

Customer Data Processing Addendum

Last updated: July 10, 2026

This Data Processing Addendum ("**DPA**") is between Nasuni Corporation ("**Nasuni**," "**we**," "**our**," or "**us**") and the customer ("**Customer**," "**you**," or "**your**"). This DPA forms part of the Software Solutions Agreement or End User License Agreement ("**Agreement**"), as applicable, entered into between Nasuni and Customer, and applies to the extent that (i) Nasuni processes Personal Data (as defined below) on behalf of Customer in the course of providing the Solutions or Software (also defined below); and (ii) the Agreement expressly incorporates this DPA by reference.

This DPA serves as the final and entire expression of the parties' agreement on the subject matter hereof. Any terms capitalized and not defined here shall have the meaning as defined in the Agreement.

HOW TO EXECUTE THIS DPA:

- 1) This DPA consists of two parts: the DPA main body (Data Processing Terms) and Exhibit 1 (which includes the Standard Contractual Clauses).
- 2) Nasuni has pre-signed this DPA. Nasuni, as the data importer, has also pre-signed The Standard Contractual Clauses in Exhibit 1.
- 3) To complete this DPA, Customer must:
 - a) Complete the information in the signature boxes and sign on page 6.
 - b) Complete the information on page 7.
 - c) Complete the information and sign on page 18.
 - d) Send the completed and signed DPA to Nasuni by email, indicating the Customer's Name and Account (as set out on the applicable Nasuni order form or invoice) to privacy@nasuni.com.

This DPA will become legally binding once Nasuni receives Customer's validly completed DPA at privacy@nasuni.com.

Data Processing Terms

/ DEFINITIONS

"Affiliate" means an entity that owns or controls, is owned or controlled by, or is or under common control or ownership with either Nasuni or Customer where control is defined as the possession, directly or indirectly, or the power to direct an entity's management and policies, whether through ownership of voting security, by contract, or otherwise.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Protection Laws" means the GDPR, UK GDPR, FADP, CCPA, and applicable data protection, privacy, security, breach notification, or similar laws of any other country or state.

"Data Security Incident" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Nasuni's possession or control.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"Data Subject Request" means a request from a Data Subject to exercise any right under relevant Data Protection Laws.

"EEA" means the European Economic Area.

"European Data Protection Laws" means the GDPR and Directive 2002/58/EC (ePrivacy), in each case as transposed into domestic legislation of each EEA Member State and in each case as amended, replaced, or superseded from time to time; the UK GDPR; and the FADP.

"EU Model Clauses" means the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 currently found at https://commission.europa.eu/law/lawtopic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, as may be amended, superseded or replaced and set forth in Exhibit 1 which apply to Processing of Personal Data.

"European Personal Data" means Personal Data that is subject to the protection of European Data Protection Laws.

"FADP" means the Swiss Federal Data Protection Act, as may be amended, superseded or replaced.

"GDPR" means the General Data Protection Regulation, 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.

"Personal Data" means any information relating to an identified or identifiable natural person; that is processed by Nasuni on behalf of Customer in connection with the Solutions and is subject to applicable Data Protection Laws.

"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.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Security, Privacy, and Architecture Documentation" means the documentation located in the Nasuni Trust Center at <https://trust.nasuni.com/>.

"Solutions" means any Nasuni product, service offering, or service provided to Customer pursuant to the Agreement.

"Sub-processor" means any Processor that Nasuni or its Affiliates engage to Process Personal Data in connection with the Solutions.

"UK GDPR" means the GDPR as transposed into 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.

"UK IDTA" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK

Information Commissioner under Section 119A(1) Data Protection Act 2018, as may be updated, amended, replaced or superseded from time to time by the UK Government.

/ PROCESSING

Roles of the Parties. The parties agree, regarding the Processing of Personal Data under relevant Data Protection Laws and this DPA, that (i) you determine the purposes and means of Processing and are the Controller of such data; and (ii) Nasuni is a Processor or service provider (as defined in the CCPA) Processing your Personal Data on Your behalf. Each party will comply with its applicable obligations under the relevant Data Protection Laws.

Sub-processing. Nasuni and its Affiliates engage Sub-processors pursuant to Section 5 below.

Processing Details. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further detailed in the Agreement, this DPA, including Exhibit 1, and Nasuni's Privacy Notice located at <https://www.nasuni.com/legal/privacy/>.

Data Subject Rights. If legally permitted, Nasuni will promptly notify you if it receives a Data Subject Request. If you have access to the data, you must respond to the Data Subject Request. If you are unable to address a Data Subject Request then upon receiving your written request Nasuni will provide commercially reasonable efforts to assist You in responding if legally permitted and/or required to under relevant Data Protection Laws. You are responsible for any costs arising from Nasuni's provision of such assistance if the requests are manifestly unfounded or excessive.

Legal Disclosure Request. If legally permitted, Nasuni will promptly notify you if it receives a legally binding request for the disclosure of Personal Data pursuant to this DPA, including from a supervisory authority. Nasuni manages such requests pursuant to the Agreement and relevant Data Protection Laws.

/ PERSONNEL

Nasuni will (i) restrict its personnel from Processing Personal Data without authorization (unless required by applicable law); and (ii) ensure personnel engaged to Process Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and are subject to confidentiality obligations.

/ SUB-PROCESSORS

Appointment of Sub-processors. You agree that: (i) Nasuni's Affiliates may be retained as Subprocessors; and (ii) Nasuni and its Affiliates respectively may engage third-party Sub-processors in connection with Processing Personal Data. Nasuni or a Nasuni Affiliate has entered into a written agreement with the applicable Sub-processors containing data protection obligations substantially similar to those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Solutions provided by such Sub-processor; and (iii) Nasuni shall be liable for its Sub-processors' acts and omissions to the same extent Nasuni would be liable if performing the Solutions of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

Current Sub-processors and Notification of New Sub-processors. Nasuni uses Sub-processors to provide its Solutions. These Sub-processors and their geographic locations are listed in *ANNEX III to Exhibit 1*.

Objection Right for New Sub-processors. Nasuni will notify you of any new Sub-processors via the email addresses you have designated in the Nasuni Portal. You may reasonably object in good faith to Nasuni's use of a new Sub-processor by sending written notification to Nasuni via privacy@nasuni.com within fifteen (15) days after receiving an updated Sub-processor List. If you object to a new Sub-processor, Nasuni will use reasonable efforts to change your configuration or use of the Solutions to avoid Processing of Personal Data by the Sub-processor in question. If Nasuni is unable to make such change within a reasonable period of time, either party may terminate the applicable Nasuni order form(s) with regard to Solutions which Nasuni cannot provide without using the new Sub-processor you objected to.

/ SECURITY

Nasuni Obligations. Nasuni shall maintain reasonable and appropriate technical and organizational measures to protect the security, confidentiality and integrity of Personal Data. You are responsible for implementing the appropriate technical and organizational measures for your Processing of Personal Data as well as using and configuring the Solutions in a manner that complies with relevant Data Protection Laws.

Certifications and Audit. Upon written request no more than once annually and subject to this Agreement's confidentiality obligations, Nasuni will provide you or your independent third party auditor information regarding Nasuni's compliance with this DPA's obligations in the form of a then-current third-party audit report, certification, or other relevant security documentation made available by Nasuni, including through Nasuni's Trust Center, as applicable. Nasuni will also reasonably cooperate and assist you in fulfilling Your GDPR obligations to carry out a data protection impact assessment related to your use of the Solutions if Nasuni has such information and you do not have access to the relevant information.

/ DATA SECURITY INCIDENT AND NOTIFICATION

If Nasuni becomes aware of a Data Security Incident involving your Personal Data, it shall: (i) notify you of the Data Security Incident without undue delay and as required by relevant Data Protection Laws; and (ii) where possible and not prohibited by law, Nasuni will use reasonable efforts to assist you in mitigating the impact of the Data Security Incident's adverse effects. Nasuni's obligations do not apply to incidents caused by you or your users.

/ TRANSFER MECHANISMS

Any European Personal Data transferred pursuant to this DPA to a country that does not ensure an adequate level of data protection within the meaning of European Data Protection Laws, or otherwise benefit from an applicable adequacy decision or other lawful transfer mechanism shall be made by Nasuni and its Affiliates in accordance with, and will be subject to, the applicable terms identified in this Section 8. For clarity, the transfer mechanisms described in this Section 8 apply to the extent required by the law governing the Personal Data transferred.

With respect to any European Personal Data transfer subject to the GDPR, the transfer shall be carried out in accordance with, and will be subject to, the Standard Contractual Clauses adopted pursuant to Commission Decision (EU) 2021/914 (the "EU SCCs," also referred to as the "Model Clauses"), as set out in Exhibit 1, which will form contractual terms between the parties for that particular transfer of European Personal Data with You as data exporter and Nasuni as data importer.

With respect to any European Personal Data transfer subject to the UK GDPR, the parties hereby enter into the UK IDTA (with you as data exporter and Nasuni as data importer), which is incorporated by reference into this DPA and which shall come into effect upon the commencement of such transfer. Any conflict between the terms of the EU Model Clauses and the UK IDTA will be resolved in accordance with Section 10 and Section 11 of the UK IDTA. The parties make the following selections for the purpose of the UK IDTA:

Part 1: Tables

Table 1

1. The Start Date is the Effective Date of the Agreement.
2. The Exporter is Customer and the Importer is Nasuni.
3. The Exporter's details are found in Annex I to Exhibit 1. The Importer's details are found in Annex I to Exhibit 1.
4. The Exporter's Key Contact can be found in Annex I to Exhibit 1. The Importer's Key Contact information can be found in Annex I to Exhibit 1.

Table 2:

The Parties choose the EU Model Clauses as set out in Exhibit 1, including the Appendix Information and with only the following modules, clauses, or optional provisions of the EU Model Clauses brought into effect for the purposes of this IDTA:

1. Clause 7 – See Exhibit 1, Clause 7.
2. Clause 9 – See Exhibit 1, Clause 9.
3. Clause 11 – See Exhibit 1, Clause 11.

Table 3

1. Annex IA: See Annex I to Exhibit 1.
2. Annex IB: See Annex I to Exhibit 1.
3. Annex II: See Annex II to Exhibit 1.
4. Annex III: See Annex III to Exhibit 1.

Table 4

1. The Importer may end this IDTA to the extent permitted by the UK IDTA, including where the transfer is no longer restricted or another lawful transfer mechanism applies.

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 18 of those Mandatory Clauses.

With respect to any European Personal Data transfer subject to the FADP, the transfer shall be carried out in accordance with, and will be subject to, the EU Model Clauses set out in Exhibit 1, which will form contractual terms between the parties for that particular transfer of European Personal Data with You as data exporter and Nasuni as data importer. The parties make the same elections as outlined in Exhibit 1 for European Personal Data, with the following additional modifications:

- i. References to the GDPR shall be interpreted as references to the FADP, including any applicable implementing ordinances and any amendment, replacement, or successor legislation (whereby "the competent supervisory authority" and "competent courts" shall mean the "Swiss Federal Data Protection and Information Commissioner" and the "relevant courts in Switzerland").
- ii. "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the meaning assigned to them by the FADP, including any applicable implementing ordinances and any amendment, replacement, or successor legislation (whereby "the competent supervisory authority" and "competent courts" shall mean the "Swiss Federal Data Protection and Information Commissioner" and the "relevant courts in Switzerland").
- iii. References to "Member State", "EU" and "Union law" and shall be interpreted as references to Swiss law.

In the event You transfer Personal Data that relates to data subjects in Switzerland to Nasuni, the terms in this subsection shall modify the corresponding references in this DPA. For clarity and avoidance of doubt, the terms in this subsection will amend this DPA to the extent necessary for compliance with the FADP. The terms in this subsection shall only apply to personal data subject to the FADP.

/ TERMINATION RIGHT

Either party may terminate the EU Model Clauses to the extent permitted by the EU Model Clauses or applicable Data Protection Laws, including where the applicable transfer is no longer a restricted transfer or another lawful transfer mechanism applies.

/ MISCELLANEOUS

The Agreement and this DPA apply only to the parties. Neither the Agreement or this DPA confers any rights to any other person or entity. This DPA does not modify the risk allocation agreed upon by the parties in the Agreement.

/ CCPA PROVISIONS

This Section 11 (CCPA Provisions) applies solely to Personal Data of California residents as defined in Section 1798.140(g) of the CCPA.

The parties agree that Nasuni is a Service Provider and Customer is a Business for CCPA's purposes and that Nasuni will process personal information pursuant to your instructions in connection with the Solutions.

SIGNATURE PAGE FOLLOWS



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):

Signature:.....

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Amanda Ray

Position: General Counsel

Address: One Marina Park Drive, Boston, Massachusetts 02210

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

Signature:..... /s/ *Amanda Ray*.....

Exhibit 1

Standard Contractual Clauses

For purposes of Article 46 of Regulation (EU) 2016/679 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: Nasuni Corporation

Address: One Marina Park Drive, Boston, Massachusetts 02210

E-mail: privacy@nasuni.com

Other information needed to identify the organisation: None

(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 the Appendix.

Clause 1

Definitions Purpose and scope

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

(b) The Parties:

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

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

(hereinafter: “Clauses”).

- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - (iii) Clause 9;
 - (iv) Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e); and (viii) Clause 18.
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

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

- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful

summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

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

- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 60 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the subprocessor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the subprocessor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the subprocessor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13; (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

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

- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. 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 the EU Member State in which the data exporter is established.

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name of the data exporting organisation:

Address:

Contact details:

.....

.....

Activities relevant to the data transferred under these Clauses:.....

.....

Signature and date:.....

Role: controller

Data importer(s):

2. Name of the data importing organisation: Nasuni Corporation

Address: One Marina Park Drive, Boston, Massachusetts 02210

Tel.: +1.857.444.8500

E-mail: privacy@nasuni.com

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of Nasuni's Solutions under the Agreement.

Other information needed to identify the organisation: None

Signature and date:..... /s/ *Amanda Ray*.....

Role: processor

B. DESCRIPTION OF TRANSFER

Data exporter may submit personal data to the Solutions, 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 personal data relating to the following categories of data subjects, when obtained, retained, and transmitted in accordance with the policies of the data exporter and with all legal requirements to which the data exporter is subject:

Categories of data subjects whose personal data is transferred

- Data exporter's Users;
- Data exporter's employees;
- Data exporter's consultants;
- Data exporter's contractors;
- Data exporter's agents; and
- Third parties that data exporter conducts business with.

Categories of personal data transferred

Any personal data in the Customer Data that data exporter provides to data importer or makes available through the Solutions. Personal data may include, but is not limited to, the following categories:

- First and last name
- Contact information (company, email address, phone and physical address)
- Financial information
- Account information
- IP and MAC address
- Browser information
- Product information, including localization data, network device information, activity logs, connection data, system usage and network data, application information, email data, traffic data, and other electronic data submitted, stored, uploaded, sent, or received by data exporter or data subjects via the Solutions

Sensitive data transferred (if applicable):

The frequency of the transfer:

Continuously as required to provide the Solutions.

Nature of the processing:

Data importer will process personal data in connection with providing the Solutions as described in the Agreement.

Purpose(s) of the data transfer and further processing

Data importer will transfer and process personal data in connection with providing the Solutions as described in the Agreement.

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

Personal data will be processed for the duration of the Agreement and any applicable Order, and thereafter as necessary to comply with the Agreement, this DPA, applicable Data Protection Laws, and Nasuni's standard backup, deletion, legal, compliance, and security retention practices. Data exporter may determine the duration of Processing through its use and configuration of the Solutions, except to the extent Personal Data is retained by data importer as required or permitted by the Agreement, this DPA, or applicable law.

C. COMPETENT SUPERVISORY AUTHORITY

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

ANNEX II

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

Nasuni's procedures for ensuring ongoing privacy, confidentiality, integrity, availability and resilience of processing systems and Solutions are described in its Trust Center at <https://trust.nasuni.com>.

ANNEX III

Nasuni's List of Sub-processors is located at: <https://www.nasuni.com/legal/nasuni-sub-processors/>.