CUSTOMER DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedules and Annexes ("DPA"), forms part of the Agreement (as defined below), by and between Customer and Palo Alto Networks (also referred to herein as a "Party" or collectively as the "Parties"). For the avoidance of doubt, execution of the Agreement shall constitute Customer's signature and acceptance of this DPA and its Schedules, including Annex 1 to Schedule 1 (Standard Contractual Clauses).

This DPA between Customer and Palo Alto Networks contains the legal terms and conditions that apply to the Processing of Personal Data by any of the Subscription Services. Unless otherwise specified in this DPA, the terms of the Agreement shall continue in full force and effect. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. In the event of any inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail.

1. DEFINITIONS

"**Affiliates**" means, solely for the purposes of this DPA, (i) with respect to Customer, its Affiliates as defined in the Agreement, and (ii) with respect to Palo Alto Networks, entities Controlled by, or under common Control with Palo Alto Networks that Process Personal Data under the direct authority of Palo Alto Networks in order to provide the Subscription Services, 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.

"**Agreement**" means any underlying Palo Alto Networks End User License Agreement, Master Services Agreement, Engagement Letter, Statements of Work, or other legally entered and binding written, or electronic agreement entered into between Palo Alto Networks and Customer that governs the provision of Subscription Services by Palo Alto Networks to Customer.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act, and its implementing regulations.

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

"**Data Protection Laws**" means all mandatory applicable data protection laws that apply to the Processing of Personal Data under this DPA and the Agreement.

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

"Personal Data" means electronic information submitted by or on behalf of Customer to the Subscription Service(s) 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.

"Privacy Datasheet(s)" means the applicable document located in Palo Alto Networks Trust Center, that further describes the Processing activities in relation to the Subscription Services provided to Customer under the Agreement.

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

“Processor” means the entity which Processes Personal Data on behalf of the Controller, including as applicable any “service provider” as that term is defined by the CCPA.

“**Security Incident**” means a breach of security, of which Palo Alto Networks becomes aware, leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data in Palo Alto Networks’ possession, custody, or control that compromises the security, confidentiality, or integrity of such Personal Data.

“Security Measures” means the technical and organizational measures implemented by Palo Alto Networks designed to secure Personal Data, which are included by reference in Annex II to Schedule 1 to this DPA.

“Statement of Work” or **“SOW”** shall include any form of statement of work, purchase order, or documentation of specific terms agreed between Palo Alto Networks and Customer regarding the provision of a Subscription Service.

"**Sub-processor**" means an entity engaged by Palo Alto Networks to assist in fulfilling its obligations with respect to providing the Subscription Service(s) pursuant to the Agreement or this DPA, insofar as such an entity Processes Personal Data on behalf of Palo Alto Networks. For the avoidance of doubt, Palo Alto Networks Affiliates may act as Sub-processors and Process Personal Data on behalf of Palo Alto Networks.

“Subscription Service(s)” means (i) software-as-a-service and cloud-delivered security services, including updates, provided by Palo Alto Networks to Customer, regardless of whether a fee is charged for its use; and (ii) Unit 42 services. Support services, customer success services, and focused services constitute Subscription Services under this DPA. Professional services are not considered Subscription Services under this Agreement.

“Trust Center” means the dedicated Palo Alto Networks website that provides customers with comprehensive information, resources and documentation about the company's commitment to data privacy, security, and compliance, found at https://www.paloaltonetworks.com/legal-notices/trust-center.

2. PROCESSING OF PERSONAL DATA

2.1 Scope of Processing. Palo Alto Networks will only Process Personal Data in accordance with Customer’s documented instructions, the applicable Privacy Datasheets, Data Protection Laws, and this DPA. The Parties agree that this DPA, including all applicable Schedules, the applicable Privacy Datasheets, and the Agreement set out the Customer’s instructions to Palo Alto Networks in relation to the Processing of Personal Data by Palo Alto Networks. Palo Alto Networks shall promptly inform Customer if, in its opinion, any Customer instructions infringe Data Protection Laws.

2.2 Customer Obligations. Customer shall (i) comply with all applicable laws, including Data Protection Laws, in respect of its use of the Subscription Service(s); (ii) ensure that any instructions provided to Palo Alto Networks are at all times in accordance with Data Protection Laws; (iii) collect all Personal Data in accordance with Data Protection Laws and obtain all consents and rights necessary for the Processing of Personal Data; (iv) maintain at all times the accuracy, quality, and legality of Personal Data; and (v) provide to Palo Alto Networks the minimum amount of Personal Data necessary for the provision of the

Subscription Service(s).

2.3 Confidentiality of Processing. Palo Alto Networks shall ensure that any person who is authorized by Palo Alto Networks to Process Personal Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

3. SUB-PROCESSING

3.1 As part of the provision of a Subscription Service, Palo Alto Networks may engage Sub-processors to Process Personal Data on Customer's behalf. Customer hereby grants Palo Alto Networks a general authorisation to appoint and use the Sub-processors currently listed on the "List of Subprocessors" which is available in the Trust Center.

3.2 In the event Palo Alto Networks contracts the Processing of Personal Data to a new Sub-processor, Customer will be notified via email in advance of this change, provided Customer has subscribed to receive notifications through the Palo Alto Networks Support Portal. Customer will have fifteen (15) calendar days from the date of notification to notify Palo Alto Networks of Customer's objections based on reasonable grounds and only in respect to data protection concerns ("Review Period"). In such cases, Palo Alto Networks will then endeavor to offer alternate options for the delivery of the relevant Subscription Service(s) that does not involve the new Sub-processor. The Parties agree that Customer's non-response during the Review Period will be taken as the Customer's approval of such Sub-processor.

3.3 Palo Alto Networks will: (i) enter into a written agreement with all Sub-processors that imposes data protection terms as stringent as those set forth in this DPA; and (ii) remain fully liable for the Sub-processor's compliance with the obligations of this DPA.

3.4 Palo Alto Networks may engage Sub-processors located outside the EEA or the UK. In such cases, Palo Alto Networks will implement and maintain an appropriate transfer mechanism to ensure compliance with the Data Protection Laws. This may include, as appropriate, (i) Module 3 of the Standard Contractual Clauses; (ii) an adequacy decision or equivalent issued by the European Commission or the UK Secretary of State (such as the EU-U.S. Data Privacy Framework or the UK Extension); or (iii) or any other mechanism permitted under the Data Protection Laws.

4. COOPERATION

4.1 Government requests for Personal Data. If a law enforcement, national security, or other government agency sends Palo Alto Networks a request (e.g. warrant, court order, or subpoena) to access Personal Data, Palo Alto Networks commits to following the process described here.

4.2 Data Subject requests. In the event of a Personal Data request from a Data Subject related to a Customer is made directly to Palo Alto Networks, Palo Alto Networks shall inform the requestor that Palo Alto Networks is not authorized to directly respond to the request, and recommend the requestor submit the request directly to Customer, unless legally compelled to respond under the law applicable to such a request. Customer shall bear the responsibility for responding to all such requests. In the event Customer requires support from Palo Alto Networks in responding to a request from a Data Subject, it may contact privacy@paloaltonetworks.com for assistance. To the extent legally permitted, Customer shall be responsible for any costs arising from Palo Alto Networks' assistance.

4.3 Data Protection Impact Assessments. Taking into account the nature of the Processing and information available to Palo Alto Networks, Palo Alto Networks shall provide reasonable information regarding the Subscription Service(s) to enable the Customer to carry out data protection impact assessments or similar evaluations and assessments if required by Data Protection Laws.

4.4 Supervisory/Regulatory Authorities. Palo Alto Networks shall provide reasonable assistance to Customer in the cooperation or prior consultations with supervisory authorities or other competent regulatory authorities.

5. SECURITY

5.1 Security Measures. Palo Alto Networks shall implement and maintain the Security Measures.

5.2 Customer Responsibilities. Customer is responsible for secure and appropriate use of the Subscription Service(s), to ensure a level of security appropriate to the risk in respect of the Personal Data.

5.3 Security Reports. Palo Alto Networks shall make available to Customer, upon written request and without undue delay (subject to appropriate confidentiality obligations), a summary copy of applicable third-party audit report(s) or certifications it maintains for its Subscription Service(s) (e.g. ISO 27001 or SOC2 Type II standard), so that the 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 Security Measures.

5.4 Security Incidents. Upon confirming that a Security Incident has occurred, without undue delay, Palo Alto Networks shall: (i) taking into account the nature of Palo Alto Networks Processing of Personal Data and the information available to Palo Alto Networks, notify the Customer; and (ii) promptly take such steps as Palo Alto Networks deems necessary and reasonable to contain, investigate, and mitigate the Security Incident to the extent the remediation is within Palo Alto Networks' reasonable control. Palo Alto Networks shall reasonably cooperate with Customer in any post-Security Incident communication efforts. The obligations contained herein shall not apply to Security Incidents that are caused by Customer or Customer's users.

6. DELETION AND RETENTION

On termination or expiration of the Agreement, and upon Customer's written request, Palo Alto Networks shall, without undue delay: (i) return a copy of Personal Data to the Customer by secure file transfer in such format as is reasonably requested by the Customer; or (ii) securely delete existing copies of Personal Data, unless continued retention is required and/or permitted by Data Protection Laws and/or mandatory applicable law. If Palo Alto Networks determines that continued retention is required and/or permitted by Data Protection Laws and/or mandatory applicable law, Palo Alto Networks shall ensure the confidentiality of such Personal Data and shall extend the protections of this DPA to such Personal Data.

7. 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, as permitted by applicable law.

8. JURISDICTION-SPECIFIC SCHEDULES

Attached to this DPA are Schedules that provide terms specific to the Processing of Personal Data arising out of specific legal requirements from particular jurisdictions, which shall apply to the extent Personal Data is Processed in one or more of these jurisdictions. In the event of a conflict or inconsistency between this DPA and a Schedule, the Schedule applicable to Personal Data from the relevant jurisdiction shall prevail with respect to Personal Data from that relevant jurisdiction, but solely with regard to the portion of the provision in conflict or inconsistency.

SCHEDULE 1
EUROPEAN ECONOMIC AREA

1. DEFINITIONS

1.1 **"EEA"** means the European Economic Area.

1.2 **"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” or “GDPR”), as implemented by countries within the EEA and/or other laws that are similar, equivalent to, or successors to the GDPR.

1.3 **"Standard Contractual 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.

1.4 For the purpose of this Schedule 1, all terms used herein not defined in the DPA will have the meaning assigned to them in the applicable European Data Protection Law and all references to Data Protection Law or laws in the DPA shall be read in the context of EU or Member State Law.

2. TRANSFERS OUTSIDE OF THE EEA

2.1 Module 2 (Controller to Processor) of the Standard Contractual Clauses. To the extent that Customer, as a Controller, transfers any Personal Data from the EEA for Processing directly to any Palo Alto Networks entity or Affiliate in a third country not deemed by the European Commission to provide an adequate level of data protection, Module 2 (Controller to Processor) of the Standard Contractual Clauses will apply with respect to such transfers.

2.2 Module 3 (Processor to Processor) of the Standard Contractual Clauses. To the extent Palo Alto Networks transfers Personal Data from the EEA for Processing to any Sub-processor in a third country not deemed by the European Commission to provide an adequate level of data protection, Palo Alto Networks shall ensure such transfer is supported by a valid transfer mechanism, which may include use of the Module Three (Processor-to-Processor) of the Standard Contractual Clauses.

2.3 In the event of any change in Data Protection Laws or binding legal decision by the relevant judicial authority that renders the data transfer mechanism described in Clauses 2.1 and 2.2 of this Schedule 1 invalid or insufficient to support the transfer of Personal Data, and to the extent that Palo Alto Networks adopts an available alternative data transfer solution for the lawful transfer of Personal Data outside of the EEA (as recognized under European Data Protection Laws) such as the EU-U.S. Data Privacy Framework, the Parties agree that such transfer will be made in reliance on such alternative data transfer solution. To the extent the execution of additional documents is required to give effect to such data transfer solution, the Parties shall work in good faith to execute such documentation.

3. STANDARD CONTRACTUAL CLAUSES

3.1 To the extent applicable under Clause 2.1 of this Schedule 1, Module Two (Controller to Processor) of the Standard Contractual Clauses is incorporated by reference into this Schedule 1. For clarity, Annexes

I and II of the Standard Contractual Clauses are attached to this Schedule 1. Signatures applied to the Agreement will be taken as equally signing and effectuating the Standard Contractual Clauses.

3.2 In respect to Clause 7 *Docking clause*, the option shall not apply.

3.3 In respect to Clause 9(a) *Sub-processors*, option 2 is selected and Customer grants a General Written Authorization for the use of Sub-processors listed here. All other provisions contained in Clause 3 of this Schedule 1 shall apply.

3.4 In respect to Clause 11 *Redress*, the option shall not apply.

3.5 In respect to Clause 17 *Governing Law*, option 1 is selected and the governing law is that of The Netherlands.

3.6 In respect to Clause 18 *Choice of forum and jurisdiction*, the courts of The Netherlands shall resolve any disputes arising from the Standard Contractual Clauses.

ANNEX I TO SCHEDULE 1

A. List of Parties

Data exporter*:* The data exporter is the entity identified as the Customer in the Agreement, acting as a data exporter on behalf of itself and its Affiliates.

Data importer*:* The data importer is Palo Alto Networks.

B. Description of Transfer

1. *Categories of Data Subjects whose personal data is transferred:* The Personal Data transferred may relate to the following categories of Data Subjects: Employees, contractors, consultants, individuals belonging to Customer, Customer's clients', and partners' workforce and/or other individuals whose Personal Data is Processed as part of the provision of the Subscription Service(s).

2. *Categories of personal data transferred:* The Personal Data transferred may relate to the following categories of Personal Data: 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 Subscription Service(s); and/or f) Unstructured data provided to Palo Alto Networks for the purpose of providing services (e.g., packet capture (PCAP) for file testing).

For the specific categories of Personal Data Processed on a Subscription Service per Subscription Service basis, refer to the applicable Privacy Datasheets available at the Trust Center.

3. *Sensitive data transferred (if applicable)*: When Processing Personal Data, primarily with forensic investigations Subscription Service(s) of which the purpose is to identify the underlying data, Palo Alto Networks may process sensitive Personal Data. The nature and scope of the sensitive personal data that is transferred may not be known until after the Processing has taken place and may include: Personal Data 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.

4. *The frequency of the transfer (e.g., Whether the data is transferred on a one-off or continuous basis)*: The transfer of Personal Data between the Parties will occur on a continuous basis.

5. *Nature of the Processing*: Personal Data will be subject to processing activities such as storing, recording, using, sharing, transmitting, analyzing, collecting, transferring, and making available Personal Data. Additional details regarding Palo Alto Networks' Processing activities are reflected in the applicable Privacy Datasheets, available at the Trust Center.

6. *Purpose*: The purpose of the Processing of Personal Data under this DPA is to enable Palo Alto Networks to deliver the Subscription Service(s) 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. For specific details on Palo Alto Networks purposes for Processing Personal Data under a specific Subscription Service,

please refer to the applicable Privacy Datasheets available at the Trust Center.

7. *The period for which the personal data will be retained, or if that's not possible, the criteria used to determine that period:* Palo Alto Networks will retain Personal Data to fulfill the purposes for which it was collected and as necessary to comply with business requirements, legal obligations, resolve disputes, and enforce its rights. Specific data retention periods are listed for certain Subscription Service(s) in the applicable Privacy Datasheets available at the Trust Center.

8. *For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing:* Personal Data will be transferred to Palo Alto Networks Sub-processors as described in the applicable Privacy Datasheet available at the Trust Center.

C. Competent Supervisory Authority

Competent supervisory authority/ies to be chosen in accordance with Clause 13.

ANNEX II TO SCHEDULE 1

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

Palo Alto Networks Security Measures can be found at: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/information-security-measures.pdf

SCHEDULE 2
UNITED KINGDOM

1. DEFINITIONS

1.1 **"Mandatory Clauses"** means Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s199A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

1.2 **"Standard Contractual 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.

1.3 **"UK"** means the United Kingdom.

1.4 **"UK Data Protection Law"** means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including: (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.

1.5 **"UK GDPR"** as defined in Section 3 of the Data Protection Act 2018.

1.6 For the purposes of this Schedule 2, all terms used herein not defined in the DPA will have the meaning assigned to them in the applicable UK Data Protection Law and all references to Data Protection Law or laws in the DPA shall be read in the context of UK Law.

2. TRANSFERS OUTSIDE OF THE UK

2.1 To the extent that Customer transfers any Personal Data from the UK for Processing directly to any Palo Alto Networks entity or Affiliate in countries not deemed to provide an adequate level of data protection under UK Data Protection Law, the Parties agree to enter into and comply with Module 2 of the Standard Contractual Clauses (as amended by the Mandatory Clauses) and having selected the options identified in Clauses 3.2 - 3.6 of Schedule 1 above. Palo Alto Networks agrees that it is a "data importer" and Customer is the "data exporter" under the Standard Contractual (as amended by the Mandatory Clauses).

2.2 In the event of any change in UK Data Protection Law or binding legal decision by the relevant judicial authority that renders the data transfer mechanism described in Clause 2.1 of this Schedule 2 invalid or insufficient to support the transfer of Personal Data, and to the extent that Palo Alto Networks adopts an available alternative data transfer solution for the lawful transfer of Personal Data outside of the UK (as recognized under UK Data Protection Law) such as the UK Extension to the EU-U.S. Data Privacy Framework, the Parties agree that such transfer will be made in reliance on such alternative data transfer solution. To the extent the execution of additional documents is required to give effect to such data transfer solution, the Parties shall work in good faith to execute such documentation.

3. MANDATORY CLAUSES

3.1 To the extent applicable under Clause 2.1 of this Schedule 2, Module Two (Controller to Processor) of the Standard Contractual Clauses and the Mandatory Clauses are incorporated by reference into this Schedule 2, and the Standard Contractual Clauses are amended in accordance with the Mandatory Clauses. For clarity, Annexes I and II of the Standard Contractual Clauses included in Schedule 1 are incorporated by reference to this Schedule 2. Signatures applied to the Agreement will be taken as equally signing and effectuating the Approved Addendum, including the Mandatory Clauses.

3.2 Neither the Mandatory Clauses or this Schedule 1 shall be interpreted in a way that conflicts with rights and obligations provided for under UK Data Protection Law.

3.3 Data importer may end this DPA (including this Schedule 2) to the extent the Mandatory Clauses apply, in accordance with Clause 19 of the Mandatory Clauses.

SCHEDULE 3

SWITZERLAND

1. DEFINITIONS

1.1 **“FDIP”** means the Federal Data Protection and Information Commissioner.

1.2 **“GDPR” or “General Data Protection Regulation”** means the EU General Data Protection 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.

1.3 **“Swiss FADP”** means the Swiss Federal Act of 19 June 1992 on Data Protection, the Ordinance to the Swiss Federal Act on Data Protection and the revised Swiss Federal Act of 25 September 2020 on Data Protection which comes into force in 2023.

1.4. For the purpose of this Schedule 3, all terms used herein not defined in the DPA will have the meaning assigned to them in the applicable Swiss FADP and all references to Data Protection Law or laws in the DPA shall be read in the context of the Swiss FADP.

2. TRANSFERS OUTSIDE OF SWITZERLAND

2.1 To the extent that Customer transfers any Personal Data from Switzerland for Processing directly to any Palo Alto Networks entity or Affiliate in a third country not deemed to provide an adequate level of data protection under the Swiss FADP, Module 2 (Controller to Processor) of the Standard Contractual Clauses will apply with respect to such transfers.

2.2 In the event of any change in the Swiss FADP or binding legal decision by the relevant judicial authority that renders the data transfer solution identified in Clause 2.1 of this Schedule 3 invalid or insufficient to support the transfer of Personal Data, and to the extent that Palo Alto Networks adopts an available alternative data export solution for the lawful transfer of Personal Data outside of Switzerland (as recognized under the Swiss FADP) such as the Swiss-U.S. Data Privacy Framework, the Parties agree that such transfer will be made in reliance on such alternative data transfer solution. To the extent the execution of additional documents is required to give effect to such data transfer solution, the Parties shall work in good faith to execute such documentation.

3. STANDARD CONTRACTUAL CLAUSES

3.1. To the extent applicable under Clause 2.1 of this Schedule 3, Module Two (Controller to Processor) of the Standard Contractual Clauses is incorporated by reference into this Schedule 3. Annexes I and II, as set forth in Schedule 1, shall form the Annexes to the Standard Contractual Clauses incorporated in this Schedule 3. Signatures applied to the Agreement will be taken as equally signing and effectuating the Standard Contractual Clauses.

3.2 References to General Data Protection Regulation and/ or GDPR shall be deemed to refer to the Swiss FADP.

3.3 All references to the competent supervisory authority shall be deemed to refer to the Federal Data Protection and Information Commissioner (“FDPIC).

3.4 References to the “European Union”, “Union”, “EU”, and “Member State(s)/EU Member State(s)” shall be deemed to include Switzerland and references to the exporter in the EU shall be deemed to include the exporter in Switzerland.

3.5 Where the Standard Contractual Clauses use terms that are defined in the GDPR, those terms shall be deemed to have the meaning as the equivalent terms are defined in the Swiss FADP.

3.6 In respect to Clause 17 *Governing law,* the applicable law shall be Swiss law.

3.7 In respect to Clause 18 *Choice of forum and jurisdiction,* the Swiss courts shall resolve any disputes arising from the Standard Contractual Clauses.

SCHEDULE 4
U.S. PRIVACY LAWS

1. DEFINITIONS

1.1 **"U.S. Privacy Laws"** means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the U.S., including the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act, and its implementing regulations.

1.2 For the purpose of this Schedule 4, all terms used herein not defined in this Schedule 4 will have the meaning assigned to them in the U.S. Privacy Laws, its implementing regulations or the Agreement and all references to Data Protection Law or laws in the DPA shall be read in the context of U.S. Privacy Laws.

2. COMMITMENTS UNDER U.S. PRIVACY LAWS

2.1 Palo Alto Networks agrees that:

2.1.1 It is acting solely as a "Service Provider" or "Processor" as defined under the U.S. Privacy Laws;

2.1.2 It will comply with, and provide at least the same level of privacy protection as is required under the U.S. Privacy Laws;

2.1.3 It will notify the business promptly after making the relevant determination if it determines that it can no longer meet its obligations under the U.S. Privacy Laws;

2.1.4 Customer will have the right to take reasonable and appropriate steps to (i) ensure that Palo Alto Networks uses Personal Data in a manner consistent with Customer's obligations under the U.S. Privacy Laws; and (ii) upon reasonable notice, stop and remediate the unauthorized Processing of Personal Data by Palo Alto Networks.

2.1.5 To the extent Palo Alto Networks receives Personal Data in deidentified form from the Customer or deidentifies Personal Data received from Customer such that it cannot reasonably be linked to such Personal Data, directly or indirectly ("Deidentified Data"), Palo Alto Networks will (1) take reasonable measures to ensure that the Deidentified Data cannot be associated with a consumer or household; (2) publicly commit to maintain and use the Deidentified Data in a de-identified form and not attempt to re-identify the information (except that Palo Alto Networks may attempt to re-identify the data solely for the purpose of determining whether its deidentification processes are compliant with U.S. Privacy Laws); and (3) contractually obligate any recipients of the Deidentified Data to comply with the foregoing requirements and US Privacy Laws.

2.1.6 For the avoidance of doubt, Palo Alto Networks is permitted to deidentify Personal Data through a reliable state of the art anonymization procedure and use such Deidentified Data for its own business purposes, including without limitation for security and fraud detection and research and development of new products and services, provided such Deidentified Data cannot reasonably be linked to the Personal

Data, directly or indirectly.

2.2. Except as otherwise permitted by the U.S. Privacy Laws, this DPA or the Agreement, Palo Alto Networks shall not:

2.2.1 retain, use or disclose Personal Data outside of its direct business relationship with Customer or retain, use or disclose Personal Data for any purposes other than the business purposes specified in this DPA or the Agreement;

2.2.2 combine Personal Data of consumers that Palo Alto Networks receives from, or on behalf of, Customer with Personal Data that Palo Alto Networks receives from, or on behalf of, another person or persons or collects from its own interaction with consumers; and

2.2.3 sell or share Personal Data, as those terms are defined by the U.S. Privacy Laws.