SENTINELONE DATA PROTECTION ADDENDUM

This Data Protection Addendum, including all appendices ("**DPA**") forms a part of the SentinelOne Master Subscription Agreement ("**Agreement**") between SentinelOne and the Customer. The Parties agree that this DPA sets forth their obligations with respect to the processing and security of Customer Data in connection with Customer's use of the Solutions.

1. **OVERVIEW.** This DPA applies only to the processing of Customer Data in environments controlled by SentinelOne (including SentinelOne Subprocessors), which includes Customer Data sent to SentinelOne by the Solutions but does not include data that remains on Customer's premises or in any Customer-selected third-party operating environments. This DPA will be effective on the Effective Date of the Agreement and will replace any terms previously applicable to the processing and security of Customer Data. Capitalized terms used but not defined in this DPA have the meaning given to them in the Agreement.

2. **DEFINITIONS**.

   2.1. "**Applicable Data Protection Law**" means, as applicable to the processing of Customer Data (including any personal data contained therein), any national, federal, European Union, state, provincial, or other privacy, data protection, or data security law or regulation.

   2.2. "**Customer Data**", if not defined in the Agreement, means data ingested from Customer endpoints, or otherwise provided, by or on behalf of Customer to SentinelOne via Customer's use of the Solutions, excluding System Data.

   2.3. "**Customer Personal Data**" means the personal data contained within the Customer Data, including any special categories of personal data or sensitive data defined under Applicable Privacy Law.

   2.4. "**EU GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

   2.5. "**Security Breach**" means a breach of SentinelOne's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

   2.6. "**Subprocessor**" means a third party authorized as another processor under this DPA to process Customer Data in order to provide the Solutions.

   2.7. The terms "**personal data**", "**data subject**", "**controller**", and "**processor**" as used in this DPA have the meanings given by Applicable Data Protection Law or, absent any such meaning or law, by the EU GDPR.

   2.8. The terms "**personal data**", "**data subject**", "**controller**", and "**processor**" include "**personal information**", "**consumer**", "**business**", and "**service provider**", respectively, as required by Applicable Data Protection Law.

3. **LEGAL COMPLIANCE AND JURISDICTION-SPECIFIC TERMS.**

   3.1. Roles of the Parties. SentinelOne is a processor and Customer is a controller or processor, as applicable, of Customer Data.

   3.2. Compliance with Law. Each Party will comply with its obligations related to the processing of Customer Data under Applicable Data Protection Law.

   3.3. Jurisdiction-Specific Terms. To the extent the processing of Customer Data is subject to an Applicable Data Protection Law described in Appendix 3 (Jurisdiction-Specific Data Protection Laws), the corresponding terms in Appendix 3 shall also apply. In the event of a conflict between the general terms of this DPA and Appendix 3, Appendix 3 will prevail.

4. **PROCESSING OF CUSTOMER DATA.**

4.1. Summary of the Processing. The subject matter and details of the processing of Customer Data are described in Appendix 1 (Details of Processing of Customer Data).

4.2. SentinelOne Obligation. SentinelOne shall: (a) not process Customer Data other than to provide the Solutions in accordance with this Agreement (including as set forth in this DPA and as described in Appendix 1 to this DPA) and applicable law (the "**Permitted Purpose**"); and (b) immediately notify Customer if, in SentinelOne's opinion, Applicable Data Protection Law prohibits SentinelOne from complying with the Permitted Purpose or SentinelOne is otherwise unable to comply with the Permitted Purpose.

4.3. Customer Instructions and Obligation. Customer hereby: (a) instructs SentinelOne to process Customer Data for the Permitted Purpose; (b) warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out herein on behalf of each relevant controller of Customer Data; and (c) warrants and represents that the relevant controller of Customer Data has provided all notices and obtained all consents required by Applicable Data Protection Law to provide Customer Data to SentinelOne under the Agreement.

5. SECURITY.

5.1. Security Measures. SentinelOne will implement and maintain the technical and organizational measures set forth in Appendix 2 (Security Measures) (the "**Security Measures**"). SentinelOne may update the Security Measures from time to time provided that such updates do not result in a reduction of the security of the Solutions or SentinelOne's obligations under the Agreement.

5.2. Customer's Security Responsibilities. Without prejudice to SentinelOne's obligations under Section 5.1 (Security Measures) and elsewhere in the Agreement, Customer is responsible for its use of the Solutions, including: (a) using the Solutions to ensure a level of security appropriate to the risk to Customer Data; (b) securing the authentication credentials, systems, and devices Customer uses to access the Solutions; and (c) backing up its Customer Data as appropriate.

5.3. Customer's Security Assessment. Customer agrees that the Solutions and Security Measures implemented and maintained by SentinelOne provide a level of security appropriate to the risk to Customer Data.

5.4. Confidentiality. SentinelOne shall ensure that its personnel engaged in the processing of Customer Data (a) will process such data only on instructions from Customer or as described in this DPA, and (b) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. SentinelOne shall provide periodic and mandatory data privacy and security training and awareness to its employees in accordance with Applicable Data Protection Law and industry standards.

5.5. Security Breaches.

5.5.1. Notification. SentinelOne shall notify Customer promptly and in any event within 48 hours upon becoming aware of a Security Breach, and promptly take reasonable steps to minimize harm and secure Customer Data.

5.5.2. Details of Notification. SentinelOne's notification of a Security Breach will describe: (a) the nature of the Security Breach including the Customer resources impacted; (b) the measures SentinelOne has taken, or plans to take, to address the Security Breach and mitigate its potential risk; (c) the measures, if any, SentinelOne recommends that Customer take to address the Security Breach; and (d) the details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, SentinelOne's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

5.5.3. No Acknowledgement of Fault or Liability. SentinelOne's notification of or response to a Security Breach under this Section will not be construed as an acknowledgement by SentinelOne of any fault or liability with respect to the Security Breach.

6. SUBPROCESSING

6.1. Specific Consent. Customer specifically authorizes SentinelOne to engage as Subprocessors those entities listed as of the effective date of this DPA at the URL specified in Section 6.2 (Subprocessor Details). In addition, and without prejudice to Section 6.3 (Engagement of New Subprocessors), Customer generally authorizes the engagement as Subprocessors of any other third parties (each a "**New Subprocessor**").

6.2. Subprocessor Details. Information about Subprocessors, including their functions and locations, is available at: www.sentinelone.com/legal/sentinelone-sub-processors/ (as may be updated by SentinelOne from time to time in accordance with this DPA).

6.3. Engagement of New Subprocessors. When any New Subprocessor is engaged while this DPA is in effect, SentinelOne shall provide Customer at least thirty days' prior written notice of the engagement of any New Subprocessor, including details of the processing to be undertaken by the New Subprocessor. If, within thirty days of receipt of that notice, Customer notifies SentinelOne in writing of any objections to the proposed appointment, and further provides commercially reasonable justifications to such objections based on that New Subprocessor's inability to adequately safeguard Customer Data, then: (a) SentinelOne shall work with Customer in good faith to address Customer's objections regarding the New Subprocessor; and (b) where Customer's concerns cannot be resolved within thirty days from SentinelOne's receipt of Customer's notice, notwithstanding anything in the Agreement, Customer may, by providing SentinelOne with a written notice with immediate effect, terminate the Purchase Order(s) with respect to only those aspects which cannot be provided by SentinelOne without the use of the New Subprocessor.

6.4. Subprocessor Due Diligence Requirements. With respect to each Subprocessor, SentinelOne shall: (a) before the Subprocessor first processes Customer Data, carry out adequate due diligence to ensure that the Subprocessor is capable of performing the obligations subcontracted to it in accordance with the Agreement (including this DPA); (b) periodically reassess the Subprocessor to ensure it remains capable of performing the obligations subcontracted to it in accordance with the Agreement (including this DPA); (c) ensure that the processing of Customer Data by the Subprocessor is governed by a written contract including terms no less protective of Customer Data than those set out in this DPA, including that the applicable data protection obligations in this DPA are imposed on the Subprocessor; and (d) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

7. COOPERATION.

7.1. Individual Rights. Taking into account the nature of the processing, SentinelOne shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise individuals' rights under Applicable Data Protection Law.

7.2. Individual Requests. SentinelOne shall: (a) promptly notify Customer if SentinelOne receives a request from an individual Applicable Data Protection Law with respect to Customer Data to the extent that SentinelOne recognizes the request as relating to Customer; and (b) ensure that SentinelOne does not respond to that request except on the documented instructions of Customer or as required by applicable law, in which case SentinelOne shall to the extent permitted by applicable law inform Customer of that legal requirement before SentinelOne responds to the request.

7.3. Impact Assessments and Consultation. To the extent SentinelOne is required by Applicable Data Protection Law, SentinelOne shall (taking into account the nature of the processing and the information available to SentinelOne) provide reasonable assistance to Customer with any impact assessments or consultations with data protection regulators by providing information in accordance with Section 7.4 (Audits and Records).

7.4. Audits and Records. SentinelOne shall make available to Customer upon request information necessary to demonstrate compliance with Applicable Data Protection Law and this DPA in accordance with the following procedures: (a) SentinelOne will provide Customer with the most recent certifications and/or summary audit report(s) which SentinelOne has procured to regularly test, assess, and evaluate the effectiveness of the Security Measures; (b) SentinelOne will reasonably cooperate with Customer by

providing available additional information concerning the Security Measures to help Customer better understand the Security Measures; and (c) if further information is required by Customer to comply with its own or other controller's audit obligations or a competent supervisory authority's request, Customer will inform SentinelOne and the Parties shall discuss in good faith the content and delivery of the required information.

8. DATA PROCESSING LOCATIONS.

8.1. Data Hosting Location. SentinelOne will only host Customer Data at rest in the regions offered by SentinelOne and selected by Customer on an Order Form or as Customer otherwise configured via the Solutions (the "**Hosting Location**").

8.2. Data Processing Location. Taking into account the safeguards set forth in this DPA, Customer Data may be processed in the United States or any other country in which SentinelOne or its Subprocessors operate.

9. DATA DELETION.

9.1. Deletion Upon Termination. SentinelOne shall promptly and in any event within sixty days of the date of cessation of providing any Solutions involving the processing of Customer Data (the "**Cessation Date**"), delete all copies of Customer Data, unless applicable law requires storage.

9.2. Certification of Deletion. SentinelOne shall provide written certification to Customer that it has complied with this Section within ten days of receiving Customer's written request to receive such certification.

10. GENERAL TERMS.

10.1. Interpretation. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

10.2. Liability. Any liability associated with failure to comply with this DPA will be subject to the limitations of liability provisions stated in the Agreement.

10.3. Invalid or Unenforceable Provisions. 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 (a) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible, or if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein.

APPENDIX 1:

DETAILS OF PROCESSING OF CUSTOMER DATA

Subject matter and duration of processing

SentinelOne will process Customer Data, including any personal data contained therein, exclusively to provide the Solutions pursuant to the Agreement, including any retention period(s) purchased by Customer for specific Solutions.

Nature and purpose of processing

SentinelOne will process Customer Data only for the Permitted Purpose.

Categories of Data

The specific nature of Customer Data processed by SentinelOne depends upon the Solutions Customer purchases, but broadly relates to the following categories of data:

- Identification and business contact data (e.g., name, email address)
- Endpoint and endpoint usage data (e.g., active directory user ID, installed applications)
- Network and network usage data (e.g., IP address, URLs)
- Log data provided to SentinelOne by Customer in furtherance of SentinelOne services
- Unstructured data provided to SentinelOne by Customer in furtherance of SentinelOne services

Special categories of data

The Solutions are not intended to process special categories of personal data, and special categories of personal data are not required to deliver the Solutions to Customer. Notwithstanding the foregoing, when Customer controls the data sent to SentinelOne, or in specific services engagements (e.g., forensic investigations requiring analysis of the underlying data), SentinelOne may process special categories of personal data on behalf of Customer. The nature and scope of the special categories of sensitive personal data that is transferred may not be known until after the processing has taken place but may include: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation.

Data subjects

Data subjects include the individuals about whom data is provided to SentinelOne via the Solutions by (or at the direction of) Customer, and may include employees, contractors, consultants, or other individuals belonging to Customer, Customer's customers or clients, and Customer's partners' workforce.

APPENDIX 2:

SECURITY MEASURES

SentinelOne maintains an information security program that is designed to protect the confidentiality, integrity, and availability of Customer Data (the "**SentinelOne Information Security Program**"). The SentinelOne Information Security Program will be implemented on an organization-wide basis and will be designed to ensure SentinelOne's compliance with Applicable Data Protection Law. As of the Effective Date, SentinelOne will implement and maintain the Security Measures described in this Appendix 2.

1. ORGANIZATION OF INFORMATION SECURITY.

1.1. Security Ownership. SentinelOne has appointed a senior officer responsible for coordinating and monitoring the SentinelOne Information Security Program.

1.2. Security Roles and Responsibilities. SentinelOne personnel with access to Customer Data are subject to confidentiality obligations.

1.3. Risk Management Program. SentinelOne has implemented a security risk management program which is based on the requirements of ISO 27005. The Program defines a systematic and consistent process to ensure that security risks to Customer Data are identified, analyzed, evaluated, and treated. Risk treatment and the risk remaining after treatment (i.e., residual risk) is communicated to risk owners, who decide on acceptable levels of risk, authorize exceptions to this threshold, and drive corrective action when unacceptable risks are discovered.

2. HUMAN RESOURCE SECURITY.

2.1. Background Checks. SentinelOne takes reasonable steps to ensure the reliability of any employee, agent, or contractor who may have access to Customer Data, including by conducting background checks on all new employees to the extent permitted by applicable law in the jurisdiction where the employee is located.

2.2. Security Training. SentinelOne informs its personnel about the SentinelOne Information Security Program and Applicable Data Protection Law upon hire and annually thereafter. Personnel are also informed of possible consequences – up to and including termination – of breaching the SentinelOne Information Security Program.

3. ASSET MANAGEMENT.

3.1. Inventory Maintenance. Assets utilized to process Customer Data are identified and an inventory of these assets is listed and maintained. Assets maintained in the inventory and assigned an owner. Company-provided assets are governed by SentinelOne's Acceptable Use Policy.

3.2. Return. All employees and external party users are required to return organizational assets in their possession upon termination of their employment, contract, or agreement.

4. ACCESS CONTROL.

4.1. Internal Data Access. SentinelOne's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process Customer Data. SentinelOne employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. SentinelOne requires the use of unique user IDs, strong passwords, two factor authentication, and monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on the authorized personnel's job responsibilities, job duty requirements necessary to perform authorized tasks, and a need to know basis. The granting or modification of access rights must also be in accordance with SentinelOne's internal data access policies and training. Access to systems is logged to create an audit trail for accountability.

4.2. VPN and Zero Trust. Employees must be in a SentinelOne office or connected via VPN or zero trust network (authenticated with user ID, password, and MFA) then login to an internal portal via SSO before connecting to any system storing Customer Data.

5. CRYPTOGRAPHY.

5.1. Encryption Practices. Customer Data is encrypted in transit using TLS and at rest using AES ciphers.

6. PHYSICAL SECURITY.

6.1. Datacenter Security. The standard physical security controls at each geographically-distributed data center utilized to host Customer Data are comprised of reliable, well-tested technologies that follow generally accepted industry best practices: custom-designed electronic card access control systems, alarm systems, biometric identification systems, interior and exterior cameras, and a 24x7x365 presence of security guards.

6.2. Office Access. Access to SentinelOne offices is protected via card access control systems including individually-assigned keycards, access logging, and interior and exterior surveillance and alarm systems.

7. OPERATIONS AND COMMUNICATIONS SECURITY

7.1. Operational Policy. SentinelOne maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.

7.2. Network Security. Customer management console servers are isolated to help ensure that no access is possible among servers of different customers. The SentinelOne network is protected by redundant firewalls, commercial-class router technology, and a host intrusion detection system on the firewall that monitors malicious traffic and network attacks.

7.3. Vulnerability Assessment and Penetration Testing. SentinelOne conducts annual, comprehensive penetration testing by a third party service. This includes testing of the management console and agents (black and grey box), corporate infrastructure penetration testing and social targeted attack, and public website automatic testing for open vulnerabilities. Quarterly network vulnerability assessments are conducted on all servers in the corporate network as well as the production environment.

7.4. Event Logging. SentinelOne logs access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.

7.5. Data Deletion. Customer Data is deleted irretrievably upon request or contract termination in accordance with the DPA.

8. SUPPLIER RELATIONSHIPS.

8.1. Approval Process. Before onboarding any supplier to process Customer Data, SentinelOne conducts an audit of the security and privacy practices of the supplier to ensure the supplier provides a level of security and privacy appropriate to their proposed access to Customer Data and the scope of the services they are engaged to provide. Once SentinelOne has assessed the risks presented by the supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy terms prior to processing any Customer Data in accordance with the DPA.

9. INFORMATION SECURITY INCIDENT MANAGEMENT.

9.1. Incident Response Process. SentinelOne has put in place a security incident management process for managing security incidents that may affect the confidentiality, integrity, or availability of its systems or data, including Customer Data. The process specifies courses of action, procedures for notification, escalation, mitigation, post-mortem investigations after each incident, response actions, periodic testing, and documentation.

9.2. Security Operations Center. SentinelOne has a dedicated SOC function which manages and monitors a Security Information & Event Management (SIEM) solution deployed across the organization.

10. BUSINESS CONTINUITY MANAGEMENT.

10.1. Customer Data Backups. SentinelOne conducts a daily backup of all Customer Data in the Hosting Location. Where available, backups are physically located in a different availability zone from where Customer Data is hosted (but within the same Hosting Location). A monitoring process is in place to ensure successful ongoing backups within a defined RTO and RPO.

APPENDIX 3:
JURISDICTION-SPECIFIC DATA PROTECTION LAWS

The terms in each Module of this Appendix 3 apply only where the corresponding law applies to the processing of Customer Data.

MODULE 1: EUROPEAN DATA PROTECTION LAW

1. ADDITIONAL DEFINITIONS.

1.1. "**Adequate Country**" means: (a) for data processed subject to the EU GDPR: any county within the EEA, or a country or territory that is the subject of an adequacy decision by the Commission under Article 45(1) of the EU GDPR; (b) for data processed subject to the UK GDPR: the UK or a country or territory that is the subject of the adequacy regulations under Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act of 2018; and/or (c) for data processed subject to the Swiss FDPA: Switzerland or a country or territory that (i) is included in the list of states whose legislation ensures an adequate level of protection as published by the Swiss Federal Protection and Information Commissioner, or (ii) is the subject of an adequacy decision by the Swiss Federal Council under the Swiss FDPR.

1.2. "**Alternative Transfer Mechanism**" means a mechanism, other than the SCCs, that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Law, for example a data protection framework recognized as ensuring that participating entities provide adequate protection.

1.3. "**European Data Protection Law**" means, as applicable: (a) the EU GDPR; (b) the UK GDPR; or (c) the Swiss FADP.

1.4. "**European Law**" means, as applicable: (a) EU or EU member State law (if the EU GDPR applies to the processing of Customer Data); (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Data); or (c) the law of Switzerland (if the Swiss FADP applies to the processing of Customer Data).

1.5. "**Restricted Transfer**" means the transfer or processing of Customer Personal Data to or in a country that is not an Adequate Country.

1.6. "**SCCs**" means the SCCs (Controller-to-Processor) or the SCCs (Processor-to-Processor), as applicable.

1.7. "**SCCs (Controller-to-Processor)**" means the terms at: https://www.sentinelone.com/legal/sccs/eu-c2p.

1.8. "**SCCs (Processor-to-Processor)**" means the terms at: https://www.sentinelone.com/legal/sccs/eu-p2p.

1.9. "**Swiss FDPA**" means the Federal Data Protection Act of 19 June 1992 (Switzerland).

1.10. "**UK GDPR**" means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act of 2018, and applicable secondary legislation made under the same.

2. NOTIFICATION OF COMPLIANCE. Without prejudice to SentinelOne's obligations under Section 4.3 (Customer Instructions and Obligation) of the DPA or any other rights or obligations of either party under the Agreement, SentinelOne will immediately notify Customer if, and to the extent such notice is not otherwise prohibited by European Law, in SentinelOne's opinion: (a) European Law prohibits SentinelOne from complying with an instruction; (b) an instruction does not comply with European Data Protection Law; or (c) SentinelOne is otherwise unable to comply with an instruction. If Customer is a processor, Customer will immediately forward to the relevant controller any notice provided by SentinelOne under this Section.

3. DATA TRANSFERS.

3.1. **Restricted Transfers**. If the processing of Customer Personal Data constitutes a Restricted Transfer then, subject to Section 3.2 of this Module 1 of Appendix 3, the SCCs will apply (according to whether Customer is a controller and/or a processor) with respect to such Restricted Transfer between SentinelOne and Customer.

3.2. **Alternative Transfer Mechanism**. The SCCs will not apply to a Restricted Transfer if SentinelOne has adopted an Alternative Transfer Mechanism for that Restricted Transfer.

3.3. **Information About Restricted Transfers**. SentinelOne will provide Customer with information relevant to a Restricted Transfer (a) as described in Section 7.5 (Audits and Records) of the DPA, and (b) in relation to SentinelOne's adoption of an Alternative Transfer Mechanism, at

https://www.sentinelone.com/legal/alternative-transfer-mechanism/.

3.4. **SCCs Audit**. If the SCCs apply as described in Section 3.1 (Restricted Transfers) of this Module 1 of Appendix 3, SentinelOne will allow Customer, or an independent auditor appointed by Customer, to conduct audits as described in those SCCs an, during an audit, make available all information required by those SCCs, both in accordance with Section 7.4 (Audits and Records) of the DPA.

3.5. **No Modification of SCCs**. Nothing in the Agreement (including this Appendix 3) is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under European Data Protection Law.

3.6. **Precedence of SCCs**. To the extent there is any conflict or inconsistency between any SCCs and the remainder of the Agreement, including this Appendix, the SCCs will prevail.

MODULE 2: U.S. STATE DATA PROTECTION LAWS

1. ADDITIONAL DEFINITIONS.

1.1. "**CCPA**" means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations.

1.2. "**CPA**" means the Colorado Privacy Act, Colo. Rev. Stat. §§ 13-61-101 et seq., and all implementing regulations.

1.3. "**CTDPA**" means the Connecticut Privacy Act and all implementing regulations.

1.4. "**UCPA**" means the Utah Consumer Privacy Act, Utah Code Ann. §§ 13-61-101 et seq., and all implementing regulations.

1.5. "**VCDPA**" means the Virginia Consumer Data Protection Act, VA Code Ann. §§ 59.1-575 et seq., and all implementing regulations.

1.6. "**U.S. Data Protection Law**" means, as applicable, the CCPA, the CPA, the UCPA, the VCDPA, and all other laws and regulations relating to data protection, the processing of personal data, privacy, and/or electronic communications in force from time to time in the United States.

2. PROHIBITIONS. Without prejudice to SentinelOne's obligations under Section 4.3 (Customer Instructions and Obligation) of the DPA, with respect to the processing of Customer Data in accordance with the CCPA, SentinelOne will not, unless otherwise permitted under U.S. Data Protection Law: (a) sell or share Customer Data; (b) retain, use, or disclose Customer Data for any purpose other than those specified in the Agreement and the DPA; (c) retain, use, or disclose Customer Data for any commercial purpose other than the business purpose specified in the Agreement and the DPA, including in the servicing of a different business; (d) retain, use, or disclose Customer Data outside the direct business relationship between SentinelOne and Customer; or (e) combine or update Customer Data with any other personal information that SentinelOne receives from or on behalf of a third party or collects from its own interactions with the consumer.

3. NOTIFICATION OF COMPLIANCE. Without prejudice to SentinelOne's obligations under Section 4.3 (Customer Instructions and Obligation) of the DPA, or any other rights or obligations of either party under the Agreement, SentinelOne will notify Customer if, in SentinelOne's opinion, SentinelOne is unable to meet its obligations under U.S. Data Protection Law, unless such notice is prohibited by applicable law.

4. DEIDENTIFIED DATA. If Customer Data contains deidentified data, SentinelOne will (a) take reasonable measures to ensure the information cannot be associated with a consumer, (b) publicly commit to process deidentified data solely in deidentified form and not attempt to reidentify the information; and (c) contractually obligate any recipients of deidentified data to comply with the foregoing requirements and U.S. Data Protection Law.

5. CUSTOMER REMEDIATION. SentinelOne grants Customer the right, upon reasonable notice, to take reasonable and appropriate steps to stop and remediate any and all unauthorized use of Customer Data.

APPENDIX 4:
SOLUTIONS-SPECIFIC TERMS

The terms in each Module of this Appendix 4 apply solely with respect to the processing of Customer Data by the corresponding Solution(s).

MODULE 1: PROMPT PRODUCTS

1. ADDITIONAL DEFINITIONS.

1.1. "**Prompt Products**", if not defined in the Agreement, means the SentinelOne products and services identified as a Prompt product in a Quote.

2. AMENDMENTS. The DPA is amended as follows with respect to Prompt Products:

2.1. Sub-processor Details. In addition to the Sub-processors identified in Section 6.2 (Sub-processor Details), the following additional Sub-processor shall also apply to the processing of Customer Data for Prompt Products: Prompt Security, Ltd.; Beit Rubinstein, Lincoln St 20, Floor 2, Tel Aviv-Yafo, 6713412, Israel.

2.2. Hosting Location. Notwithstanding any Hosting Location selected by Customer for other Solutions as set forth in Section 8.1 (Data Hosting Location), Customer Data hosted by SentinelOne related to Customer's use of Prompt Products shall be hosted in the regions offered by SentinelOne for Prompt Products and selected by Customer on an Order Form for the Prompt Products.

MODULE 2: OBSERVO PRODUCTS

1. ADDITIONAL DEFINITIONS.

1.1. "**Observo Products**", if not defined in the Agreement, means the SentinelOne products and services identified as an Observo product in a Quote.

2. AMENDMENTS. The DPA is amended as follows with respect to Observo Products:

2.1. Hosting Location. Notwithstanding any Hosting Location selected by Customer for other Solutions as set forth in Section 8.1 (Data Hosting Location), Customer Data hosted by SentinelOne related to Customer's use of Observo Products shall be hosted in the regions offered by SentinelOne for Observo Products and selected by Customer on an Order Form for the Observo Products.