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. Capitalized terms defined in this DPA shall apply to this DPA and any terms not defined in this DPA shall have their meaning as defined in the Agreement.

1. DEFINITIONS.

1.1 "**Adequate Country**" means:

1.1.1. or data processed subject to the EU GDPR: the EEA, or a country or territory that is the subject of an adequacy decision by the Commission under Article 45(1) of the GDPR;

1.1.2. 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 2018; and/or

1.1.3. or data processed subject to the Swiss FDPA: Switzerland, or a country or territory that (i) is included in the list of the 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 FDPA.

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 Laws;

1.3 "**Customer Personal Data**" means the personal data contained within the Customer Data;

1.4 "**Contracted Processor**" means SentinelOne or a SentinelOne Subprocessor;

1.5 "**European Data Protection Laws**" means, as applicable: (i) the GDPR; (ii) the UK GDPR; and/or (iii) the Swiss FDPA;

1.6 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.7 "**Non-European Data Protection Laws**" means all laws and regulations that apply to SentinelOne processing Customer Personal Data under the Agreement that are in force outside the European Economic Area, the UK, and Switzerland;

1.8 "**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 on systems managed or otherwise controlled by SentinelOne;

1.9 "**SCCs**" means the SCCs (EU Controller-to-Processor), SCCs (EU Processor-to-Processor), and SCCs (UK Controller-to-Processor);

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

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

1.12 "**SCCs (UK Controller-to-Processor)**" means the terms at: www.sentinelone.com/legal/sccs/uk-c2p;

1.13 "**Subprocessor**" means other processors used by SentinelOne to process Customer Data, as described in Article 28 of the GDPR;

1.14 **"Swiss FDPA**" means the Federal Data Protection Act of 19 June 1992 (Switzerland); and

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

1.16 The terms "personal data", "data subject", "processing", "controller", and "processor" as used in this DPA have the meanings given in the GDPR irrespective of whether European Data Protection Laws apply.

1.17 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. PROCESSING OF CUSTOMER PERSONAL DATA.

2.1 If European Data Protection Laws apply to the processing of Customer Personal Data:

2.1.1. the subject matter and details of the processing are described in Appendix 1;

2.1.2. SentinelOne is a processor of that Customer Personal Data under European Data Protection Laws;

2.1.3. Customer is a controller or processor of that Customer Personal Data under European Data Protection Laws; and

2.1.4. Each party will comply with the obligations applicable to it under the European Data Protection Laws with respect to the processing of that Customer Personal Data.

2.2 If Non-European Data Protection Laws apply to either party's processing of Customer Personal Data, the relevant party will comply with any obligations applicable to it under that law with respect to the processing of that Customer Personal Data.

2.3 SentinelOne shall:

2.3.1. not process Customer Personal Data other than to provide the Solutions in accordance with the Agreement (including as set forth in this DPA and as described in Appendix 1 to this DPA), unless processing is required by applicable law to which the relevant Contracted Processor is subject (the "**Permitted Purpose**"), in which case SentinelOne shall to the extent permitted by applicable law inform the Customer of that legal requirement before the relevant processing of that Customer Personal Data; and

2.3.2. immediately notify Customer if, in SentinelOne's opinion, European Data Protection Laws prohibit SentinelOne from complying with the Permitted Purpose or SentinelOne is otherwise unable to comply with the Permitted Purpose. This Section does not reduce either party's rights or obligations elsewhere in the Agreement.

2.4 Customer hereby:

2.4.1. instructs SentinelOne to process Customer Personal Data for the Permitted Purpose; and

2.4.2. 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 Customer Affiliate.

3. SECURITY.

3.1 SentinelOne will implement and maintain the technical and organizational measures set forth in Appendix 2 (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.

3.2 Without prejudice to SentinelOne's obligations under Section 3.1 above and elsewhere in the Agreement, Customer is responsible for its use of the Solutions and its storage of any copies of Customer Data outside SentinelOne's or SentinelOne's Subprocessors' systems, including: **(i)** using the Solutions to ensure a level of security appropriate to the risk to the Customer Data; **(ii)** securing the authentication credentials, systems, and devices Customer uses to access the Solutions; and **(iii)** backing up its Customer Data as appropriate.

3.3 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.

4. SUBPROCESSING.

4.1 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 4.2. In addition, and without prejudice to Section 4.4, Customer generally authorizes the engagement as Subprocessors of any other third parties ("**New Subprocessors**").

4.2 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).

4.3 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 (i) SentinelOne shall work with Customer in good faith to address Customer's objections regarding the New Subprocessor; and (ii) 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 Agreement and SentinelOne shall refund to Customer all prepaid fees for the Solutions attributable to the subscription term (as outlined in the applicable Purchase Order under the Agreement) following the termination of the Agreement.

4.4 With respect to each Subprocessor, SentinelOne shall:

4.4.1. 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);

4.4.2. 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 and, if the processing of Customer Personal Data is subject to European Data Protection Laws, ensure that the data protection obligations in this DPA are imposed on the Subprocessor; and

4.4.3. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

5. INDIVIDUAL RIGHTS.

5.1 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 fulfilment of Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise Individual rights under the Data Protection Laws.

5.2 SentinelOne shall:

5.2.1. promptly notify Customer if any Contracted Processor receives a request form an Individual under any Data Protection Law with respect to Customer Personal Data to the extent that SentinelOne recognizes the request as relating to Customer; and

5.2.2. ensure that the Contracted Processor does not respond to that request except on the documented instructions of Customer or as required by applicable laws to which the Contracted Processor is subject, in which case SentinelOne shall to the extent permitted by applicable laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

6. SECURITY BREACHES.

6.1 SentinelOne shall notify Customer promptly and without undue delay upon becoming aware of a Security Breach for which notification to a supervisory authority or data subject is required under applicable European or Non-European Data Protection Laws, and promptly take reasonable steps to minimize harm and secure Customer Data.

6.2 SentinelOne's notification of a Security Breach will describe: the nature of the Security Breach including the Customer resources impacted; the measures SentinelOne has taken, or plans to take, to address the Security Breach and mitigate its potential risk; the measures, if any, SentinelOne recommends that Customer take to address the Security Breach; and 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.

6.3 As it pertains to any Security Breach, SentinelOne has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements pertaining to notification or otherwise.

6.4 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.

7. IMPACT ASSESSMENTS AND PRIOR CONSULTATION. To the extent SentinelOne is required by Data Protection Laws, 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 prior consultations with data protection regulators by providing information in accordance with Section 9.

8. DATA DELETION.

8.1 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.

8.2 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.

9. AUDITS AND RECORDS.

9.1 SentinelOne shall allow for, and contribute to, audits, including inspections, conducted by the Customer (or an independent auditor appointed by Customer) in accordance with the following procedures:

9.1.1. Upon Customer's request, SentinelOne will provide Customer or its appointed auditor 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.

9.1.2. SentinelOne will reasonably cooperate with Customer by providing available additional information concerning the Security Measures to help Customer better understand such Security Measures.

9.1.3. If further information is needed by Customer to comply with its own or other controller's audit obligations or a competent supervisory authority's request, Customer will inform SentinelOne to enable SentinelOne to provide such information or to grant access to it.

9.2 SentinelOne may object in writing to an auditor appointed by Customer if the auditor is, in SentinelOne's reasonable opinion, not suitably qualified or independent, a competitor of SentinelOne, or otherwise manifestly unsuitable, and any such objection will require Customer to appoint another auditor or conduct the audit or inspection itself.

9.3 All requests under this Section 9 shall be made in writing to SentinelOne at privacy@sentinelone.com.

10. RESTRICTED TRANSFERS.

10.1 The parties acknowledge that European Data Protection Laws do not require SCCs or an Alternative Transfer Mechanism in order for Customer Personal Data to be processed in or transferred to an Adequate Country ("**Permitted Transfers**").

10.2 If the processing of Customer Personal Data involves any transfers that are not Permitted Transfers, and European Data Protection Laws apply to those transfers ("**Restricted Transfers**"), then:

10.2.1. if SentinelOne announces its adoption of an Alternative Transfer Solution for any Restricted Transfers, SentinelOne will ensure that such Restricted Transfers are made in accordance with that Alternative Transfer Solution; or

10.2.2. if SentinelOne has not adopted an Alternative Transfer Solution for any Restricted Transfers, then:

10.2.2.1. the SCCs (EU Controller-to-Processor) and/or (EU Processor-to-Processor) will apply (according to whether Customer is a controller and/or processor) with respect to Restricted Transfers between SentinelOne and Customer that are subject to the EU GDPR and/or the Swiss FDPA; and

10.2.2.2. the SCCs (UK Controller-to-Processor) will apply with respect to Restricted Transfers between SentinelOne and Customer that are subject to the UK GDPR.

11. GENERAL TERMS.

11.1 Without prejudice to clause 18 of the Standard Contractual Clauses, **(i)** the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of it nullity; and **(ii)** this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

11.2 Nothing in this DPA reduces SentinelOne's obligations under the Agreement in relation to the protection of Customer Data or permits SentinelOne to process (or permit the processing of) Customer Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

11.3 Subject to Section 11.2, 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.

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

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

APPENDIX 1:

DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

Subject matter and duration of processing

SentinelOne will process Customer Personal Data as necessary to provide the Solutions pursuant to the Agreement. The duration of the processing will be until 60 days after the Cessation Date.

Nature and purpose of processing

SentinelOne will process Customer Personal Data only to the extent reasonably necessary to provide Customer the Solutions and associated Support.

Categories of Data

SentinelOne processes the Customer Personal Data described below in relation to the Solution(s) a Customer contracts for:

Singularity. SentinelOne may process the following categories of Customer Personal Data in connection with Singularity:

- user and endpoint data: agent ID, endpoint name, customer active directory user ID, user name, installed applications – installation time, size, publisher and version, SMTP user name, configuration data related to active directory integration;
- full file path: will include personal data only if file name as named by Customer includes data;
- in cases of suspected threats, the SentinelOne agent collects for each process (file metadata, hash, file type, certificate, command line arguments, network access metadata (IP address, protocol), registry (created keys, deleted keys, modified key names);
- network data (internal network IP address, public IP address (if running cloud-based Management Console);
- threat information (file path, agent IDs, SMS messages content (which may include user names, IP addresses, file names);
- live network monitoring (URLs, URL headers, time stamps); and
- where Customer utilizes SentinelOne's File Fetching feature: any Data contained in files fetched by Customer's administrators.

Dataset and XDR Ingest. SentinelOne may process the following categories of Customer Personal Data in connection with Dataset and/or XDR Ingest:

- data relating to individuals provided to SentinelOne by (or at the direction of) Customer in any data ingested by Customer to Dataset and/or XDR Ingest.

Special categories of data

Customer Personal Data does not include special categories of personal data or data relating to criminal convictions or offenses, except where such data is uploaded by Customer in connection with the Dataset or XDR Ingest Services or accessed by Customer using the File Fetching feature of the SentinelOne Solutions.

Data subjects

Data subjects include the individuals about whom data is provided to SentinelOne via the Solutions by (or at the direction of) Customer.

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 data protection laws and regulations applicable to SentinelOne's performance under the Agreement. The SentinelOne Information Security Program shall include the safeguards set forth below which substantially conform to the ISO/IEC 27001 control framework.

DOMAIN	PRACTICES
Organization of Information Security	**Security Ownership**. SentinelOne has appointed a senior security officer responsible for coordinating and monitoring the SentinelOne Information Security Program. **Security Roles and Responsibilities**. SentinelOne personnel with access to Customer Data are subject to confidentiality obligations. **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.
Human Resource Security	**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. **Security Training**. SentinelOne informs its personnel about the SentinelOne Information Security Program and applicable data privacy laws upon hire and annually thereafter. SentinelOne also informs its personnel of possible consequences – up to and including termination – of breaching the SentinelOne Information Security Program.
Asset Management	**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 are assigned an owner. Company-provided assets are governed by SentinelOne's acceptable use policy. **Return**. All employees and external party users are required to return organizational assets in their possession upon termination of their employment, contract, or agreement.
Access Control	**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. **VPN and Zero Trust**. Employees must be in a SentinelOne office or connected via VPN or zero trust network (authenticated with user id + password + pin/token), then login to an internal portal via SSO, before connecting to any system storing Customer Data.

Cryptography	**Encryption Practices**. Customer Data is encrypted in transit using TLS and at rest using AES ciphers.
Physical Security	**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. **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.
Operations and Communications Security	**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. **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. **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. **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.
Supplier Relationships	**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.
Information Security Incident Management	**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. **Security Operations Center**. SentinelOne has a dedicated SOC function which manages and monitors a Security Information & Event Management (SIEM) solution deployed across the organization.
Business Continuity Management	**Customer Data Backups**. SentinelOne conducts a daily backup of all Customer Data in the data center location chosen by the Customer to host Customer Data. Where available, backups are physically located in a different availability zone from where Customer Data is hosted (but within the same region). A monitoring process is in place to ensure successful ongoing backups, with an RTO of 4 hours and a RPO of 24 hours.