Customer Data Protection and Privacy Exhibit for Juniper Products and Services

This data protection and privacy exhibit (the "**DPA**") supplements the Main Agreement (as may be updated from time to time) and is based on the standard contractual clauses as per Commission Decision 2010/87/EU as of February 5, 2010 (set forth below) and includes any Appendices referenced herein. This DPA covers the products or services ("**Juniper 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, ("**Juniper Networks**") under a respective end user services agreement or other contract ("**Main Agreement**") between the contracting party receiving Juniper Products and Services and Juniper Networks (as defined in the Main Agreement, hereinafter "**Customer**"), as sold by Juniper Networks or an authorized reseller, is entered into by and between the contracting party receiving Juniper Products and Services under the Main Agreement ("**Data Exporter**") and Juniper Networks and any other data importers as specified in Appendix 1 (each a "**Data Importer**").

Clause 1

Definitions

For the purposes of the Clauses:

(a) "personal data", "special categories of data", "process/processing", "controller", "processor", "data subject" and "supervisory authority" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) "the data exporter" means the controller who transfers the personal data;

(c) "the data importer" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) "the sub-processor" means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) "the applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) "technical and organisational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

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

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

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

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

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

Clause 10
Variation of the contract

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

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

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

APPENDIX 1

Details of the Transfer

This Appendix 1 forms part of the DPA.

Data Exporter: Customer (as defined in the DPA)

Data Importer: Juniper Networks (as defined in the DPA)

Customer Instructions: The parties agree that this DPA and the Main Agreement (including the provision of instructions via configuration tools such as the Mist dashboard, if applicable, and any APIs made available by Juniper Networks) constitute Customer's documented instructions regarding Juniper Networks' processing of data of Customer ("Customer Data") (hereinafter "Documented Instructions"). Juniper Networks will process Customer Data in accordance with Documented Instructions. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between Juniper Networks andCustomer.

Data subjects: The personal data transferred concern the following categories of data subjects:

- Personnel of Customer.
- Personnel of Customer's partners (including any vendors, suppliers, agents or additional subprocessors as may be authorized by Customer).
- 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 Customer.

Categories of data: 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 Juniper Privacy Policy ("**Privacy Notice**") available at https://www.juniper.net/us/en/privacy-policy/ together with any Supplemental Privacy Information referenced therein (including for Mist Systems); and (c) in any data sheets or related product documentation provided by Juniper Networks to Customer for the particular product or service:

- 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 Juniper products or services that include Cloud services, the categories of data that may be processed are as set forth in the Juniper Privacy Notice available at https://www.juniper.net/us/en/privacy-policy/ together with any Supplemental Privacy Information referenced therein, as well as in any data sheets or related product documentation provided by Juniper Networks to Customer for the particular product or service.
  - WLAN: For WLAN products or services of Juniper Networks, such as from Juniper affiliate Mist Systems, Inc., the categories of data that may be processed are as set forth in the Juniper Privacy Notice available at https://www.juniper.net/us/en/privacy-policy/ together with any Supplemental Privacy Information referenced therein (including for Mist Systems), as well as in any data sheets or related product documentation provided by Juniper Networks to Customer for the particular product or service.
  - 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 Data Importer's Privacy Policy, which is available at https://www.juniper.net/us/en/privacy-policy/.

Special categories of data (if appropriate): The personal data transferred concern the following special categories of data:
Juniper Networks does not require any special categories of data in order to provide the Juniper 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.

Processing operations: The personal data transferred will be subject to the following basic processing activities:

Providing the Juniper Products and Services covered by 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 Data Importer's Privacy Notice.

Location(s) for processing: Unless otherwise agreed in writing by the parties or specified in the Main Agreement, Data Importers may process the personal data anywhere in the world.

APPENDIX 2
Technical and Organisational Measures

This Appendix 2 forms part of the DPA.

Data Exporter agrees that the terms set forth in this Appendix 2 are appropriate Technical and Organizational Measures to protect Data Exporter's personal data.

Description of the technical and organisational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

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, the Processor shall implement the following technical and organizational measures to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons. In assessing the appropriate level of security the Controller and the Processor took account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

1. Information Security Governance

- The information security function within Processor reports directly to a company executive.
- A Security and Privacy Steering Committee made up of representatives from the business, 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 maintained.
- 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.

3. Encryption

- Full disk encryption is configured on laptops.
- Sensitive personal data is encrypted in transit.

4. Confidentiality of the processing systems and of the services

- Data processing systems and personal data are subject to measures designed to prevent access, loss or use without authorization.
- Personal data are subject to measures designed to prevent them from being read, copied, modified or removed without authorization during electronic transmission or transport.
- Employees or contractors with access to personal data are assigned unique IDs.
- Only authorized staff may grant, modify or revoke access.
- Access rights are assigned using a least privilege approach.
- Access is revoked upon termination of the employee or contractor.

5. Physical Security

- Physical access to Processor buildings is restricted.
- Physical access controls, such as surveillance cameras and identification badges, are implemented for data centers.

6. Integrity and availability of the processing systems and of the services

- Anti-malware and anti-virus software are in place.
- Audit logging is implemented in production system

7. Ability to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident

- 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.

8. Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures

- Vulnerability scans 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.

9. Training and Information Security Review

- Background checks are required on personnel with network or facilities access, to the extent permitted under applicable law.
- Employees are required to undergo periodic privacy and information security training.
- Subprocessors undergo a vendor information security review as appropriate based on their personal data access and are required to comply with vendor security requirements.

10. 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 or services offered and the type of personal data of Data Exporter that is Processed by Data Importer.

APPENDIX 3
Additional Provisions

This Appendix 3 forms part of the DPA.

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

1.1 "Clauses" shall mean all provisions of this DPA, unless provided otherwise in the relevant context;

1.2 "Data Exporter" shall mean the Data Exporter regardless of its location, whether within or outside the EU/EEA;

1.3 "Data Importer" shall mean any Data Importers under the DPA regardless of their location, whether within or outside the EU/EEA;

1.4 "Data Protection Requirements" shall mean any laws or regulations regarding the processing of personal data or personal information (or similar term under the applicable law or regulation), where "processing" means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated 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; and

1.5 "Member State" shall mean any country, within or outside the EU/EEA.

Any other terms that are capitalized but not defined below, shall have the meaning as defined in the Main Agreement.

2. **General provisions**

2.1. Order of precedence. If and to the extent there should be contradictions or inconsistencies between this Appendix 3 and the remainder of the DPA, this Appendix 3 shall prevail, unless and to the extent the relevant DPA provision is required under applicable Data Protection Requirements.

2.2. Non-applicability of certain Clauses. Clauses 3, 4 (i), 5(i), 6, 7, 11 of the standard contractual clauses set forth above in this DPA shall not apply to the parties, unless and solely to the extent that (a) the Data Importer processes personal data of residents of the EU/EEA pursuant to the Main Agreement and the Data Importer is located outside the EU/EEA or (b) any of such Clauses is required by applicable Data Protection Law.

2.3. Fulfillment of obligations of Data Importers under Clause 5(j). Data Exporter herewith instructs any additional Data Importers (if any) to send any information or documentation in connection with the fulfillment of Data Importers' obligations under Clause 5(j) exclusively to Juniper Networks.

2.4. Bundling of Data Importers for efficiency purposes. The parties agree that the bundling of the Data Importers 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 Data Exporter and the Data Importer and (ii) shall not create any legal or other relationship whatsoever between the "bundled" Data Importers. The Data Exporter authorizes Juniper Networks to exercise the Data Exporter's contractual rights and powers (i.e., the rights and powers ensuing from this DPA) and the Data Exporter's statutory privacy law-related rights and powers (i.e., the rights and powers ensuing from the Data Exporter's position as data controller) vis-à-vis the other Data Importers (for the avoidance of doubt, the Data Exporter shall remain entitled to exercise these rights and powers in its own name at any time).

2.5. Bundling of Data Exporters. The parties agree that the bundling of Data Exporters, for example, if Data Exporter 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 Data Exporter and the Data Importer solely for 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" Data Exporters; (iii) does not create any additional rights or remedies for such bundled Data Exporters; (iv) all processing instructions must be provided by the Data Exporter that is signatory to the Main Agreement and Data Importer is not responsible for consolidating or evaluating the validity of instructions received from bundled Data Exporters; (v) any commercial terms not provided by the DPA are provided by the Main Agreement regardless of whether the bundled Data Exporters signed or were consulted regarding the terms of the Main Agreement; and (vi) any audits conducted in accordance with the DPA shall be conducted by and through the Data Importer that is signatory to the Main Agreement.

2.6. **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. The Data Exporter as data controller hereby warrants that it has provided all required notices and obtained all permissions or, if applicable and sufficient under applicable Data Protection Requirements, another valid legal basis, required under applicable Data Protection Requirements to provide the Data Importers with any personal data of the data subjects specified in Appendix 1 to this DPA or otherwise provided by the Data Exporter in connection with the Juniper Products and Services.

2.7. **Data secrecy and confidentiality**. The Data Importer and the Data Exporter shall treat the personal data processed as confidential and shall in particular not disclose the personal data processed to any third parties unless authorized by the Data Exporter. This obligation continues to apply after the expiration or termination of this DPA. In accordance with applicable law the Data Importer shall put procedures in place designed to ensure that all persons acting under its authority entrusted with the processing of personal data (i) have committed themselves to keep personal data confidential and not to use such personal data for any other purposes except for the provision of the Juniper Products and Services hereunder, or (ii) are under an appropriate statutory obligation of confidentiality. This obligation to confidentiality shall continue after the end of the respective engagement of such person. The Data Importer will further instruct such persons regarding the applicable statutory provisions on data protection and shall ensure that access to the personal data is limited to those persons with a need to know.

2.8. **Subcontracting Authorization.** When subcontracting the Juniper Products and Services or parts thereof, Data Importer will comply with requirements set forth in Clause 11 of the Standard Contractual Clauses for Processors and in Art. 28 (2) and (4) GDPR, to the extent that such requirements are applicable to the processing to be done under such subcontract. Data Importer is entitled to use subcontractors for the performance of its services hereunder in accordance with the Clause 11 of the Standard Contractual Clauses for Processors and in Art. 28 (2) and (4) GDPR. A list of subcontractors of Data Importer is available at https://support.juniper.net/support/subprocessor/index.page ("**Subcontractor List**"). Data Exporter specifically authorizes the engagement of such subcontractors, and generally authorizes Data Importer's engagement of additional subcontractors and Data Importer's replacement of any subcontractors identified on the Subcontractor List. In addition to any notifications provided by Data Importer regarding the addition or replacement of subcontractors or updates to the Subcontractor List, Data Exporter agrees to subscribe to any mechanisms that Data Importer may provide for notifications regarding subcontractors. Data Exporter agrees to 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 subcontractor does not or cannot comply with this DPA or Data Protection Requirements (as defined above)and identify the reasonable data protection basis for the objection ("**Objection**"), so that Data Importer can evaluate the Objection and determine the appropriate action. In the event of an Objection, Data Exporter and Data Importer will work together in good faith to find a mutually acceptable resolution to address such Objection, including but not limited to reviewing additional documentation supporting the subcontractor's compliance with the DPA or Data Protection Requirements.

2.9. **Notification obligation in cases of non-compliance or a security breach.** The Data Importer will provide the Data Exporter promptly with a data breach notification if the Data Importer becomes aware of any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data of Customer or any other security incident that compromises the security, confidentiality or integrity of personal data that requires a data breach notification of the Data Exporter according to applicable law. Taking into account the nature of processing and the information available to the Data Importer, the Data Importer shall provide assistance to the Data Exporter to deal with the security breach and to comply with the obligations under applicable law and any orders of competent regulators without undue delay. Data Exporter and Data Importer shall work together in good faith within the timeframes for Data Exporter 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. Data Importer's prior written approval shall be required for any statements regarding, or references to, Data Importer made by Data Exporter in any such notifications.

2.10. **Handling of complaints, inquiries and orders.** The Data Importer shall notify the Data Exporter of data subjects' 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 applicable law) received by Data Importer relating to the Juniper Products and Services covered by the Main Agreement and, at Data Exporter's expense, shall provide assistance to the Data Exporter to respond to such complaints or inquiries in a timely manner. Taking into account the nature of the processing, the Data Importer shall assist the Data Exporter by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Exporter's obligations to respond to requests for exercising the data subject's rights under applicable law. The Data Importer shall not independently respond to such complaints, requests and orders without Data Exporter's prior approval, except where required by applicable law. The same shall apply to orders and inquires of courts or regulators. Data Importer will instruct data subjects that do not identify a relevant data controller to contact the correct data controller.

2.11. **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.

2.12. **Return and further use of data after end of contract**. After the end of the provision of the Services and pursuant to written instructions provided by the Data Exporter, the Data Importer shall return to the Data Exporter or, in Data Importer's discretion, securely destroy, without undue delay, all data on physical media received from the Data Exporter and all personal data processed on behalf of Data Exporter in Data Importer's role as a processor in connection with the Services, including relevant copies, in whatever format, and shall refrain from any further processing and use of such personal data, to the extent this is possible without infringing the Data Importer's own obligations under applicable laws, regulations, or contracts, or for Data Importer to protect its own legal rights. Upon Data Exporter's written request, Data Importer shall provide Data Exporter with a written statement confirming it acted as per the above.

2.13. **Invalidity and/or unenforceability.** Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or - should this not be possible - (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

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

2.15. **Corporate Restructuring**. Data Importer may share and disclose personal data of data subjects (as defined in Appendix 1) and other data of Data Exporter 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 Data Importer's business by or to another company, including the transfer of contact information and data of customers, partners and end users.

3. Additional Local Law Provisions

3.1. **Amendments for Data Exporters subject to the General Data Protection Regulation.** The following amendments shall apply to the extent required by Data Protection Requirements applicable to the personal data processed by Data Importer for Data Exporter pursuant to the Main Agreement:

3.1.1. **Scope of Processing**: the Data Importer will process the personal data only on behalf of the Data Exporter and a Customer of Data Exporter in compliance with the Data Exporter's instructions and this DPA, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the Data Importer is subject; in such a case, the Data Importer shall inform the Data Exporter of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.1.2. **Duration of Processing**: The commissioned data processing operations hereunder may be performed for an indefinite term for as long as the Main Agreement exists and is in effect and force.

3.1.3. **Instructions**: The Data Exporter is entitled to instruct the Data Importer in connection with commissioned data processing operations generally or in the individual case. Instructions shall be given in writing or in electronic form through an approved process and means specified by Data Importer. The Data Importer shall notify the Data Exporter without undue delay if it holds that an instruction violates applicable laws. Upon providing such notification, the Data Importer shall not be obliged to follow the instruction, unless and until the Data Exporter has confirmed or changedit.

3.1.4. **Self-monitoring**: The Data Importer shall monitor, by appropriate means, its own compliance with its data protection obligations in connection with the commissioned data processing operations and, upon written request, shall provide the Data Exporter with periodic and occasion-based reports regarding such controls.

3.1.5. **Monitoring by the Data Exporter**:

3.1.5.1. The Data Importer shall make available to the Data Exporter all information reasonably necessary to demonstrate compliance with the obligations laid down in this DPA. The Data Exporter shall have the right to monitor, by appropriate means, the Data Importer's compliance with its data protection obligations annually and at any time occasion-based, such controls being limited to information and data processing systems that are relevant to the Juniper Products and Services provided under the Main Agreement. For these purposes, the Data Exporter shall also have the right to carry out on-site audits (no more than once per year), conducted by the Data Exporter or another auditor mandated by the Data Exporter, during regular business hours without disrupting the Data Importer's business operations and in accordance with the Data Importer's security policies, and after a reasonable prior notice. The Data Importer shall tolerate such audits and shall render all necessary support.

3.1.5.2. Any third party engaged by Data Exporter to conduct an audit must be pre-approved by Data Importer (such approval not to be unreasonably withheld) and sign Data Importer's confidentiality agreement. Data Exporter must provide Data Importer with a proposed audit plan at least two weeks in advance of the audit, after which Data Exporter and Data Importer shall discuss in good faith and finalize the audit plan prior to commencement of audit activities. The Data Exporter shall reimburse Data Importer for any costs or expenses incurred by Data Importer in granting access to its data processing facilities or procuring access to its subcontractors' data processing facilities. Information obtained or results produced in connection with an audit are Data Importer confidential information and may only be used by Data Exporter to confirm compliance with this DPA and complying with its obligations under Data Protection Requirements.

3.1.6. **Assistance with privacy impact assessment**: If so requested by the Data Exporter, the Data Importer shall provide, at Data Exporter's expense, required assistance to the Data Exporter in ensuring its compliance relating to data protection impact assessments and prior consultation with the supervisory authorities, taking into account the nature of the processing and the information available to the Data Importer.

3.2. Amendments for Data Exporters located outside of the EU/EEA or personal data from data subjects outside the EU/EEA.

In case the personal data processed by Data Importer pursuant to the Main Agreement includes personal data of data subjects outside the EU/EEA, the local Data Protection Requirements applicable to such personal data provided by Data Exporter related to such data subjects applies and prevails in case of, and solely to the extent of, a conflict with this DPA.

3.3. Amendments for Additional Local Data Protection Requirements.

To the extent that additional country-specific (or state-specific, or regional, provincial, or other geographic area specific) provisions are required under applicable Data Protection Requirements, such as data export provisions or data localization provisions, the parties agree to incorporate such provisions solely to the extent they are required and solely to the extent they are applicable to particular personal data processed by Data Importer. Data Importer may, from time to time, post updated provisions related to local or other specific Data Protection Requirements on the Juniper Privacy Policy available at https://www.juniper.net/us/en/privacy-policy/, such as in the "Supplemental Privacy Information" section. Such posted provisions are automatically incorporated herein solely to the extent they are required under applicable Data Protection Requirements.

3.4. California Consumer Privacy Act ("CCPA") Confirmation

Generally, Data Importer processes data as a service provider for customers and resellers, many of which are organizations who have the direct relationship with individual end users using the Juniper Products and Services. This means that, in addition to other exceptions under the CCPA that may apply (including for employees, contractors and business contacts), Data Importer's processing of data as a service provider may not involve a sale of personal information of a consumer. Data Importer's CCPA Confirmation for Customers and Partners is available at https://www.juniper.net/assets/us/en/local/pdf/executive-briefs/9020011-en.pdf