Customer Data Processing Addendum

This Data Processing Agreement, including its Addenda and Appendices, ("**DPA**") is incorporated into and forms part of the Agreement between Customer and (a) Palo Alto Networks, Inc. and its Affiliates, 3000 Tannery Way, Santa Clara, California 95054, United States, if you are located in North or Latin America or (b) Palo Alto Networks (Netherlands) B.V. and its Affiliates, Oval Towner, De Entree 99-197, 5th Floor, 1101 He Amsterdam, if you are located outside of North or Latin America ("**Palo Alto Networks**").

Palo Alto Networks and Customer may also be referred to individually as a "Party" or collectively as the "Parties" throughout this DPA.

1. SCOPE

This DPA between Customer, (which, if applicable, shall be read throughout to include Customer's Affiliates), and Palo Alto Networks and contains the legal terms and conditions that apply to the Processing of Personal Information, by any of the Products.

2. DEFINITIONS

2.1 "**Affiliate**" means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where "Control" means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

2.2 "**Agreement**" means any underlying Palo Alto Networks' End User Agreement, Master Services Agreement, Engagement Letter, Statements of Work ("SOW"), or other legally entered and binding written agreement entered into between Palo Alto Networks and Customer that governs the provision of the Products by Palo Alto Networks.

2.3 "**Data Protection Laws**" means data protection laws applicable to Palo Alto Networks in its Processing of Personal Information under this DPA and the Agreement.

2.4 "**Process**", "**Processes**", "**Processing**", and "**Processed**" means any operation or set of operations performed upon Personal Information, whether or not by automatic means.

2.5 "**Products**" means, collectively, hardware, software, subscriptions, services, or any component or combination thereof, provided to Customer by Palo Alto Networks as described in the Agreement.

2.6 **"Personal Information"** means any information Processed during the provision of a Product that (i) relates to an identified or identifiable natural person; or (ii) is defined as "personally identifiable information", "personal information", "personal data" or similar terms, as such terms are defined under Data Protection Laws, including as may be used in this DPA.

2.7 **"Security Incident"** means any unauthorized access to Customer Personal Information stored on Palo Alto Networks' equipment or in Palo Alto Networks' facilities, or unauthorized access to such equipment or facilities, resulting in loss, disclosure, or alteration of Customer Personal Information that compromises the privacy, security or confidentiality of such Customer Personal Information.

2.8 **"Statement of Work"** or **"SOW"** shall include any form of statement of work, purchase order, or documentation of specific terms regarding the provision of a Product.

2.9 "**Sub-processor**" means any entity engaged by Palo Alto Networks to assist in fulfilling its obligations with respect to providing the Products pursuant to the Agreement or this DPA, insofar as such an entity Processes Personal Information on behalf of Palo Alto Networks. Sub-processors may include subcontractors that are specified in an applicable SOW.

3. PROCESSING PERSONAL DATA

3.1 **Customer Instructions**. Except as otherwise stated in this DPA or the Agreement, Palo Alto Networks will Process Customer Personal Information only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions and applicable Data Protection Laws, except as necessary to comply with applicable law or a binding order of a governmental body. The Parties agree that this DPA, including all applicable Addenda, and the Agreement, and any Product configurations or instructions made by the Customer, set out the Customer's instructions to Palo Alto Networks in relation to the Processing of Customer Personal Information by Palo Alto Networks. Additional Processing outside the scope of these instructions (if any) will require prior written agreement between Customer and Palo Alto Networks. Palo Alto Networks shall immediately inform Customer if, in its opinion, Customer's instruction violates applicable Data Protection Laws.

3.2 Sub-processing

3.2.1 *Authorized Sub-processors*. Palo Alto Networks may engage Sub-processors to Process Customer Personal Information on Customer's behalf.

3.2.2 *Sub-processor Obligations*. Palo Alto Networks will: (i) enter into a written agreement with any Sub-processor that imposes data protection terms that require the Sub-processor to protect the Customer Personal Information that is no less protective than this DPA; and (ii) remain responsible for its compliance with the obligations of this DPA and for any failure by the Sub-processor to fulfil its data protection obligations under applicable Data Protection Laws.

3.3 Details of Data Processing

3.3.1 *Subject Matter*: The subject matter of the Processing under this DPA is Customer Personal Information.

3.3.2 *Duration*: Palo Alto Networks may Process Customer Personal Information under this DPA until the termination or expiration of the Agreement.

3.3.3 *Purpose*: The purpose of the Processing of Customer Personal Information under this DPA is to enable Palo Alto Networks to deliver the Products and perform its obligations as set forth in the Agreement (including this DPA) or as otherwise agreed by the Parties in mutually executed written form.

3.3.4 *Nature of the Processing*: To provide Products as described in the Agreement, Palo Alto Networks will Process Customer Personal Information upon the instruction of Customer and in accordance with the terms of this DPA, including all applicable Addenda, and the Agreement.

3.3.5 *Categories of Data Subjects*: Customer determines the categories and extent of any Customer Personal Information that it discloses to Palo Alto Networks, which may include without limitation Customer Personal Information relating to the following categories of data subjects:

(a) Employees, contractors, consultants, and individuals belonging to Customer, or Customer's clients' and partners' workforce; or

(b) Other individuals whose Personal Information is Processed as part of the provision of the Products.

3.3.6 *Categories of Personal Information*: Customer determines the categories of any Personal Information that it discloses to Palo Alto Networks, which may include without limitation Customer Personal Information relating to the following categories:

(a) Identification and contact data (e.g., name, address, phone number, title, email, other contact details);

(b) Employment details (e.g., job title, role, manager);

(c) IT information (e.g., entitlements, IP addresses, usage data, cookies data, online identifiers);

(d) Domain and device information (e.g., MAC address, hostnames, International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI), and qualified hostnames);

(e) Information contained in logs related to security events identified and captured by Products; and/or

(f) Unstructured data provided to Palo Alto Networks for the purpose of providing support services (e.g., packet capture (PCAP) for file testing).

3.3.7 *Sensitive data transferred (if applicable)*: When Processing Personal Information, primarily with forensic investigations Product of which the purpose is to identify the underlying data, Palo Alto Networks may process sensitive Personal Information. The nature and scope of the sensitive data that is transferred may not be known until after the Processing has taken place and may include: Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

3.3.8 *Frequency*: The transfer of information between the Parties to facilitate Palo Alto Networks' Processing on behalf of Customer will occur as needed until the termination of the Agreement.

4. SECURITY

4.1 **Security Measures**. Taking into account the nature of the Processing, Palo Alto Networks shall implement and maintain reasonable technical and organizational security measures to protect Customer Personal Information from Security Incidents and to preserve the security and confidentiality of the Customer Personal Information, in accordance with Palo Alto Networks' security standards described in Annex A, as applicable to the Services ("Security Measures"). These Security Measures are available at: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/information-security-measures.pdf.

4.2 **Updates to Security Measures**. Customer acknowledges that the Security Measures are subject to technical progress and development and that Palo Alto Networks may update or modify the Security Measures from time-to-time provided that such updates and modifications do not result in a material degradation of the overall security of the Products.

4.3 **Customer Responsibilities**. Customer is responsible for secure and appropriate use of the Products, including making appropriate use of the Products to ensure a level of security appropriate to the risk in respect of the Customer Personal Information; and.

4.4 **Customer's Security Assessment**. Customer is responsible for reviewing the Security Measures and evaluating for itself whether the Products and the Security Measures and Palo Alto Networks' commitments under this Section will meet Customer's needs, including with respect to any obligations of Customer under Data Protection Laws as applicable.

4.5 **Security Reports and Audits**

4.5.1 Upon written request, but no more than once every 12 months, Palo Alto Networks shall provide to Customer (on a confidential basis) a summary copy of any third-party audit report(s) or self certifications in accordance with the SOC2 Type II standards or a reasonable equivalent that is applicable to the data centers, systems, and computing environments used to Process Personal Information ("Report"), so that Customer can verify Palo Alto Networks' compliance with this DPA, the audit standards against which it has been assessed, and the standards specified in the Palo Alto Networks Security Measures.

4.5.2 If Customer reasonably believes that the Report provided is insufficient to demonstrate compliance with this DPA, Palo Alto Networks shall provide written responses (on a confidential basis) to reasonable requests for information made by Customer related to its Processing of Customer Personal Information, including responses to information security and audit questionnaires that are necessary to confirm Palo Alto Networks' compliance with this DPA, provided that Customer shall not exercise this right more than once every 12 months. Any such audit will be at Customer's expense, with reasonable advance notice, conducted during normal business hours no more than once every 12 months and subject to Palo Alto Networks' reasonable security and confidentiality requirements and provided that the exercise of rights under this Section would not infringe Data Protection Laws.

4.5.3 If Customer reasonably believes that the information provided pursuant to Sections 4.5.1 and/or 4.5.2 is insufficient to demonstrate compliance with this DPA, Customer (or auditors appointed by Customer and reasonably acceptable to Palo Alto Networks) may audit Palo Alto Networks in relation to its Processing of Customer Personal Information. The scope of any such audit will be mutually agreed upon to be relevant to Customer Personal Information. Audits will be at Customer's expense, with reasonable advance notice, conducted during normal business hours no more than once every 12 months and subject to Palo Alto Networks' reasonable security and confidentiality requirements and provided that the exercise of rights under this Section would not infringe Data Protection Laws.

4.6 **Additional Security**

4.6.1 *Confidentiality of Processing*. Palo Alto Networks shall ensure that any person who is authorized by Palo Alto Networks to Process Customer Personal Information (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.6.2 *Security Incident Response*. Upon confirming that a Security Incident, Palo Alto Networks shall: (i) taking into account the nature of Palo Alto Networks' Processing of Customer Personal Information and the information available to Palo Alto Networks, notify Customer without undue delay of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

4.7 **Notification**. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incidents. Unless otherwise required under Data Protection Laws, the Parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected data subjects and/or notices to the relevant supervisory authorities.

5. RELATIONSHIP WITH THE AGREEMENT

5.1 If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Information.

5.2 Any claims against Palo Alto Networks or its Affiliates under this DPA shall only be brought by the Customer entity that is a party to the Agreement against the Palo Alto Networks entity that is a party to the Agreement.

5.3 Notwithstanding any choice of law determinations applicable to specific jurisdictions that are present in the Addenda, this DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

6. JURISDICTION-SPECIFIC ADDENDA

6.1 Attached to this DPA are Addenda that provide terms specific to the Processing of Customer Personal Information arising out of specific legal requirements from particular jurisdictions. In the event that Customer Personal Information is Processed in one or more of these jurisdictions, and the applicable requirements are not already covered in this DPA, the terms in the respective Addendum shall apply and supplement this DPA.

6.2 In the event of a conflict between the Agreement or this DPA and an Addendum, the Addendum applicable to Customer Personal Information from the relevant jurisdiction shall prevail with respect to Customer Personal Information from that relevant jurisdiction, but solely with regard to the portion of the provision in conflict.

6.3 The Customer shall be solely responsible for informing Palo Alto Networks that Customer Personal Information is within the scope of one or more Addenda.

7. UPDATES TO DPA

7.1 In the event of changes to Applicable Data Protection Laws, including, but not limited to, the amendment, revision, or introduction of new laws, regulations, or other legally binding requirements to which either

party is subject, the Parties agree to revisit the terms of this DPA, and negotiate any appropriate or necessary updates in good faith, including the addition, amendment, or replacement of any Addenda.

7.2 In the event that Palo Alto Networks is required to agree to additional terms under new legal requirements, Palo Alto Networks will post the applicable terms on its website as part of an updated DPA at least 15 days in advance of the effective date of the legal requirement. Customer will be notified of this posting, and from the date of notification will have 15 days to pose any reasonably made objections. In the event that Customer makes a reasonable objection, Palo Alto Networks agrees to work with Customer to resolve the objection, but solely in relation to the Agreement with Customer. If it is not reasonably possible to post such new terms 15 days in advance of the effective date of the legal requirement Palo Alto Networks will still afford 15 days' notice to Customer, and any changes instituted following a reasonably made objection will be treated as applicable as of the effective date of the legal requirement or the date of the Agreement, whichever is later.

8. **COMPLIANCE WITH LAWS.** The Parties shall Process Personal Information in accordance with Data Protection Laws. Customer represents and warrants that (i) it complies and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its use of the Products, provision of any instructions to Palo Alto Networks, transfer of any data to Palo Alto Networks, including any technical, personal or sensitive data, its electronic communications, and its authorization for Palo Alto Networks' access to and use of any data, including any Customer Personal Information; and (ii) it has provided, and will continue to provide, all legally required notice and has and will continue to obtain, all consents and rights necessary for the accuracy, quality, and legality of Customer Personal Information and the means by which Customer acquired said Personal Information.

9. **LIMITATION OF LIABILITY.** The liability of each party and each party's Affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement and shall not be modified by this DPA. Any claims brought by a party or its Affiliates under this DPA, whether in contract, tort or under any other theory of liability, shall be subject to the exclusions and limitations set forth in the Agreement.

CALIFORNIA CONSUMER PRIVACY ACT ADDENDUM

1. **Scope**

This Addendum shall apply in the event that Palo Alto Networks Processes Customer Personal Information of California Residents. If there is any conflict between this Addendum and the Agreement, this Addendum shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Information under the CCPA.

2. **Definitions**

2.1 The California Consumer Privacy Act of 2018 ("CCPA") is Cal. Civ. Code § 1798.100, et seq., as may be amended or superseded from time-to-time, and any accompanying legally binding regulations that are promulgated to address provisions in the law.

2.2 All words or phrases used herein not defined in the DPA will have the meaning assigned to them in the CCPA.

3. **Terms**

3.1 Palo Alto Networks will not sell any Customer Personal Information received from Customer.

3.2 Palo Alto Networks will not disclose Customer Personal Information to another business, person, or third party, except for the purpose of maintaining or providing the Products specified in the Agreement, including to provide Personal Information to authorized persons, entities, advisers, or Sub-processors as described below, or to the extent such disclosure is required by law. Notwithstanding the foregoing, nothing in this Agreement shall restrict Palo Alto Network's ability to disclose Customer Personal Information to comply with applicable law.

3.3 Palo Alto Networks certifies that it understands and will comply with the requirements enumerated in Sections 3.1 and 3.2.

3.4 For the avoidance of doubt, Customer does not provide Personal Information to Palo Alto Networks for any valuable consideration.

3.5 For the avoidance of doubt, all permitted uses of Personal Information by service providers that are enumerated in the CCPA are understood to apply to the Personal Information Processed by Palo Alto Networks.

4. **Cooperation**

4.1 Taking into account the nature of the Processing, Palo Alto Networks shall provide reasonable cooperation to assist Customer with responding to any requests from data subjects in relation to their data subject rights under the CCPA. In the event that any request from data subjects is made directly to Palo Alto Networks, Palo Alto Networks shall not respond to such communication directly other than to inform the requestor that Palo Alto Networks is not authorized to directly respond to a request, and recommend the requestor submit the request directly to Customer.

EUROPEAN ECONOMIC AREA ADDENDUM

1. **Scope**

This Addendum shall apply in the event that: (i) Palo Alto Networks Processes Customer Personal Information on the behalf of Customer as a Data Processor in the course of providing Products pursuant to the Agreement; and (ii) Customer is subject to European Data Protection Law and acts as a Data Controller thereunder.

2. **Definitions**

2.1 **"EEA"** means, for the purposes of this DPA, the European Economic Area.

2.2 **"European Data Protection Law"** means: the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR") as implemented by countries within the EEA and/or other laws that are similar, equivalent to, or successors to the GDPR.

2.3 **"Model Clauses"** means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

2.4 All terms used herein not defined in the DPA will have the meaning assigned to them in the applicable European Data Protection Law. All references to Data Protection Law or laws in the DPA shall be read in the context of EU or Member State Law for the purpose of this Addendum

3. **Cooperation**

3.1 If a law enforcement agency sends Palo Alto Networks a demand for Customer Personal Information (e.g., a subpoena or court order) relating to a EU data subject ("Data Subject Personal Information"), Palo Alto Networks will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Palo Alto Networks may provide Customer's contact information to the law enforcement agency. If compelled to disclose Data Subject Personal Information to a law enforcement agency, then Palo Alto Networks will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Palo Alto Networks is legally permitted to do so.

3.2 In the event that any request from data subjects or applicable regulatory authorities that is related to Data Subject Personal Information is made directly to Palo Alto Networks, Palo Alto Networks shall not respond to such communication directly without Customer's prior authorization other than to inform the requestor that Palo Alto Networks is not authorized to directly respond to a request, and recommend the requestor submit the request directly to Customer, unless legally compelled to reply under the law applicable to such a request. Customer shall bear the responsibility for responding to all such requests. If a law enforcement agency sends Palo Alto Networks a demand for Data Subject Personal Information (e.g., a subpoena or court order), Palo Alto Networks will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Palo Alto Networks may provide Customer's contact information to the law enforcement agency. If compelled to disclose Data Subject Personal Information to a law enforcement agency, then Palo Alto Networks will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Palo Alto Networks is legally permitted to do so.

3.3 If Palo Alto Networks is legally required to respond to a request enumerated in Sections 3.1 and 3.2, Palo Alto Networks will notify Customer and provide it with the contact information of the requesting party unless legally prohibited from doing so by applicable law.

3.4 Taking into account the nature of the Processing and information available to Palo Alto Networks, Palo Alto Networks shall provide reasonably requested information regarding the Products to enable the Customer to carry out data protection impact assessments ("DPIA"). Palo Alto Networks shall provide reasonable assistance to Customer in the cooperation or prior consultations with Supervisory Authorities or other competent regulatory authorities, which the Customer reasonably considers to be required by Data Protection Laws.

3.5 For all instances in this Section 3, should Palo Alto Networks determine in good faith that the request for assistance is unreasonable, overly burdensome, and outside of industry expectation for assistance with each respective matter, Palo Alto Networks and Customer agree to discuss in good faith a fee to be charged to Customer for the support provided outside of the reasonable level of support.

4. International Transfers

4.1 To the extent that Palo Alto Networks Processes any Customer Personal Information from the EEA and transfers such Customer Personal Information outside of the EEA to countries not deemed by the European Commission to provide an adequate level of data protection, the Parties agree to enter into and comply with the Model Clauses as discussed in Section 5 of this Addendum. Palo Alto Networks agrees that it is a "data importer" and Customer is the "data exporter" under the Model Clauses.

4.2 The Parties agree that the data export solution identified in Section 5.1 (Model Clauses) will not apply if and to the extent that Palo Alto Networks adopts an alternative data export solution for the lawful transfer of Personal Information (as recognized under European Data Protection Laws) outside of the EEA, in which event, Customer shall take any action (which may include execution of documents) strictly required to give effect to such solution and the alternative transfer mechanism will apply instead (but only to the extent such alternative transfer mechanism extends to the territories to which Customer Personal Information is transferred).

5. Model Clauses

5.1 Module Two of the Model Clauses is incorporated by reference into this Addendum.

5.2 Signatures applied to the Agreement will be taken as equally signing and effectuating the Model Clauses where applicable to underlying Personal Information Processed by Palo Alto Networks.

5.3 In respect to Clause 9(a) *Sub-processors* of Module Two of the Model Clauses:

5.3.1 Customer grants Palo Alto Networks General Written Authorization for the use of Sub-processors.

5.3.2 A list of Palo Alto Networks' Sub-processors is available on its website at https://www.PaloAltoNetworks.com/legal/sub-processors.

5.3.3 Palo Alto Networks shall maintain and make available to the Customer an up-to-date list of its Sub-processors, giving the Customer fifteen (15) days' written notice ("Review Period") of any change in Sub-processor prior to any new Sub-processor being authorized to Process any Personal Information by updating the list accordingly ("Proposed Update");

5.3.4 Customer acknowledges and agrees that it will make every effort to provide Palo Alto Networks with any objections raised by Customer during the Review Period. Objections may only be based on reasonable grounds and only with respect to data protection concerns;

5.3.5 If Customer objects to a new Sub-processor, Palo Alto Networks will then endeavor to offer alternate options for the delivery of the relevant Product that do not involve the new Sub-processor, without prejudice to any of Customer's termination rights; and

5.3.6 The Parties agree that any non-response by the Customer during the Review Period will be taken as the Customer's approval of that Request where Customer continues to use the Products after the Review Period has lapsed.

5.4 In respect to Clause 17 *Governing Law*: Option 1 is selected and the governing law is that of The Netherlands.

5.5 In respect to Clause 18 *Choice of forum and jurisdiction*: The courts of The Netherlands shall resolve any disputes arising from the Model Clauses.

5.6 If there is any conflict between this Addendum and the Model Clauses, the Model Clauses shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Information.

ANNEX I

A. List of Parties

Data exporter*:* The data exporter is the entity identified as the "Customer" in the Agreement.

Data importer*:* The data importer is the US headquartered company, Palo Alto Networks, Inc. Palo Alto Networks provides cybersecurity and forensic Products as described in the Agreement and the DPA.

B. Description of Transfer

Please see Section 3 of this DPA for a description of the data subjects, categories of data, special categories of data, and Processing operations.

C. Competent Supervisory Authority

Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer acts as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established acts as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority shall be the country from which the largest percentage of data subjects whose Personal Information is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located acts as competent supervisory authority, and shall be determined from the largest percentage of data subjects from a particular country at the first instance of Personal Information being transferred to the data importer.

ANNEX II

Description of the technical and organizational measures implemented by the data importer(s)

Technical and Organization Measures can be found at:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/information-security-measures.pdf.

UK ADDENDUM

1. **Scope**

This Addendum shall apply in the event that: (i) Palo Alto Networks Processes Customer Personal Information on the behalf of Customer as a Data Processor in the course of providing Products pursuant to the Agreement; and (ii) Customer is subject to UK Data Protection Law and acts as a Controller thereunder.

2. **Definitions**

2.1 "UK Data Protection Law" means: (i) the UK GDPR and UK Data Protection Act 2018; and/or (ii) other laws that are similar, equivalent to, successors to, or that are intended to or implement the laws that are identified in (i) above.

2.2 "Model Clauses" means Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

2.3 All terms used herein not defined in the DPA will have the meaning assigned to them in the applicable UK Data Protection Law. All references to Data Protection Law or laws in the DPA shall be read in the context of UK Law for the purpose of this Addendum.

3. **Sub-processors.**

3.1 A list of Palo Alto Networks' Sub-processors is available on its website at https://www.PaloAltoNetworks.com/legal/sub-processors.

3.2 The Parties agree that:

(a) Palo Alto Networks shall maintain and make available to the Customer an up-to-date list of its Sub-processors, giving the Customer fifteen (15) days' written notice ("Review Period") of any change in Sub-processor prior to any new Sub-processor being authorized to Process any Personal Information by updating the list accordingly ("Proposed Update");

(b) Customer acknowledges and agrees that: (a) it will make every effort to provide Palo Alto Networks with its approval of Palo Alto Networks' Proposed Update within the Review Period (such approval not to be unreasonably withheld); and (b) any objections raised by Customer during the Review Period may only be based on reasonable grounds and only with respect to data protection concerns;

(c) If Customer objects to a new Sub-processor, Palo Alto Networks will then endeavor to offer alternate options for the delivery of the relevant Product that does not involve the new Sub-processor, without prejudice to any of Customer's termination rights; and

(d) The Parties agree that any non-response by the Customer during the Review Period will be taken as the Customer's approval of that Request where Customer continues to use the Products after the Review Period has lapsed.

4. **Cooperation**

4.1 Taking into account the nature of the Processing, Palo Alto Networks shall provide reasonable cooperation to assist Customer to respond to any requests from data subjects in relation to their data subject rights under Data Protection Laws or applicable regulatory authorities relating to the Processing of Customer Personal Information under the Agreement.

4.2 If a law enforcement agency sends Palo Alto Networks a demand for Customer Personal Information (e.g., a subpoena or court order) relating to a UK data subject ("Data Subject Personal Information"), Palo Alto Networks will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Palo Alto Networks may provide Customer's contact information to the law enforcement agency. If compelled to disclose Data Subject Personal Information to a law enforcement agency, then Palo Alto Networks will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Palo Alto Networks is legally permitted to do so.

4.3 In the event that any request from data subjects or applicable regulatory authorities that is related to Data Subject Personal Information is made directly to Palo Alto Networks, Palo Alto Networks shall not respond to such communication directly without Customer's prior authorization other than to inform the requestor that Palo Alto Networks is not authorized to directly respond to a request, and recommend the requestor submit the request directly to Customer, unless legally compelled to reply under the law applicable to such a request. Customer shall bear the responsibility for responding to all such requests. If a law enforcement agency sends Palo Alto Networks a demand for Data Subject Personal Information (e.g., a subpoena or court order), Palo Alto Networks will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Palo Alto Networks may provide Customer's contact information to the law enforcement agency. If compelled to disclose Data Subject Personal Information to a law enforcement agency, then Palo Alto Networks will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Palo Alto Networks is legally permitted to do so.

4.4 If Palo Alto Networks is legally required to respond to a request enumerated in Sections 4.2 and 4.3, Palo Alto Networks will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

4.5 Taking into account the nature of the Processing and information available to Palo Alto Networks, Palo Alto Networks shall provide reasonably requested information regarding the Products to enable the Customer to carry out data protection impact assessments.

5. **International Transfers**

5.1 To the extent that Palo Alto Networks Processes any Customer Personal Information from the UK and transfers such Customer Personal Information outside of the UK to countries not deemed by the European Commission to provide an adequate level of data protection, the Parties agree to enter into and comply with the Model Clauses. Palo Alto Networks agrees that it is a "data importer" and Customer is the "data exporter" under the Model Clauses.

5.2 The Parties agree that the data export solution identified in Section 5.1 (Model Clauses) will not apply if and to the extent that Palo Alto Networks adopts an alternative data export solution for the lawful transfer of Personal Information (as recognized under European Data Protection Laws) outside of the UK, in which event, Customer shall take any action (which may include execution of documents) strictly required to give effect to such solution and the alternative transfer mechanism will apply instead (but only to the extent

such alternative transfer mechanism extends to the territories to which Customer Personal Information is transferred).

6. **Model Clauses**

6.1 The Model Clauses are incorporated by reference into this Addendum.

6.2 Signatures applied to the Agreement will be taken as equally signing and effectuating the Model Clauses where applicable to underlying Personal Information Processed by Palo Alto Networks.

6.3 The Clauses shall be governed by English law.

7. **Additional Obligations**

7.1 Upon the Customer's request, upon termination or expiration of the Agreement, Palo Alto Networks will: (a) return a copy of Personal Information to the Customer by secure file transfer in such format as is reasonably requested by the Customer; or (ii) delete and procure the deletion of copies of Personal Information. This requirement shall not apply to the extent Data Importer is required by Data Protection Law to retain all or some of the Personal Information or to Personal Information that Data Importer has archived on back-up or archival systems that cannot readily be deleted, such as due to standard deletion schedules. Data Importer shall ensure the confidentiality of such retained Personal Information and securely isolate and protect such retained Personal Information from any further Processing except to the extent required by such Data Protection Law until such time as the relevant back-up is destroyed in accordance with Data Importer's standard back-up destruction policies.

7.2 Palo Alto Networks shall ensure that persons authorized to Process the Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the Parties.

Data exporter*:* The data exporter is the entity identified as the "Customer" in the Data Processing Addendum in place between data exporter and data importer and to which these Clauses are appended.

Data importer*:* The data importer is Palo Alto Networks, Inc. Palo Alto Networks provides cybersecurity Products as described in the Agreement and the DPA.

Description of Data Processing: Please see Section 3 of this DPA for a description of the data subjects, categories of data, special categories of data and Processing operations.

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organizational measures implemented by the data importer(s)

Technical and Organization Measures can be found at:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/information-security-measures.pdf.

SWITZERLAND ADDENDUM

1. **Scope**

1.1 This Addendum shall apply in the event that: (i) Palo Alto Networks Processes Customer Personal Information on the behalf of Customer as a Data Processor in the course of providing Products pursuant to the Agreement; and (ii) Customer is subject to Swiss Data Protection Law.

1.2 This Addendum applies to and is a part of the Model Clauses found in the European Economic Area Addendum ("Clauses").

2. Terms

2.1 The Parties agree that the following provisions shall apply with respect to data transfers that are governed by the Federal Act on Data Protection ("FADP"), e.g. personal data transferred by a data exporter from Switzerland to a data importer outside of Switzerland (including personal data located in Switzerland that a data exporter makes accessible to the data importer) (the "Swiss Personal Information"):

2.1.1 The term "personal data" shall be deemed to include information relating to an identified or identifiable legal entity;

2.1.2 References to (articles in) the EU General Data Protection Regulation 2016/679 shall be deemed to refer to (respective articles in) the FADP;

2.1.3 Reference to the competent supervisory authority in Annex I(C) under Clause 13 shall be deemed to refer to the Federal Data Protection and Information Commissioner ("FDPIC");

2.1.4 References to Member State(s)/EU Member State(s) shall be deemed to include Switzerland;

2.1.5 Reference to the exporter in the EU shall be deemed to include the exporter in Switzerland;

2.1.6 Reference to the European Union Clause 8.8 of Module Two and in Annex I (A) shall be deemed to include Switzerland; and

2.1.7 Where the Clauses use terms that are defined in the EU General Data Protection Regulation 2016/679, those terms shall be deemed to have the meaning as the equivalent terms are defined in the FADP.

2.2 The list of data subjects and categories of data indicated in Annex I(B) to the Clauses shall not be deemed to restrict the application of the Clauses to the Swiss Personal Information.