Splunk Data Protection Agreement

Applies to Customer's Personal Data

This Data Protection Agreement (**"DPA"**) applies where, and to the extent that, Splunk Processes Personal Data as a Processor for You when You purchase the Offerings and any applicable Orders (each a "**Party**" and together the "**Parties**").

If You are a Party to the Splunk General Terms, this DPA is an addendum to and forms part of the General Terms. The Splunk entity that is a party to the General Terms is a party to this DPA. You enter this DPA on behalf of yourself and, to the extent required under applicable law, in the name and on behalf of your Affiliates authorized to use the Offerings under the General Terms (whether or not such Affiliates have executed an Order).

If You are an Affiliate authorized to use the Offerings under the General Terms, are not subject to a separate agreement with Splunk, and have executed an Order with a Splunk entity, this DPA is an addendum to that Order and applicable renewal Order. The Splunk entity that is party to such Order is party to this DPA.

This DPA is made effective as of the date of the last signature to, or electronic acceptance of, the General Terms or applicable Order, ("**DPA Effective Date**"), and will become effective on the DPA Effective Date and remain in effect until all Your Offerings have expired, unless earlier terminated pursuant to the General Terms.

To the extent of any conflict between the General Terms and the DPA, the DPA will prevail.

This DPA is not available for and does not apply to trial, evaluation, beta, free, donated, test, or development licenses of Splunk's products or services. A DPA executed in connection with any such license is void.

All capitalized terms not defined in Section 1 or otherwise in this DPA will have the meanings set forth in the General Terms. Any privacy or data protection related clauses or agreement previously entered into by the Parties with regards to the subject matter of this DPA will be superseded by and replaced with this DPA. No one other than a Party to this DPA, their successors and permitted assignees will have any right to enforce any of its terms.

1. Definitions

"CCPA" means the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 to 1798.199) as amended by the California Privacy Rights Act ("CPRA"), and any related regulations or guidance provided by the applicable regulators.

"Controller" means an entity that determines the purposes and means of the processing of Personal Data. It will have the same meaning ascribed to "controller" under the GDPR and other equivalent terms under applicable Data Protection Laws (e.g.: "Business" as defined under the CCPA), as applicable.

"Customer" or "**You**" means the Party identified in the General Terms and any applicable Orders that purchases the Offerings from Splunk under the General Terms.

"Data Breach" means a breach of the Information Security Exhibit, leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

"Data Protection Laws" means all mandatory applicable laws that apply to the Processing of Personal Data under the General Terms.

"**Data Subject**" means the individual to whom Personal Data relates (e.g.: "Consumer" as defined under the CCPA).

"General Terms" means the Splunk General Terms or such other written or electronic agreement between Splunk and Customer for the purchase of Offerings and any applicable Orders.

"GDPR" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

"Information Security Exhibit" means the document describing the measures that Splunk implements to secure Personal Data, which can be found here.

"**Personal Data**" means any information about, or related to, an identified or identifiable natural person Processed by Splunk and/or its Affiliates on behalf of You. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person.

"Offer Disclosure(s)" means the applicable document located on Cisco's Trust Portal that describes the Processing activities in relation to Splunk Offering(s) supplied to You under the General Terms.

"**Processing**" means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. "Processes" and "Process" will be construed accordingly.

"Processor" means an entity that processes Personal Data on behalf of a Controller. It will have the same meaning ascribed to "processor" under the GDPR and other equivalent terms under other Data Protection Laws (e.g.: "Service Provider" as defined under the CCPA), as applicable.

"Representatives" means either Party's (including its Affiliates') officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.

"Subprocessor" means another Processor engaged by Splunk to carry out Processing of Your Personal Data, as set forth in the applicable Offer Disclosure(s).

2. Processing of Personal Data

2.1 The Parties agree that, for this DPA, (i) You will be the Controller and Splunk will be the Processor and/or (ii) You will be the Processor and Splunk will be a further Processor.

2.2 Splunk Processes Personal Data as part of this DPA as follows:

a) The duration of the Processing under this DPA is determined by You and as set forth in the General Terms and any applicable Order.

b) The purpose of the Processing under this DPA is the provision of the Offerings and any applicable Orders by Splunk to You as specified in the General Terms and as further detailed in the DPA and applicable Offer Disclosure(s).

2.3 You will:

a) use the Offerings in compliance with Data Protection Laws;

b) ensure all instructions given by You to Splunk in respect of the Processing of Personal Data are at all times in accordance with Data Protection Laws;

c) ensure all Personal Data provided to Splunk has been collected in accordance with Data Protection Laws and that You have all authorizations and/or consents necessary to provide such Personal Data to Splunk;

d) keep the amount of Personal Data provided to Splunk to the minimum necessary for the provision of the Offerings; and

e) when acting as a Processor, be responsible for passing on to the Controller all the information, assistance and notices needed to comply with its obligations as a Controller under Data Protection Laws, as well as the details of this DPA and the applicable Offer Disclosures, given that You are the Party having a direct relationship with the Controller; and be responsible for passing on to Splunk all Controller's requests and instructions related to the Processing of Personal Data under this DPA.

2.4 Splunk will:

a) only Process Personal Data in accordance with Data Protection Laws, this DPA, the applicable Offer Disclosure(s), the Information Security Exhibit, and any other of Your agreed documented instructions. Splunk will promptly notify You if Splunk reasonably believes that any of Your instructions are inconsistent with Data Protection Laws;

b) ensure its applicable Representatives who may Process Personal Data have written contractual obligations in place with Splunk to keep the Personal Data confidential or are under an appropriate statutory obligation of confidentiality;

c) appoint data protection lead(s). Upon request, Splunk will provide the contact details of the appointed person(s);

d) assist You as reasonably needed to respond to requests from supervisory authorities, Data Subjects, customers, or others to provide information related to Splunk's Processing of Personal Data;

e) if required by Data Protection Laws, court order, subpoena, or other legal or judicial process to Process Personal Data other than in accordance with Your instructions, notify You without undue delay of any such requirement before Processing the Personal Data (unless mandatory applicable law prohibits such notification, in particular on important grounds of public interest);

f) maintain records of the Processing of any Personal Data received from You under the General Terms;

g) not lease, sell, distribute, or otherwise encumber Personal Data unless mutually agreed to by the Parties in a separate agreement;

h) not combine Personal Data received from or on behalf of You and Personal Data collected by Splunk's own interactions with the Data Subject other than as provided in the General Terms or as otherwise permitted by Data Protection Laws;

i) provide such assistance as You reasonably require (either on its own behalf or on behalf of its customers), and Splunk or a Representative is able to provide, in order to meet any applicable filing, approval or similar requirements in relation to Data Protection Laws;

j) provide such information and assistance as You reasonably require (taking into account the nature of Processing and the information available to Splunk) to enable your compliance with Your obligations under Data Protection Laws with respect to:

i security of Processing;

ii data protection impact assessments (as such term is defined by the GDPR);

iii prior consultation with a supervisory authority regarding high-risk Processing; and

iv notifications to the applicable supervisory authority and/or communications to Data Subjects by You in response to any Data Breach;

k) on termination of the DPA for whatever reason, cease to Process Personal Data, and upon your written request and without undue delay, (i) return, or make available for return, Personal Data in its possession or control, or (ii) securely delete or permanently render unreadable or inaccessible existing copies of the Personal Data; unless continued retention and Processing is required or is permitted by Data Protection Laws and/or mandatory applicable law. At your request, Splunk will give You confirmation in writing that it has fully complied with this Section 2.4 (k) or provide a justification as to why such compliance is not feasible.

3. Transfers of Personal Data

Splunk may transfer and Process Personal Data to and in locations where Splunk or its Subprocessors Process Personal Data to provide the Offerings. Splunk, as further detailed in the respective Offer Disclosure(s) and as a wholly-owned subsidiary of Cisco, will conduct such transfers in accordance with the transfer mechanisms set out at Cisco's DPA Portal, which in any event will be subject to the terms and conditions of this DPA. Any further changes to such transfer mechanisms approved with an official decision by the applicable competent authority will be incorporated by reference to this DPA and a copy of the new transfer mechanism will be available at Cisco's DPA Portal.

4. Subprocessing

4.1 Where Splunk appoints a Subprocessor, Splunk will execute a written agreement with the Subprocessor containing terms at least as protective as this DPA. Current Subprocessor(s) are listed in the applicable Offer Disclosure(s).

4.2 Splunk will not subcontract its obligations under this DPA to new Subprocessors, in whole or in part, without providing You with at least 30 days advance notice (e.g.: by publishing this information at Cisco's Trust Portal and/or by email upon Your subscription at Cisco's Trust Portal) and an opportunity to object. If within 10 days of Splunk's notice, You object to the proposed subcontracting by providing reasonable grounds related to the protection of the Personal Data and the Parties cannot resolve the objection within 30 days of Splunk's notice, then You may on written notice, terminate the applicable part of the General Terms and/or Order relating to those Offerings which cannot be provided by Splunk without the use of the Subprocessor(s) giving rise to the objection.

4.3 Splunk will be liable for the acts or omissions of Subprocessors to the same extent it is liable for its own actions or omissions under this DPA.

5. Rights of Data Subjects

Data Subject requests. To the extent legally permitted, Splunk will promptly redirect the Data Subjects to send their requests to You or notify You if it receives a Data Subject request. Unless required by Data Protection Laws, Splunk will not respond to any such Data Subject request without Your prior written consent except to redirect the Data Subject request to You. Splunk will provide such information and cooperation and take such action as you reasonably request in relation to a Data Subject request. You can address Data Subject requests within the Offering in accordance with the applicable Documentation.

6. Security

Controls for the protection of Personal Data. Splunk will implement, maintain and regularly monitor compliance with the security measures specified in the applicable Information Security Exhibit.

7. Audits and Certifications

Upon Your written request, and subject to the confidentiality obligations set forth in the General Terms, Splunk will make available to You reasonably necessary information to demonstrate Splunk's compliance with the obligations of this DPA and Data Protection Laws, in accordance with the Information Security Exhibit, including copies of third-party audit reports or certifications it maintains in the ordinary course of business (such as SOC1, SOC2, SOC3 attestations, or ISO 27001:2013 certifications, or their equivalent under any successor standards) that apply to the relevant Offering. The security certifications that Splunk holds for the Offerings can be found on Splunk's Customer Trust Portal**.**

8. Notification and Communication

8.1 **Notification**. Splunk will notify You within 48 hours of confirmation of a Data Breach under applicable law relating to Your Personal Data. Splunk will provide all such timely information and cooperation as You may reasonably require for you to fulfil Your Data Breach reporting obligations under (and in accordance with the timescales required by) Data Protection Law. Splunk will further take such measures and actions as it considers necessary or appropriate to remedy or mitigate the effects of the Data Breach and will keep You informed in connection with the Data Breach.

8.2 **Information Security Communication in case of Data Breach**. Except as required by mandatory applicable law, Splunk agrees that it will not inform any third party of a Data Breach referencing or identifying You, without Your prior written consent. Splunk will reasonably cooperate with You and law enforcement authorities concerning a Data Breach. Splunk will retain, for an appropriate period of time, all information and data within Splunk's possession or control that is directly related to any Data Breach. If disclosure of the Data Breach referencing or identifying You is required by mandatory applicable law, Splunk will work with You regarding the timing, content, and recipients of such disclosure.

8.3 **Post-incident**. Splunk will reasonably cooperate with You in any post-incident investigation, remediation, and communication efforts.

8.4 **Complaints or notices related to Personal Data**. If Splunk receives any official complaint, notice, or communication that relates to Splunk's Processing of Personal Data or either Party's compliance with Data Protection Laws in connection with Personal Data, to the extent legally permitted, Splunk will promptly notify You and, to the extent applicable, Splunk will provide you with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication.

9. Liability

Splunk's aggregate liability to You arising out of or related to the DPA will be subject to the same limitations and exclusions of liability as apply under the General Terms, whether liability arises under the General Terms or this DPA.