Customer Data Protection and Privacy Exhibit for Juniper Products and Services

This Customer Data Protection and Privacy Exhibit for Juniper Products and Services ("**DPA**") supplements the Main Agreement (as may be updated from time to time) and covers the products or services ("**Products and Services**") provided or rendered by Juniper Networks, Inc., 1133 Innovation Way, Sunnyvale, CA 94089, United States and any of its affiliates, as applicable, that may Process Customer Personal Data ("**Juniper Networks**") under a respective end user services agreement or other contract ("**Main Agreement**") between and Juniper Networks and the contracting party receiving Products and Services (as defined in the Main Agreement, hereinafter "**Customer**"), as sold by Juniper Networks or an authorized reseller. This DPA is entered into by and between Juniper Networks and Customer, whether Customer entered into a Main Agreement with Juniper Networks or an authorized reseller.

1. Definitions. Terms used in this DPA shall have the meaning indicated below unless otherwise defined in this DPA.

1.1 "Customer Personal Data" shall mean the Personal Data described in Schedule 1 of this DPA, in respect of which Customer is the Controller and which is provided to Juniper Networks by or on behalf of Customer and Processed by Juniper Networks, each in connection with the Main Agreement for Juniper Networks to provide Products and Services to Customer.

1.2 "Data Protection Requirements" shall mean any laws or regulations applicable to the Processing of Personal Data or personal information (or similar term under the applicable law or regulation).

1.3 "**Personal Data**", "**Data Subject**", "**Process**", "**Processor**", "**Controller**", "**Supervisory Authority**", "**Sell**", "**Share**", and "**Service Provider**" will each have the meaning given to them in applicable Data Protection Requirements.

1.4 "Standard Contractual Clauses" means: (i) the Standard Contractual Clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 or any subsequent version thereof released by the European Commission (which will automatically apply) (the "**EU SCCs**"); (ii) where UK Data Protection Requirements (as defined in Section 4.4 applies), the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**").

Any other terms that are capitalized but not defined below shall have the meanings set forth in Data Protection Requirements and/or the Main Agreement, as applicable.

2. General Provisions.

2.1. This DPA applies to the Processing of Customer Personal Data. If Data Protection Requirements recognize the roles of "Controller", "Processor", or "Service Provider" as applied to Customer Personal Data then, as between Juniper Networks and Customer, Customer acts as Controller and Juniper Networks acts as a Processor (or Subprocessor, as the case may be) or Service Provider of Customer Personal Data. Juniper Networks will only Process Customer Personal Data as a Processor on behalf of and in accordance with Customer's prior written instructions, including with respect to transfers of Customer Personal Data, unless Processing is required by Data Protection Requirements to which Juniper Networks is subject, in which case Juniper Networks shall, to the extent permitted by applicable law, inform Customer of that legal requirement before so Processing that Customer Personal Data. The Parties agree that such instructions are contained in the Main Agreement and that Juniper Networks may Process Customer Personal Data as necessary to enable Juniper Networks to provide the Products and Services according to the Main Agreement, which includes processing Customer Personal Data as reasonably necessary for the internal purposes of improving the Products and Services and enhancing the user experience. Any additional or different instructions require a signed agreement between Juniper Networks and Customer and may be subject to additional fees. For the avoidance of doubt, Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Requirements. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Personal Data. Juniper Networks will immediately inform Customer if, in its opinion, an instruction from Customer infringes the Data Protection Requirements, provided, however, Juniper Networks is not responsible for performing legal research and/or for providing legal advice to Customer.

2.2. If Juniper Networks cannot Process Customer Personal Data according to Customer's instructions due to a legal requirement under any Data Protection Requirements, Juniper Networks will promptly notify Customer of such inability, providing a

reasonable level of detail as to the instructions with which it cannot comply and the reasons why it cannot comply, to the greatest extent permitted by applicable law.

2.3. Unless set forth in a statement of work, order, or other document, Customer Personal Data may not include any sensitive or special data that imposes specific data security or data protection obligations on Juniper Networks in addition to or different from those specified in any documentation or which are not provided as part of the Products and Services.

2.4. Subject matter and other details of Juniper Networks' Processing are set forth in Schedule 1. Juniper Networks shall Process Customer Personal Data for an indefinite term for as long as the Main Agreement is in effect.

2.5. If and to the extent there are conflicts between this DPA (excluding its Schedules) and the Schedules, the applicable Schedule(s) shall prevail, unless otherwise required under Data Protection Requirements.

3. Additional US Privacy Obligations. To the extent required under applicable US Data Protection Requirements, Juniper Networks: (i) shall not Sell or Share Customer Personal Data; (ii) shall retain, use, or disclose Customer Personal Data only to provide the Products and Services and shall not retain, use, or disclose Customer Personal Data for any other purpose, except as may be permitted by applicable US Data Protection Requirements or this Agreement; (iii) shall not retain, use, or disclose Customer Personal Data collected by Juniper Networks outside of the direct business relationship between the parties, except as may be permitted by applicable US Data Protection Requirements or this Agreement; (iv) grants Customer the right, upon notice, and consistent with the terms in Section 18, to take reasonable and appropriate steps to stop and remediate Juniper Networks' unauthorized use of Customer Personal Data as permitted by applicable US Data Protection Requirements; (v) shall not combine Customer Personal Data that Juniper Networks receives from or on behalf of another person(s), except as permitted by applicable US Data Protection Requirements; and (vi) shall notify Customer if it determines that it can no longer meet its obligations under US Data Protection Requirements.

4. International Transfers.

4.1. In accordance with Customer's instructions under Section 2.1, Juniper Networks may Process Customer Personal Data on a global basis as necessary to provide the Products and Services, including for IT security purposes, maintenance and provision of the Products and Services and related infrastructure, technical support, and change management. Without limiting Sections 4.2 through 4.6, Juniper Networks shall implement technical and organizational measures consistent with this DPA to provide a comparable level of protection for Customer Personal Data in the jurisdiction in which it is Processed. Juniper Networks shall comply with Schedule 2 in its processing of Customer Personal Data outside of the country from which the Personal Data originated.

4.2. To the extent that the Processing of Customer Personal Data by Juniper Networks involves the transfer of such Customer Personal Data from the European Economic Area ("**EEA**") to a country or territory outside the EEA, other than a country or territory that has received a binding adequacy decision as determined by the European Commission (an "**EEA Transfer**"), such EEA Transfer shall be subject to the EU SCCs as set forth below.

4.3. Customer shall be deemed to have signed the EU SCCs in Annex I in its capacity as "data exporter" and Juniper Networks in its capacity as "data importer." Module Two or Module Three of the EU SCCs shall apply to the transfer depending on whether Customer is Controller of the Customer Personal Data (for Module Two) or a Processor of the Customer Personal Data on behalf of its end customer(s) (for Module Three). If Module Three applies, Customer notifies Juniper Networks that Customer is a Processor and the instructions are set forth in Section 2.1. With regards to optional clauses within the EU SCCs, Clause 7 is not selected and the optional paragraph within Clause 11 is not selected. For purposes of Clauses 17 and 18 of the EU SCCs, the parties select The Netherlands.

4.4. Where Customer Personal Data originating from the United Kingdom specifically is processed by Juniper Networks outside of the United Kingdom, in a territory that has not been designated by the UK Information Commissioner's Office as ensuring an adequate level of protection pursuant to Data Protection Requirements, and to the extent such processing would be subject to the Data Protection Requirements applicable in the United Kingdom ("**UK Data Protection Requirements**") the Parties agree that: (i) the EU SCCs shall also apply to the processing of such Customer Personal Data, subject to the UK Addendum, which is completed as follows: (i) Table 1, 2, and 3 of the UK Addendum completed with the information within Schedule 1, attached hereto, and in accordance with the information set forth within Sections 4.3 and 10; and (ii) and the option "neither party" is selected in Table 4.

4.5. For Personal Data originating from Switzerland, references in the EU SCCs to: (i) the words "EU" and "EEA" are replaced with the "Switzerland"; (ii) "EU Data Protection Law" is replaced with "Federal Act on Data Protection"; and (iii) the "European Commission" is be replaced with the "Federal Data Protection and Information Commissioner". The term "member state" is interpreted to include data subjects in Switzerland.

4.6. In the event of any conflict between any terms in the Standard Contractual Clauses and DPA, the Standard Contractual Clauses shall prevail to the extent of the conflict. The Standard Contractual Clauses will cease to apply if Juniper Networks implements an alternative recognized compliance mechanism for the lawful transfer of Personal Data in accordance with Data Protection Requirements, in which case such alternative mechanism shall apply.

5. Bundling of Data Importers. The parties agree that the bundling of Juniper Networks entities as processors within this single DPA is only undertaken for efficiency purposes (*i.e.*, to avoid a multitude of different contract documents) and (i) shall result in legally separate DPAs between the respective Customer entity and the Juniper Networks entity and (ii) shall not create any legal or other relationship whatsoever between the "bundled" Juniper Networks entity.

6. Bundling of Data Exporters. The parties agree that the bundling of Customer entities, for example, if Customer is comprised of multiple global affiliates, as Controllers within this single DPA is undertaken for efficiency purposes (*i.e.*, to avoid a multitude of different contract documents) and (i) shall result in legally separate DPAs between the respective Customer entity and Juniper Networks solely for purposes of addressing any such obligations under Data Protection Requirements; (ii) shall not create any new or different legal or other relationship whatsoever between the "bundled" Customer entities; (iii) does not create any additional rights or remedies for such bundled Customer entities; (iv) all Processing instructions must be provided by the Customer entity that is signatory to the Main Agreement and Juniper Networks is not responsible for consolidating or evaluating the validity of instructions received from bundled Customer entities; (v) any commercial terms not provided by the DPA are provided by the Main Agreement regardless of whether the bundled Customer entities signed or were consulted regarding the terms of the Main Agreement; and (vi) any audits conducted in accordance with the DPA and by and through the Customer entity that is signatory to the Main Agreement.

7. Data Protection Compliance. Each party undertakes to comply with the Data Protection Requirements applicable to such party's Processing of Personal Data in connection with the Main Agreement. Customer as a Controller hereby warrants that it has provided all required notices and obtained all permissions or, if applicable and sufficient under Data Protection Requirements, another valid legal basis, required under Data Protection Requirements to provide Juniper Networks with any Personal Data of the Data Subjects specified in Schedule 1 to this DPA or otherwise provided by Customer in connection with the Products and Services. Customer acknowledges that Juniper Networks is reliant on Customer for direction as to the extent to which Juniper Networks is entitled to Process Customer Personal Data. Consequently, Juniper Networks will not be liable for any claim brought against Juniper Networks by a Data Subject arising from (i) Juniper Networks' actions in compliance with Customer's instructions or (ii) any act or omission by Customer in Customer's use of the Products and Services.

8. Data Secrecy and Confidentiality. Juniper Networks shall treat the Customer Personal Data as confidential and shall not disclose such data to any third parties unless authorized by Customer and in accordance with this DPA. This obligation continues to apply after the expiration or termination of this DPA for so long as Juniper Networks Processes Customer Personal Data. In accordance with Data Protection Requirements, Juniper Networks shall put procedures in place designed to ensure that all persons acting under its authority entrusted with the Processing of Customer Personal Data (i) have committed themselves to keep such data confidential and not to use such data for any purposes except for the provision of the Products and Services, or (ii) are under an appropriate statutory obligation of confidentiality. This obligation of confidentiality shall continue after the end of the respective engagement of such person. Juniper Networks will further instruct such persons regarding the applicable statutory provisions on data protection and shall ensure that access to Customer Personal Data is limited to those persons with a need to know.

9. Security Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Juniper Networks will implement appropriate technical and organizational measures designed to protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data (described under Annex II to the Standard Contractual Clauses). Juniper Networks may update its security practices from time to time but will not materially decrease the overall security of the Products and Services during the term of a statement of work or other ordering document. Such measures shall include process for regular testing, assessing and evaluating the effectiveness of the measures.

10. Subcontracting Authorization. When subcontracting the Products and Services or parts thereof to another Juniper Networks entity or a third party, if the subcontractor will Process Customer Personal Data, such subcontractor shall be a "Subprocessor"

and Juniper Networks will enter into a binding written agreement with the Subprocessor that imposes on the Subprocessor the same level of restrictions that apply to Juniper Networks under this DPA as well as any terms required to be included under applicable US Data Protection Requirements, in each case to the extent that such requirements are applicable to the Processing to be done under such subcontract. A list of Juniper Networks Subprocessors is available at https://support.juniper.net/support/subprocessor/index.page ("**Subprocessor List**"). For the avoidance of doubt and in accordance with Clause 9, Option 2 of the Standard Contractual Clauses, the above constitutes Customer's general authorization for Juniper Networks' engagement of Subprocessors and Juniper Networks' appointment of additional Subprocessors or replacement of any Subprocessors identified on the Subprocessor List and in Annex III. In addition to any notifications provided by Juniper Networks regarding the addition or replacement of Subprocessors or updates to the Subprocessor List, Customer agrees to subscribe to any mechanisms that Juniper Networks may provide for notifications regarding Subprocessors. Customer will provide any objections promptly (in any event no later than fourteen (14) days following any notification or update), provided such objections are based on documented evidence that establish the Subprocessor does not or cannot comply with this DPA or Data Protection Requirements and identify the reasonable data protection basis for the objection ("**Objection**"), so that Juniper Networks can evaluate the Objection and determine any appropriate action. In the event of an Objection, Customer and Juniper Networks will work together in good faith to find a mutually acceptable resolution to such Objection, including but not limited to reviewing additional documentation supporting the Subprocessor's compliance with the DPA or Data Protection Requirements.

11. Personal Data Breach Notification.

11.1. Juniper Networks will provide Customer promptly with a data breach notification (with contents detailed below) if Juniper Networks becomes aware of and confirms any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data or any other security incident that compromises the security, confidentiality or integrity of Customer Personal Data that requires a data breach notification to Customer according to Data Protection Requirements ("**Personal Data Breach**"). Customer and Juniper Networks shall work together in good faith within the timeframes for Customer to provide notifications in accordance with Data Protection Requirements to finalize the content of any such notifications to Data Subjects or Supervisory Authorities, as required by Data Protection Requirements. Juniper Networks' prior written approval shall be required for any statements regarding, or references to, the Personal Data Breach or Juniper Networks made by Customer in any such notifications.

11.2. As information regarding the Personal Data Breach becomes available for Juniper Networks to disclose to Customer, Juniper Networks will provide Customer with information regarding (1) the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Customer Personal Data records concerned; (2) the reasonably anticipated consequence of the Personal Data Breach; (3) summary of measures taken to address or mitigate any possible adverse effects; and (4) other information concerning the Personal Data Breach reasonably known or available to Juniper Networks that Customer is required to disclose to a Supervisory Authority or Data Subjects under Data Protection Requirements. Juniper Networks' contact point for additional details regarding a Personal Data Breach is privacy@juniper.net. Except as required by Data Protection Requirements, the obligations in this Section shall not apply to Personal Data Breaches caused by Customer.

12. Handling of Complaints, Inquiries and Orders. To the extent a Data Subject identifies Customer as the entity that collected its Personal Data, Juniper Networks shall notify Customer of the Data Subject's complaints and inquiries (e.g., regarding the rectification, deletion and blocking of or the access to Personal Data, or any other rights Data Subject has under Data Protection Requirements) ("**Data Subject Inquiry**") received by Juniper Networks relating to the Products and Services covered by the Main Agreement. To the extent Customer, in its use of the Products and Services, does not have the ability to address a Data Subject Inquiry, then at Customer's expense, Juniper Networks shall provide assistance to Customer to respond to such Data Subject Inquiry in a timely manner. Taking into account the nature of the Processing, Juniper Networks shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, in the fulfilment of Customer's obligations to respond to Data Subject Inquiry under Data Protection Requirements. Juniper Networks shall not independently respond to Data Subject Inquiries without Customer's prior approval, except where required by Data Protection Requirements. The same shall apply to orders and inquiries of courts or regulators. Juniper Networks will instruct Data Subjects that do not identify a relevant Controller to contact the correct Controller. Juniper Networks shall comply with Customer's instructions regarding the handling of a Data Subject Inquiry, subject to the terms of Section 2.1.

13. Term. The term of this DPA is identical with the term of the Main Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Main Agreement.

14. **Data Retention**. After the end of the provision of the Products and Services and pursuant to written instructions provided by Customer, Juniper Networks shall return to Customer or securely destroy all copies of Customer Personal Data Processed on behalf of Customer in Juniper Networks' role as a Processor in connection with the Products and Services. Upon Customer's written request, Juniper Networks shall provide Customer with a written statement confirming such return or destruction. Juniper Networks may retain Customer Personal Data to the extent required by applicable laws only for such period as required by applicable laws, or as necessary to protect its legal rights. Juniper Networks shall protect the confidentiality of all such retained Customer Personal Data and Process such Customer Personal Data only as necessary for the relevant purpose(s) requiring its storage and for no other purpose.

15. **Invalidity and/or Unenforceability.** Should any provision of this DPA be found invalid or unenforceable by a competent court of law, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, should this not be possible, construed in a manner as if the invalid or unenforceable part had never been contained therein.

16. **Liability.** Indemnification, liability, limitations of liability and any applicable exclusions under this DPA shall be governed by the Main Agreement to the extent permitted by Data Protection Requirements.

17. **Corporate Restructuring**. Juniper Networks may share and disclose Customer Personal Data and other data of Customer in connection with, or during the negotiation of, any merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of Juniper Networks' business by or to another company, including the transfer of contact information and data of customers, partners and end users.

18. **Information, Audits, and Assistance.**

    18.1. Upon Customer's written request, and subject to the confidentiality obligations set forth in the Agreement, Juniper Networks shall make available to Customer information reasonably necessary to substantiate Juniper Networks' compliance with this DPA. Customer may only use such information to confirm Juniper Networks' compliance with this DPA and to assist Customer with complying with its obligations under Data Protection Requirements. If no such information is available at the time of Customer's request, Juniper Networks will allow and cooperate in audits as set forth below.

    18.2. Customer shall have the right to carry out on-site audits (no more than once per year), during regular business hours without disrupting the Juniper Networks' business operations and in accordance with the Juniper Networks' security policies. Any third party engaged by Customer to conduct an audit must be pre-approved by Juniper Networks (such approval not to be unreasonably withheld) and sign Juniper Networks' confidentiality agreement.

    18.3. For any audits, Customer must provide Juniper Networks with a proposed audit plan at least two weeks in advance of the audit, after which Customer and Juniper Networks shall discuss in good faith and finalize the audit plan prior to commencement of audit activities. Customer shall reimburse Juniper Networks for any costs or expenses incurred by Juniper Networks in connection with an audit. Information obtained or results produced in connection with an audit are Juniper Networks' confidential information and may only be used by Customer to confirm Juniper's compliance with this DPA and to comply with Customer's obligations under Data Protection Requirements.

    18.4. At Customer's request and solely in order to support Customer's compliance with Data Protection Requirements, Juniper Networks shall provide, at Customer's expense, reasonably required assistance to Customer relating to data protection impact assessments and prior consultation with Supervisory Authorities, taking into account the nature of the processing and the information available to Juniper Networks. All information provided is Juniper Networks' confidential information.

19. **Amendments for Additional Local Data Protection Requirements.** To the extent that additional country-specific (or state, regional, provincial, or other geographic area specific) provisions are required under Data Protection Requirements, the parties agree to incorporate such provisions solely to the extent they are required and solely to the extent they are applicable to Customer Personal Data processed by Juniper Networks. Juniper Networks may, from time to time, post updated provisions related to local or other specific Data Protection Requirements at https://www.juniper.net/us/en/privacy-policy. Such posted provisions are automatically incorporated herein solely to the extent they are required under Data Protection Requirements.

SCHEDULE 1

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data Exporter:
Name: The Data Exporter is the entity identified "Customer" in the DPA.
Address: as set forth in the Main Agreement.
Contact person: as set forth in the Notices provision in the Main Agreement.
Activities relevant to the data transferred under this DPA: as set forth in the Main Agreement.
Signature and date: refer to DPA.
Role: Controller, except when processing data on behalf of another entity, in which case Data Exporter is a Processor.

Data Importer:
Name: The Data Importer is the entity identified as "Juniper Networks" in the DPA.
Address: as set forth in the Main Agreement.
Contact person: as set forth in the Notices provision in the Main Agreement.
Activities relevant to the data transferred under this DPA: as set forth in the Main Agreement.
Signature and date: refer to DPA.
Role: Processor, or Sub-processor if Data Exporter is a Processor.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects: The Customer Personal Data transferred concern the following categories of data subjects:

- Personnel of Data Exporter.
- Personnel of Data Exporter's partners (including any vendors, suppliers, agents or additional subprocessors as may be authorized by Data Exporter).
- Solely to the extent that such data is processed by Data Exporter and shared with Data Importer for processing under the Main Agreement, end users of Data Exporter.

Categories of Personal Data transferred: The personal data transferred concern the following categories of data in addition to any other categories as specified in: (a) the Main Agreement; (b) the Data Exporter Privacy Notice available at https://www.juniper.net/us/en/privacy-policy together with any Supplemental Privacy Information referenced therein (including for Mist Systems) ("**Privacy Notice**"); and (c) in any data sheets or related product documentation provided by Data Importer for the particular product or service ("**Documentation**"):

- Business Contact Data: Business contact information of the data subjects.
- End User Data:
    - Network Devices: Occasionally, Data Exporter or its end users' IP addresses, and less frequently, core dump files or network traffic snippets from a network device, may also be provided when requesting support and could be deemed to contain Personal Data to the extent it can be associated with an individual data subject.
    - Cloud Services: For Data Importer Products and Services that include Cloud services, the categories of data that may be processed are as set forth in the Privacy Notice and Documentation.
    - WLAN: For WLAN Products and Services of Data Importer, such as from its affiliate Mist Systems, Inc., the categories of data that may be processed are as set forth in the Privacy Notice and Documentation.
    - Professional Services: Any Personal Data that is shared with Data Importer by or on behalf of Data Exporter in connection with any professional services provided by Data Importer under the Main Agreement.

Supplemental product-specific information: Additional information regarding data processing related to particular Products and Services of Data Importer is available in the "**Supplemental Privacy Information**" section of the Privacy Notice.

Sensitive categories of data (if appropriate): The Personal Data transferred concerns the following special categories of data:
Data Importer does not require any special categories of data in order to provide its Products and Services. Unless otherwise specified in the Main Agreement, Data Exporter shall not provide and must receive prior written consent of Data Importer before transferring any special categories of data or sensitive data to Data Importer.

The frequency of the transfer: As set forth in the Main Agreement.

Nature of the Processing: The Personal Data transferred will be subject to the following basic processing activities:

> Providing the Products and Services in connection with the Main Agreement, providing related technical support and professional services under the Main Agreement (as applicable), and improving/enhancing such Products and Services and support services.

Data Importer also retains the right to process the Personal Data for purposes including enforcing its legal rights, complying with legal requirements, providing information on Products and Services, training resources, and opportunities for upgrades and enhancements, and other permitted purposes under applicable law, as set forth in the Privacy Notice.

Purposes of the data transfer and further Processing: The Processing activities defined in Section 2 of the DPA and in the Main Agreement.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period: As set forth in Sections 2.4 and 14 of the DPA, and in the Main Agreement.

For transfers to (sub-) Processors, also specify subject matter, nature and duration of the Processing: As set forth in Sections 2.4, 10, and 14 of the DPA, and as set forth in the Main Agreement.

C. COMPETENT SUPERVISORY AUTHORITY
If the Data Exporter is established in an EU Member State, the competent Supervisory Authority shall be the Supervisory Authority applicable to the establishment location of the Data Exporter. If the Data Exporter is not established in an EU Member State, the competent Supervisory Authority shall be the Supervisory Authority located where the Data Exporter has appointed its EU Representative. If the Data Exporter is not established in an EU Member State and is not required to appoint an EU Representative, the competent Supervisory Authority shall be the supervisory authority applicable to the location of the Data Subject whose data is at issue.

ANNEX II

Technical and organizational measures including technical and organizational measures to ensure the security of the Customer Personal Data:

1. **Information Security Governance**
   - The information security function within Data Importer reports directly to a company executive.
   - A Security and Privacy Steering Committee made up of representatives from business, information security, and privacy meets regularly to discuss and review information security policies, projects, and practices.
   - A comprehensive set of information security policies and standards are documented, approved, and regularly reviewed.
   - Personnel with access to Personal Data are subject to confidentiality obligations.

2. **Network Security**
   - Network security is maintained using industry standard techniques, including, for example, firewalls, intrusion detection systems, access control lists, and routing protocols.
   - Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 12 characters with at least three of the following four classes: upper case, lower case, numeral, special character) and be changed periodically.
   - WiFi networks are secured and encrypt data in transit. Guests are permitted to connect only to the guest WiFi network and are not allowed to connect to any production systems.
   - An intrusion detection or prevention system covers network traffic to the Data Importer information systems.
   - Network changes are tested prior to production deployment.
   - Firewalls are appropriately configured and implemented. Firewall policies are reviewed on a regular basis.
   - Employees and contractors are required to use VPN to connect remotely to the corporate network.

3. **Encryption**
   - Full disk encryption is configured on Data Importer-managed end point devices.
   - Encryption methods for Data Importer's systems which Process Data Exporter Personal Data are based on factors such as length of time such data are Processed, technical capabilities of third-party attackers, Data Importer's resources, and sensitivity of the Personal Data.
   - Encryption keys to Data Exporter's Personal Data are stored in a key management solution. Keys are rotated periodically and access to keys is restricted to limited personnel with administrative access only. Membership for encryption key ownership groups is regularly reviewed according to a written Encryption Key Management Standard.
   - Sensitive Personal Data is encrypted in transit and at rest in compliance with Data Importer's Information Security Cryptographic Policy.

4. **Identity and Access Management**
   - Data processing systems handling Personal Data are subject to measures designed to prevent access, loss or use without authorization.
   - Employees or contractors with access to Personal Data are assigned unique IDs.
   - Only authorized staff may grant, modify, or revoke access to Data Exporter's Personal Data. The list of authorized staff is regularly reviewed.
   - Systems processing Personal Data are required to integrate with Data Importer's single sign on authentication.
   - Access rights are assigned using the principle of least privilege and need-to-know.
   - Access is revoked upon termination of the employee or contractor.
   - Login attempts are limited, and accounts locked after a predetermined number of failed login attempts.
   - Remote access for critical applications is controlled via multi-factor authentication.
   - Systems processing Data Exporter's Personal Data implement session or screen lockouts after a predetermined period of inactivity.

5. **Physical Security**
   - Physical access to Data Importer buildings by unauthorized personnel is restricted.
   - Physical access controls, such as surveillance cameras and identification badges, are implemented for Data Importer's facilities.
   - Physical security systems such as fire suppression systems, flood controls, smoke detection, and UPS are utilized.

- Data Importer has implemented significant physical security measures such as perimeter security, access control, CCTV and alarm monitoring, visitor screening and control, security guarding and reception services, and 24-hour Security Operations Centers for monitoring and incident response.

6. Patch and Vulnerability Management

- Anti-malware and anti-virus software are in place and are updated on a regular cadence, including for Data Importer's managed devices handling Personal Data.
- Data Importer implements a patch management program designed to ensure security patches are appropriately applied to systems.
- Vulnerability scans for systems processing Data Exporter's Personal Data are performed on a periodic basis.
- Any known critical vulnerabilities as defined by Data Importer's risk assessment are assessed and remediated in a timely manner.
- Annual penetration tests are conducted for certain Data Exporter-facing systems.

7. Continuous System Monitoring

- Audit logging is implemented in production system. Audit logs are retained for appropriate periods, including as required by applicable regulatory requirements.
- Data Importer reviews and analyses information system audit records for indications of unusual activities.

8. Business Continuity Management

- Emergency and contingency plans are available and maintained in an effort to restore personal data, where applicable, as reasonably deemed appropriate by Data Importer.
- Business continuity plans are tested and updated on a periodic basis, as reasonably deemed appropriate by Data Importer.
- Backups of data are maintained for business continuity purposes, as reasonably deemed appropriate by Data Importer.

9. Incident Response

- Data Importer maintains a written Incident Response plan providing a standard process to investigate and address security incidents and regularly reviews the Incident Response plan.
- Data Importer will notify Data Exporter of Personal Data Breaches in accordance with the DPA and its Breach Notification Plan.
- Data Exporter may contact Data Importer at IT-CIRT@juniper.net for any available details regarding a Personal Data Breach.

10. Security Awareness

- Background checks are required on personnel at the time of hire, to the extent permitted under applicable law.
- Employees are required to undergo periodic privacy and information security training.
- Training is updated as deemed necessary by Data Importer.

11. Third Party Risk Management

- Sub-processors undergo a vendor information security review as appropriate based on their Personal Data access and are required to comply with vendor security requirements.
- Data Importer has a program to review the information security risk and control of third-party service providers. The review is performed on new and existing vendors. This includes reviews of the effectiveness of the controls of our third-party service providers who process Personal Data, for example through review of their SOC-2 Reports.

12. Secure Development

- Data Importer maintains a secure development program that includes measures such as secure coding practices; use of industry-standard practices to mitigate and protect against vulnerabilities; separate coding environments; source code vulnerability scanning; pre-release source code and application testing; and review of any open source of third-party code prior to its use.

13. Additional and/or Supplemental Technical Security Measures

- Additional and/or supplemental technical security measures, and appropriate modifications to the measures listed above, may be established by Data Importer periodically depending on the Products and Services offered and the type of Personal Data of Data Exporter that is Processed by Data Importer.

- Data Importer's policy does not permit BYOD or personally-owned devices to process Personal Data provided through the Services.
- In assisting Data Exporter with fulfilling data subject requests, Data Importer shall either (a) provide to Data Exporter an online self-service solution to enable Data Exporter to fulfill data subject requests or (b) otherwise provide reasonable means for Data Exporter to submit requests.
- A change control process is in place for changes to Data Importer production systems.
- Personal Data hosted for different Data Importer customers are logically separated.
- Storage media for customer-facing systems are either destroyed or securely erased at the end of their lifecycle.
- Data Importer incorporates privacy by design and privacy by default practices in its solution development processes.

ANNEX III

List of Data Importer's Subprocessors

As set forth on the webpage https://support.juniper.net/support/subprocessor/index.page.

SCHEDULE 2 – ADDITIONAL PROVISIONS
BASED ON EUROPEAN DATA PROTECTION BOARD RECOMMENDATIONS 01/2020

1. Juniper Networks shall, unless prohibited by law or a legally binding order of an applicable body or agency, promptly notify Customer of any request for the disclosure of Customer Personal Data by a governmental or regulatory body or law enforcement authority (including any Supervisory Authority) ("**Disclosure Request**") without responding to such request, unless otherwise required by applicable law (including to provide acknowledgement of receipt of the request). Juniper Networks will review applicable law to evaluate any Disclosure Request, for example the ability of the requesting authority to make the Disclosure Request, and will challenge the Disclosure Request if, after a careful assessment, it concludes that there are grounds under applicable law to do so. When challenging a Disclosure Request, Juniper Networks shall seek interim measures to suspend the effects of the Disclosure Request until an applicable court or other authority has decided on the merits. Juniper Networks shall not disclose Customer Personal Data requested until required to do so under applicable law. Juniper Networks shall only provide the minimum amount of Customer Personal Data permissible when responding to the Disclosure Request, based on a reasonable interpretation of the Disclosure Request. If the Disclosure Request is incompatible with the Standard Contractual Clauses or other data transfer mechanism utilized in accordance with Section 4 in this DPA, Juniper Networks will so notify the requesting authority and, if permitted by applicable law, notify the competent EEA government authority with jurisdiction over the Customer Personal Data subject to the Disclosure Request. Juniper Networks will maintain a record of Disclosure Requests and its evaluation, response, and handling of the requests. Juniper Networks will provide Customer with such records relevant to Customer Personal Data except as prohibited by applicable law or legal process or in the interest in protecting Juniper Networks' legal rights in connection with threatened, pending, or current litigation.
2. Juniper Networks has not purposefully created "back doors" or similar programming in its systems that provide Products and Services that could be used to access the systems and/or Customer Personal Data, nor has Juniper Networks purposefully created or changed its business processes in a manner that facilitates access to Customer Personal Data or its systems that provide the Products and Services. To the best of Juniper Networks' knowledge, United States Data Protection Requirements do not require Juniper Networks to create or maintain "back doors" or to facilitate access to Customer Personal Data or systems that provide Products and Services or for Juniper Networks to possess or provide the encryption key in connection with a United States Disclosure Request.
3. Juniper Networks shall use reasonable efforts to assist Customer and its Data Subjects, as instructed by Customer (in accordance with Section 12 of the DPA), regarding Disclosure Requests, unless prohibited by applicable law, for example to provide information to Customer in connection with the Data Subject's efforts to exercise its rights and obtain legally-available redress, provided Juniper Networks shall not be required to provide Customer or Data Subjects with legal advice.
4. Customer may request to audit Juniper Networks information regarding access to Customer Personal Data, subject to the terms of Section 18 of the DPA.
5. In the event Juniper Networks receives a request to voluntarily disclose unencrypted Customer Personal Data to a government authority, Juniper Networks will use reasonable efforts to first obtain Customer's consent, either on its behalf or on behalf of the relevant Data Subject.