" means Personal Data included in Customer Data.

1.3 "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates, including, a person located in the European Economic Area, United Kingdom, and/or California, including a "Consumer" as the term is defined in the CCPA.

1.4 "**EEA" or "European Economic Area**" means the European Union (as defined herein), as well as Iceland, Liechtenstein, and Norway.

1.5 "**EU**" or "**European Union**" means the European Union, inclusive of Switzerland and the United Kingdom, even after the United Kingdom has officially withdrawn from the European Union.

1.6 "**Personal Data**" means information related to and linked or reasonably linkable to a Data Subject, as interpreted under Applicable Data Protection Laws and includes the terms "personal data" or "personal information" under such laws.

1.7 "**Process**", "**Processes**", "**Processing**", "**Processed**" means any operation or set of operations which is performed upon Personal Data whether or not by automatic means, including collecting, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing, and destroying Personal Data, and as otherwise defined under Applicable Data Protection Laws.

1.8 "**Security Incident**" means an event about which JumpCloud knows, discovers, or is notified of, and of which JumpCloud confirms Customer Personal Data has been, to the actual knowledge of JumpCloud, unlawfully destroyed, lost, altered, accessed, disclosed, acquired, or used by any unauthorized person, in violation of Applicable Data Protection Laws, including any "personal data breach" or "data breach" as defined by Applicable Data Protection Laws. A Security Incident shall not include an unsuccessful attempt or activity that does not compromise the security of Customer Personal Data, including without limitation pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

1.9 "**Services**" means the services provided by JumpCloud to Customer pursuant to the Agreement.

1.10 "**Sub-Processor**" means JumpCloud's contractors, agents, vendors, and third-party service providers that Process Personal Data.

2. DATA HANDLING AND ACCESS

2.1 **General Compliance**. Customer hereby authorizes and instructs JumpCloud to, and JumpCloud will, and will require Sub-Processors to, Process Customer Personal Data in compliance with the Agreement, this DPA, and Applicable Data Protection Laws. Customer represents and warrants that (i) it has all authority, grounds, bases, rights, or consents necessary (including without limitation with respect to Article 6 of GDPR) to authorize JumpCloud's Processing of the Customer Personal Data in accordance with the Agreement, and (ii) Customer's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws.

2.2 **JumpCloud and Sub-Processor Compliance.** Where JumpCloud uses a Sub-Processor to Process Customer Personal Data, JumpCloud agrees to (i) enter into a written agreement with such Sub-Processor regarding such Sub-Processor's Processing of Customer Personal Data that imposes on such Sub-Processor data protection and security requirements that are compliant with Applicable Data Protection Laws, and that, at a minimum, impose data protection and security terms substantially similar to the data protection and security terms under this DPA; (ii) reasonably enforce compliance with such written agreement, including updating the written agreement when necessary under Applicable Data Protection Laws; and (iii) remain responsible to Customer for any noncompliance by Sub-Processors (and their sub-processors, if applicable) with respect to the Processing of Customer Personal Data.

2.3 **Authorization to Use Sub-Processors**. Customer hereby authorizes (i) JumpCloud to engage Sub-Processors, and (ii) Sub-Processors to engage sub-processors. JumpCloud will provide Customer, upon Customer's request, the name, location, and role of each Sub-Processor used to Process Customer Personal Data and copies of any other records of Processing of Customer Personal Data that Sub-Processors are required to maintain and/or provide under Applicable Data Protection Laws. Customer hereby approves of the Sub-Processors listed on JumpCloud's website at: https://jumpcloud.com/gdpr/.

2.4 **Objection Right for New Sub-Processors**. JumpCloud will inform Customer of any new Sub-Processor in connection with the provision of the applicable Services and may provide such notifications through updates to the list of Sub-Processors on JumpCloud's website at: https://jumpcloud.com/gdpr/. Customer may object to JumpCloud's use of a new Sub-Processor on reasonable data protection grounds by notifying JumpCloud of such grounds in writing within ten (10) business days after such information has been sent. In the event Customer objects to a new Sub-Processor as permitted in the preceding sentence, JumpCloud may address the concerns with respect to the Sub-Processor or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to Sub-Processor without unreasonably burdening Customer. If JumpCloud is unable to make such change available within a reasonable period of time, which shall not exceed thirty (30) days, Customer's sole and exclusive remedy is, within thirty (30) days, to provide written notice of termination to JumpCloud of the applicable Order Form(s), but only with respect to any such Services which cannot be provided by JumpCloud without the use of the objected-to new Sub-Processor.

2.5 **Following Instructions**. JumpCloud will Process Customer Personal Data only in accordance with the written instructions of Customer and may Process Customer Personal Data: (i) in accordance with the Agreement and applicable Order Form(s); (ii) as initiated by Users in their use of the Services; (iii) to further develop and provide services to JumpCloud's customers; (iv) to facilitate the anonymization of Personal Data; and/or (v) to comply with other documented reasonable instructions provided by Customer (e.g., via email). JumpCloud will notify Customer without undue delay in writing if, in JumpCloud's reasonable opinion, Customer's instructions infringe Applicable Data Protection Laws, provided that Customer acknowledges that the Services may Process Personal Data on an automated basis in accordance with Customer's configurations, which JumpCloud does not monitor.

2.6 **Details of the Processing**. The subject matter of Processing of Personal Data by JumpCloud is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data, and the categories of Data Subjects' Personal Data Processed under this DPA are further specified in Annex I.

3. RIGHTS OF DATA SUBJECTS

JumpCloud will, to the extent legally permitted, notify Customer without undue delay if JumpCloud receives a request from a Data Subject to exercise the Data Subject's rights afforded under the Applicable Data Protection Laws regarding Customer Personal Data ("**Data Subject Request**"). To the extent Customer does not have access to the applicable Customer Personal Data in JumpCloud's custody or control, JumpCloud will

(a) assist Customer by appropriate technical and organizational measures for the fulfilment of Customer's obligation to respond to a Data Subject Request under Applicable Data Protection Laws, and (b) upon Customer's request and at Customer's expense, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent JumpCloud is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Laws.

4. COMPLIANCE

4.1 **JumpCloud Data Transfer Mechanism**. For all transfers from the EEA of Customer Personal Data pursuant to the Agreement, the parties hereby incorporate Modules 2 and 3 of the Standard Contractual Clauses (as applicable) approved by the European Commission (the "**SCCs**") as described in Exhibit A. To the extent there is any conflict between the terms of this DPA and the SCCs, the SCCs shall control to the extent of the conflict. The SCCs will apply only with respect to Customer Personal Data transferred from the EEA, if any. Customer shall take all reasonable steps to determine whether the parties are required under the Applicable Data Protection Laws to either: (a) register the SCCs with any supervisory authority in any member state of the EEA, or (b) procure approval from each such supervisory authority for the transfer referred to in the SCCs and shall promptly inform JumpCloud upon becoming aware of such requirements. With respect to data transfers from the United Kingdom to the United States, the parties hereby incorporate the International Data Transfer Addendum to the SCCs attached hereto as Exhibit B.

4.2 **Prior Consultation**. JumpCloud agrees to provide reasonable assistance to Customer (at Customer's expense) where, in Customer's reasonable judgement, the type of Processing performed by JumpCloud is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale, systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant supervisory authorities.

4.3 **Demonstrable Compliance**. JumpCloud agrees to keep records of its Processing in compliance with Applicable Data Protection Laws. If the parties have expressly agreed in writing that JumpCloud will collect Customer Personal Data on Customer's behalf and that JumpCloud must obtain verifiable consent therefor, such records will include but not be limited to records of the verifiable consent under Applicable Data Protection Laws.

4.4 **Sale of Personal Data**. JumpCloud shall not sell Customer Personal Data as the term "sell" is defined by the CCPA, except as required to provide services to Customer or as instructed by Customer. The foregoing restriction will not apply to "aggregate consumer information" or "deidentified personal information" as each term is defined by the CCPA.

4.5 **Service Provider**. JumpCloud shall not retain, use, or disclose Customer Personal Data for any purpose other than performing services and as described in the Agreement. The parties acknowledge and agree that the Processing of Customer Personal Data authorized by Customer's instructions described in this DPA is integral to and encompassed by JumpCloud's provision of services and the relationship between the parties.

5. INFORMATION SECURITY

JumpCloud will maintain appropriate technical and organizational measures for protection of the security, confidentiality, and integrity of Personal Data, including those described on JumpCloud's website at: https://jumpcloud.com/security/.

6. ASSESSMENTS, AUDITS AND REMEDIATION

If and to the extent Applicable Data Protection Laws include a right for Customer to audit JumpCloud's Processing of Customer Personal Data, Customer may exercise such audit right, and JumpCloud will fulfill its corresponding obligations, as follows:

6.1 **Assessments**. Relevant records of JumpCloud's Processing of Customer Personal Data to demonstrate compliance with this DPA and Applicable Data Protection Laws will be maintained by JumpCloud and provided to Customer upon Customer's reasonable request. JumpCloud will complete any data protection questionnaire reasonably requested by Customer, no more than once annually, relating to JumpCloud's Processing of Customer Personal Data.

6.2 **Audits**.

6.2.1. If the relevant records and/or questionnaire responses provided by JumpCloud pursuant to Section 6.1 are not sufficient for Customer to verify compliance with Applicable Data Protection Laws, for the purpose of verifying JumpCloud's compliance with Applicable Data Protection Laws and this DPA, JumpCloud shall provide a copy of JumpCloud's most recent relevant third-party audits or certifications, as applicable,or any summaries thereof to Customer.

6.2.2. If the information made available pursuant to Section 6.2.1 is insufficient to confirm JumpCloud's compliance with its obligations under this DPA, JumpCloud may permit Customer, upon reasonable written notice of no less than thirty (30) days, at Customer's cost, and no more than once annually, to conduct on-site audits through a JumpCloud-approved third-party auditor.

6.2.3. JumpCloud agrees to allow audits to be conducted directly by Customer where, under Applicable Data Protection Laws, Customer is required to conduct audits directly. JumpCloud agrees to cooperate in good faith with the audit and without undue delay (i) provide access to books, records (including, but not limited to, security scan records), systems, files, and other information necessary for the audit, and (ii) at Customer's request, enable access to JumpCloud's premises if absolutely necessary to properly conduct the audit or required under Applicable Data Protection Laws. Notwithstanding the foregoing, Customer may not conduct any security scans or other intrusion testing on JumpCloud's systems without the express prior written consent of JumpCloud. Customer agrees to (x) schedule audits to minimize disruption to JumpCloud's business, (y) require any third party it employs to sign a non-disclosure agreement, and (z) make the results of the audit available to JumpCloud. The results of the audit will be JumpCloud's Confidential Information and Customer will only disclose the portion of results of the audit to third partiesto the extent such disclosure is (A) required to demonstrate Customer's own compliance, or (B) otherwiserequired under the Applicable Data Protection Laws. To the extent permitted by law, Customer shall provide written notice to JumpCloud prior to disclosing results of an audit to any third party.

6.3 **Remediation**. JumpCloud agrees to take action without undue delay to correct any documented material security issue affecting Customer Personal Data identified by such audit and to inform Customer of such actions. If such action is not taken without undue delay, Customer's sole remedy will be to terminate any or all Order Forms at Customer's discretion provided that JumpCloud will incur no penalty for any such termination.

7. SECURE DISPOSAL

JumpCloud will securely dispose of Customer Personal Data (i) during the term of the Agreement upon Customer's written request if such Customer Personal Data is no longer reasonably required to perform the Services, or (ii) after the termination of the provision of the Services. If requested by Customer before the provision of the Services has terminated and such Customer Personal Data is not available to Customer within the Service, JumpCloud will make available a copy of such Customer Personal Data prior to disposal. JumpCloud may retain Customer Personal Data to the extent that it is required to do so under Applicable Data Protection Laws.

8. CHANGES TO REQUIREMENTS

The parties will work together in good faith to amend or supplement this DPA from time to time to reflect new requirements under Applicable Data Protection Laws.

9. SECURITY INCIDENT

9.1 **Policy**. JumpCloud maintains reasonable Security Incident management policies and procedures and will, to the extent required under Applicable Data Protection Laws, notify Customer without undue delay, and in any event, no more than 72 hours after becoming aware of any Security Incident. JumpCloud will make reasonable efforts to identify the cause of such Security Incident and take those steps as JumpCloud deems necessary and reasonable in order to remediate the cause of such Security Incident to the extent the remediation is within JumpCloud's reasonable control. The obligations in this Section shall not apply to any Security Incident that is caused by Customer and/or Users.

9.2 **Reports**. Upon request by Customer, JumpCloud will enable Customer to review the non-privileged results of, and reports relating to, the investigation and response to a Security Incident, which Customer will treat as Confidential Information of JumpCloud.

10. TERMINATION

This DPA shall automatically terminate in the event the Agreement is terminated or expires. Notwithstanding anything to the contrary in the Agreement or this DPA, Customer may terminate any Order Form, or any portion thereof, immediately upon written notice to JumpCloud, and without judicial notice or resolution or prejudice to any other remedies, in the event a data protection or other regulatory authority or other tribunal or court in any country finds there has been a breach of Applicable Data Protection Laws by virtue of Customer's or JumpCloud's Processing of Customer Personal Data in connection with the Agreement, and such breach has not been cured within sixty (60) days of JumpCloud's receiving notice thereof.

11. LIMITATION OF LIABILITY

Without prejudice to any limitations afforded to data processors under any Applicable Data Protection Laws, each party's liability arising out of or related to this DPA (whether in contract, tort, or under any other theory of liability) is subject to the limitations of liability set forth in the Agreement; provided, in no event will such limitation apply to any Data Subject's rights to the extent such limitation is prohibited under the SCCs or any Applicable Data Protection Laws.

12. CONTACT INFORMATION

JumpCloud will designate a point of contact as its "Privacy and Security Coordinator". This Privacy and Security Coordinator will: (i) maintain responsibility for applying adequate protections to Customer Personal Data, including the development, implementation, and maintenance of its information security.

Exhibit A

OPERATIVE PROVISIONS AND TERMS OF THE STANDARD CONTRACTUAL CLAUSES

Modules Two and Three of SCCs are incorporated by reference and form part of the DPA, as applicable. The information required for the purposes of the Appendix to the SCCs are set out in Annexes I and II. The operative provisions and status of optional terms of the SCCs are specified below in this Exhibit A.

1. Clause 7 (Docking Clause) is not applicable.
2. Clause 9 Option 2 (General Written Authorisation) is applicable. JumpCloud's list of Sub-Processors is located at www.jumpcloud.com/gdpr. Details in respect of notifications and objection rights relating to new Sub-Processors are described in Section 2.4 of the DPA.
3. The optional language in Clause 11(a) (Redress) is not applicable.
4. Clause 17 (Governing Law) Option 1 is applicable and is completed with "Ireland".
5. Clause 18(b) (Choice of Forum and Jurisdiction) is completed with "Ireland".

Annex I

A. LIST OF PARTIES

Data exporter: Customer, as identified in the Agreement.
Contact person's name, position, and contact details: see Order Form or Cover Section of the Agreement.Activities relevant to the data transferred under these Clauses: receiving the Services.
Role: controller or processor, as applicable
Signature and date: _____

Data importer: JumpCloud Inc.; 361 Centennial Parkway, Suite 300, Louisville, CO 80027
Contact person's name, position, and contact details: Eric Gunning, Chief Legal Officer, eric.gunning@jumpcloud.com
Activities relevant to the data transferred under these Clauses: providing the Services
Role: processor
Signature and date: _____

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred –

- Data exporter's Users

Categories of personal data transferred –

- Name (first, middle, last)
- Employment Information (e.g., title, department, employee ID)
- Location
- Contact Information (company, email, phone number, physical address)
- Online Identity (username, display name, passwords)
- IP Address
- Account Name
- Network Activity Information
- Geolocation (e.g., router location)
- System Information (e.g., memory information, storage availability, apps and programs, disk information, patches)
- Custom Attributes (any data that Customer or a User chooses to store with their account/user record)

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.

- No sensitive data required to be transferred for the Services. Unless expressly agreed in writing in the DPA or the Agreement, the data exporter will not export any sensitive data.

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

- Continuous

Nature & Purpose of the processing

- JumpCloud will Process Customer Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the applicable Order Form, the Agreement, and the DPA.

The period for which the personal data will be retained –

- During the term of the Agreement.

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

- As described in the DPA, with respect to each sub-processor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authorities in accordance with Clause 13

- Ireland

Annex II

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

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.

See https://jumpcloud.com/security.

Exhibit B

UK International Data Transfer Addendum to SCCs

Table 1: Parties

Start date	As identified in the Agreement	
The Parties	**Exporter**	**Importer**
Parties' details	See Annex I	See Annex I
Key Contact	See Annex I	See Annex I

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
2	Customer as Controller	No	No	General	See Section 2.4 of DPA	N/A
3	Customer as Processor	No	No	General	See Section 2.4 of DPA	N/A

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex I
Annex 1B: Description of Transfer: See Annex I
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II
Annex III: List of Sub processors: See jumpcloud.com/gdpr

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: Importer

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section **Error! Reference source not found.** of those Mandatory Clauses.