DATA PROCESSING ADDENDUM

Last Updated: April 2020

This Data Processing Addendum (the ***"Addendum")*** reflects the parties' agreement with respect to the Processing of Personal Data under the Nasuni Subscription Agreement for Cloud-Scale Enterprise File Services or other written or electronic agreement referencing this Addendum under which Nasuni Processes Customer's Personal Data that is subject to Applicable Data Protection Law (the ***"Agreement")***. This Addendum amends the Agreement and is effective upon its incorporation into the Agreement, as specified in the Agreement itself or in any Order. Upon its incorporation into the Agreement, this Addendum will form part of the Agreement. Notwithstanding anything to the contrary in the Agreement, if there is a conflict between this Addendum and the Agreement, this Addendum will control. This Addendum will be incorporated into the Agreement in accordance with the terms of the Agreement.

1. **DEFINITIONS.** For the purposes of this Addendum, the following terms have the following meanings unless the context otherwise requires. Other capitalized terms not defined herein will have the same meaning as set forth in the Agreement.

(a) ***"Affiliate"*** means an entity that owns or controls, is owned or controlled by or is under common ownership or control with you, where "control" means the power to direct the management or affairs of an entity and "ownership" means the beneficial ownership of fifty percent (50%) or more of the voting securities or other equivalent voting interests of an entity.

(b) "***Applicable Data Protection Law"*** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States including its federal, state, and local laws), applicable to the Processing of Personal Data under the Agreement;

(c) "***Business Purpose***" has the meaning given to it in the CCPA;

(d) "***CCPA***" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations;

(e) "***Data Processor***" means Nasuni Corporation, as the entity which Processes Personal Data on behalf of Customer, the Data Controller (and which shall have the same meaning as "service provider" as that term is defined by the CCPA);

(f) ***"Data Subject"*** means the identified or identifiable person to whom Personal Data relate (and which shall have the same meaning as "consumer" as that term is defined by the CCPA);

(g) "***General Data Protection Regulation***" or "***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);

(h) "***Personal Data***" means any information Processed by Data Processor for Data Controller relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under Applicable Data Protection Law) (and, which shall have the same meaning as "personal information" as that term is defined by the CCPA).

(i) "***Processing***" means any operation or set of operations which is performed upon Personal Data,

whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(j) ***"Regulator"*** means the governmental data protection agency which has jurisdiction over a Data Controller's Processing of Personal Data;

(k) "***Sell***" has the meaning given to it in the CCPA;

(l) ***"Standard Contractual Clauses"*** means the standard contractual clauses for the transfer of Personal Data to Processors established in Third Countries as set out in the European Commission Decision 2010/87/EU; and

(m) ***"Third Countries"*** means all countries outside of the European Economic Area ***("EEA")***, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time, which, at the date of this Addendum, include Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

In cases where Applicable Data Protection Law uses different terms to cover concepts similar to those covered under the aforementioned terms (e.g., for the CCPA, 'business' instead of "controller," 'consumer' instead of "data subject," 'personal information' instead of "personal data," and 'service provider' instead of "processor"), then those different terms shall have the meaning assigned to those different terms under such Applicable Data Protection Law (and shall be subject to the territorial and material scope of such applicable privacy laws).

2. **BACKGROUND.** Customer (for the purpose of this Addendum, the ***"Data Controller"***) wishes to appoint Nasuni (for the purpose of this Addendum, the ***"Data Processor"***) as a Data Processor to Process Personal Data (i) in accordance with the Agreement; (ii) at the Data Controller's or its Authorized User's request in using the Software; or (iii) to comply with other reasonable instructions of the Data Controller (*e.g.,* via email or support tickets) that are consistent with the terms of this Addendum (individually and collectively, the ***"Purpose"***). The Personal Data that may be Processed under the Agreement, the extent of which is determined and controlled by the Data Controller in compliance with Applicable Data Protection Law, may include, but is not limited to, data relating to the following categories of Data Subject: Authorized User to Nasuni Data Controller's employees, consultants, contractors, agents, and/or third parties with whom the Data Controller conducts business. Such Personal Data is that Personal Data that is included in the data and information submitted by Authorized Users and that may or may not contain special categories of data (such as, but not necessarily limited to, data concerning health, genetic data, or biometric data) in the Data Controller's discretion. If Customer's Affiliates have placed Orders with Nasuni for the Software under the Agreement, then this Addendum amends those Orders, and each such Affiliate shall be deemed to be the "Data Controller" for Personal Data pertinent to its Order for the purposes of this Addendum. Customer shall be responsible for coordinating all communications with Nasuni and Customer's Affiliates under this Addendum and shall be entitled to make and receive any communication in relation to the Addendum, on behalf of itself and its Affiliates.

3. DATA CONTROLLER

(a) Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or Processed by the Data Processor. The Data Processor will process the Personal Data only as set forth in Data Controller's written instructions.

(b) Data Controller warrants that it has all necessary rights to provide the Personal Data to Data Processor for the Processing to be performed in relation to the Services. To the extent required by Applicable Data Protection Law, Data Controller is responsible for ensuring that any necessary Data Subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by the Data Subject, Data Controller is responsible for

promptly communicating the fact of such revocation to the Data Processor, and Data Processor remains responsible for implementing any Data Controller instruction with respect to the further Processing of such Personal Data.

(c) Data Controller warrants that it will disclose Personal Data to Data Processor only for valid Business Purposes.

4. **DATA PROCESSOR'S OBLIGATIONS.**

To the extent the Data Processor Processes Personal Data on behalf of the Data Controller, it shall:

(a) Process the Personal Data only on documented instructions from the Data Controller in such manner as, and to the extent that, this is appropriate for the provision of the Services, except as required to comply with a legal obligation to which the Data Processor is subject. In such a case, the Data Processor shall, to the extent legally permitted, inform the Data Controller of that legal obligation before Processing. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes the Applicable Data Protection Law, including with regard to transfers of Personal Data to Third Countries;

(b) without prejudice to any existing contractual arrangements between the Parties, treat all Personal Data as strictly confidential and inform all its employees, agents and/or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data; further, the Data Processor shall ensure that such persons or parties authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue the Purpose, subject to the requirements of this Addendum;

(d) at all times have in place an appropriate written security policy with respect to the processing of Personal Data, outlining in any case the measures referenced in Section 5 below;

(e) not Sell Customer Personal Data;

(f) not retain, use, or disclose Personal Data for any purpose other than the Purpose; and

(g) certifies that it understands the restrictions set forth in this Section 4 and shall comply with such restrictions.

5. SECURITY

(a) 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 violations of the rights and freedoms of natural persons, without prejudice to any other security standards agreed upon by the Parties, the Data Controller and Data Processor shall implement appropriate technical and organizational measures for the protection of the security, confidentiality and integrity of the Personal Data appropriate to the risk, taking into account the risks that are presented by the Processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, Processing, access or disclosure of Personal Data. These measures include, as appropriate:

(i) controls to permit access to the Personal Data only by authorized personnel for the Purpose;
(ii) the pseudonymization and encryption of Personal Data;
(iii) controls for the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
(iv) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
(v) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing of Personal Data; and

(vi) measures to identify vulnerabilities with regard to the Processing of Personal Data in systems used to provide Services to the Data Controller.

(b) The Data Processor will regularly monitor the measures as implemented by it in accordance with this Section 5. The Data Processor will not materially decrease or diminish the overall security measures applicable to the Services during the term of the Subscription.

(c) The parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in the Applicable Data Protection Law or by Regulators.

(d) At the Data Controller's request, subject to the confidentiality obligations set forth in the Agreement, the Data Processor shall provide to the Data Controller information regarding the measures it has taken pursuant to this Section 5 in order to ensure its compliance with its obligations under this Addendum. Such information may include the Data Processor's third-party audit reports or third-party certifications. Data Controller may contact the Data Processor in accordance with the "Notices" section of the Agreement to request an on-site audit of the Data Processor's procedures relevant to the protection of Personal Data, but only to the extent required under the Applicable Data Protection Law. The Data Controller may conduct such audit not more than once annually, unless otherwise required by Applicable Data Protection Law. The Data Controller shall reimburse the Data Processor for any time spent on any such on-site audit at the Data Processor's then-current rates, which are available upon request. The Data Controller shall provide at least fourteen (14) days' prior written notice of its intent to undertake such on-site audit, and the Data Controller and Data Processor shall, before the commencement of any such audit, mutually agree upon the scope, the timing, the duration and the rate of reimbursement of such audit. (All reimbursement rates shall be reasonable, taking into account the resources expended by the Data Processor.) The Data Controller shall promptly notify the Data Processor of any non- compliance discovered during the course of such audit, and the Data Processor will use commercially reasonable efforts to address any confirmed non-compliance. If the Standard Contractual Clauses apply to this Addendum, then the Data Controller agrees to exercise its audit rights under the Standard Contractual Clauses as described in this Section 5(d), and the Data Controller has the right under the Standard Contractual Clauses to change its instruction and agrees to do so in writing in accordance with the "Notices" section of the Agreement.

6. INTERNATIONAL TRANSFERS

In order to ensure adequate safeguards for the Personal Data where it is transferred from the Data Controller, if in the EU, to the Data Processor in a Third Country, the Data Controller shall comply with the exporter's obligations in the Standard Contractual Clauses, and the Data Processor shall comply with the importer's obligations in the Standard Contractual Clauses in respect of that transferred Personal Data. The Standard Contractual Clauses are deemed to be incorporated into and form part of this Addendum, and Appendix 1 to the Standard Contractual Clauses is deemed to incorporate the information set out in Section 2 of this Addendum and Appendix 2 to the Standard Contractual Clauses is deemed to incorporate the information set out in Section 5 of this Addendum. To the extent that the Standard Contractual Clauses, as a statutory mechanism to normalize international data transfers, are subsequently modified, revoked, or held by the Court of Justice of the European Union to be invalid, the Data Controller and the Data Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support such transfer, which may include reliance on the Data Processor's self-certification under the US-EU Privacy Shield Framework.

7. SUB-PROCESSING

(a) The Data Controller hereby grants the Data Processor general written authorization to engage the Data Processor's Affiliates to Process the Personal Data of the Data Controller and authorizes the Data Processor and its Affiliates to engage sub-processors in connection with the delivery of services under the Agreement. The Data Controller hereby authorizes the use by the Data Processor and its Affiliate of

the sub-processors identified at https://www.nasuni.com/legal/data-processing-addendum/subprocessors/ (subject to the requirements of this Section 7). The Data Processor may engage new sub-processors or may change sub-processors from time to time. The Data Processor will provide the Data Controller with notice (by updating the sub-processor list at https://www.nasuni.com/legal/data-processing-addendum/subprocessors/ and by providing the Data Controller with a mechanism to receive notice of such updates) of any new sub-processor at least 14 days in advance of providing such sub-processor with access to Personal Data. The Data Controller will have 14 days from the date of receipt of the notice to approve or reject the new sub-processor. In the event of no response from the Data Controller, the sub- processor will be deemed accepted. If the Data Controller rejects the new or replacement sub-processor, the Data Processor may terminate Support with immediate effect, and without liability to Nasuni, on written notice to the Data Controller.

The Data Processor shall enter into written agreements with its sub-processors containing data protection obligations that provide at least the same level of protection for the Personal Data as are imposed under this Addendum and shall in particular impose on its sub-processors the obligation to implement appropriate technical and organizational measures in such a manner that the sub-Processing will meet the requirements of Applicable Data Protection Law. The Data Processor shall supervise the sub-processor's compliance with its obligations and, where a sub-processor fails to fulfil its obligations, the Data Processor shall remain fully liable under the Applicable Data Protection Law to the Data Controller for the performance of that sub-processor's obligations.

(b) The Data Controller may request that the Data Processor audit a third party sub-processor or provide confirmation that such an audit has occurred or, where available, obtain or assist customer in obtaining a third-party audit report concerning the sub-processor's operations, to ensure the sub-processor's compliance with its obligations imposed by the Data Processor in conformity with this Addendum.

8. RETURN OR DESTRUCTION OF PERSONAL DATA

Upon termination of this Addendum, upon the Data Controller's written request, or upon fulfillment of the Purpose whereby no further Processing is required, the Data Processor shall, at the discretion of the Data Controller, either delete, destroy or return all Personal Data to the Data Controller and destroy or return any existing copies, except where otherwise required by applicable law. The return of data may incur additional charges by the Data Processor. The Data Processor agrees to preserve the confidentiality of any retained Personal Data and will only Process such Personal Data after the date of termination in order to comply with the laws to which it is subject and to fulfill its obligations under this Addendum.

9. ASSISTANCE TO DATA CONTROLLER

(a) The Data Processor shall, to the extent legally permissible, promptly notify the Data Controller of any requests from a Data Subject to exercise the following rights of the Data Subject under the Applicable Data Protection Law: access, rectification, restriction of Processing, erasure (the "right to be forgotten"), data portability, objection to the Processing, or to not be subject to automated individual decision making (each a ***"Data Subject Request"***). Taking into the account the nature of the Processing, the Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as this is commercially reasonable, for the fulfilment of the Data Controller's obligation to respond to the Data Subject Request under Applicable Data Protection Law. In addition, to the extent the Data Controller, in its use of the Services, does not have the ability to address a Data Subject Request, the Data Processor shall, upon the Data Controller's request, use commercially reasonable efforts to assist the Data Controller in responding to such Data Subject Request, to the extent the Data Processor is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Law.

(b) Upon the Data Controller's request, the Data Processor shall provide the Data Controller with reasonable cooperation and assistance to help the Data Controller fulfill its obligations (if applicable) under the GDPR to carry out a data impact assessment related to the Data Controller's use of the Services, to

the extent the Data Controller does not otherwise have access to the relevant information, and to the extent such information is available to the Data Processor. The Data Processor will provide reasonable assistance to the Data Controller in the cooperation or prior consultations with Regulators as required under Article 36 of the GDPR, taking into account the nature of the Processing.

(c) The Data Controller shall be responsible for any costs arising from the Data Processor's provision of such assistance, under this Section 9.

10. INFORMATION OBLIGATIONS AND INCIDENT MANAGEMENT

(a) When the Data Processor becomes aware of an incident that materially adversely affects the Processing of the Personal Data that is the subject of the Agreement, it shall promptly notify the Data Controller about the incident, shall provide commercially reasonable cooperation to the Data Controller, and shall take commercially reasonable steps to remediate the incident, if applicable, to the extent that remediation is within the Data Processor's control. The obligations of this Section 10(a) do not apply to incidents that are caused by the Data Controller, Authorized Users, and/or any products and services other than Data Processor's.

(b) The term ***"incident"*** used in Section 10(a) shall mean in any case:

(i) a government investigation into or seizure of the Personal Data held by Data Processor or a sub-processor, or a specific indication that such an investigation or seizure is imminent;

(ii) any unauthorized or accidental access, processing, deletion, loss or any form of unlawful Processing of the Personal Data held by Data Processor or a sub-processor; or

(iii) any breach of the security and/or confidentiality obligations as set out in Sections 4 or 5 of this Addendum leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or being about to take place.

(c) The Data Processor shall maintain written procedures to enable it to promptly respond to the Data Controller about an incident. Where the incident is reasonably likely to require a data breach notification by the Data Controller under the Applicable Data Protection Law, the Data Processor shall implement its written procedures in such a way that it is able to notify the Data Controller in the time frame required by Applicable Data Protection Law after becoming aware of such an incident.

11. MISCELLANEOUS

(a) The liability of each party and its respective Affiliates', taken together in the aggregate, arising out of or relating to this Addendum shall be subject to the section(s) of the Agreement governing limitations of liability, and any reference in such section(s) to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all Data Processing Addendums together.

(b) This Addendum and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes and claims) shall be governed by and construed in accordance with the laws applicable to the Agreement of which this Addendum forms a part.

(c) This Addendum shall automatically terminate on the expiration or earlier termination of the Agreement.

[END]