Splunk Data Processing Addendum – US Laws

This Data Processing Addendum ("**DPA**") is incorporated into and forms part of the Splunk General Terms or such other written or electronic agreement between Splunk and Customer for the purchase of Offerings and any applicable Orders ("**Agreement**") and is made as of the date of last signature to the Agreement ("**DPA Effective Date**").

Capitalized terms used but not defined in the body of this DPA or the Agreement are defined in the Definitions section below.

In case of any conflict between the Agreement 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 licences of Splunk's products or services. A DPA executed in connection with any such licence will be void.

How and to Whom this DPA Applies

This DPA applies to Splunk as a Service Provider for the Customer, as follows:

1. If the Customer is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. The Customer enters into this DPA on behalf of itself and, to the extent required under applicable law, in the name and on behalf of its Affiliates authorized to use the Offerings under the Agreement (whether or not such Affiliates have executed an Order).
2. If the Customer is an Affiliate authorized to use the Offerings under the Agreement, is not subject to a separate agreement with Splunk, and has executed an Order with a Splunk entity, this DPA is an addendum to that Order and applicable renewal Order.
3. If the Customer is neither a party to the Agreement nor a party to an Order, this DPA is not valid and is not legally binding.

For data not Processed by Splunk as a Controller, see Splunk's Privacy Policy.

Part I – Applicable Terms for Protecting Personal Information

Subject to the Agreement, the below terms apply to all Personal Information regardless of its source of origin.

1. Processing Personal Information

1.1 **Roles and Responsibilities**. Splunk is a "service provider" for purposes of the Offerings it provides to Customer pursuant to the Agreement, according to the meaning given to that term under Data Protection Law. Customer is a Business or a Service Provider. Customer grants a general authorization to engage Sub-processors and specifically authorizes: (i) Splunk to appoint any other Splunk Affiliate as a Sub-processor; and (ii) Splunk and any Splunk Affiliate to appoint third-party Sub-processors to support the performance of the Offerings as provided below.

1.2 **Splunk Processing Activities**. Splunk agrees that it (and its Sub-processors) will: (i) Process Personal Information only on the specific purpose of performing the Offerings specified in the Agreement with the Customer, unless otherwise agreed or permitted under Data Protection Law, including for a Business Purpose; (ii) ensure that only authorized personnel who are under written obligations of confidentiality have access to such Personal Information; and (iii) take appropriate technical and organizational measures to secure the Personal Information as set out in Section 7 (Technical and Organizational Measures).

Splunk certifies that it will not Sell or Share a Consumer's Personal Information or combine it with Personal Information Splunk receives from, or on behalf of, another person or entity, unless otherwise agreed.

Splunk certifies that it understands the restrictions set out for service providers under Data Protection Law and will comply with them. In the event of Splunk's uncured material breach of Section 1.2 above, Customer retains the right, upon reasonable notice to Splunk, to take reasonable and appropriate steps to stop and remediate any unauthorized Processing of Personal Information by Splunk

1.3 Customer Processing Activities. Customer agrees that if it uses the Offerings to submit Personal Information to Splunk, it will: (i) do so in accordance with the requirements of Data Protection Law, including, if applicable, providing notice to Consumers of the use of Splunk; and (ii) provide documented instructions for the Processing of Personal Information that comply with Data Protection Law. Customer will have sole responsibility for the accuracy, quality and legality of Personal Information and the means by which Customer or any relevant third-party acquired Personal Information. Unless specifically identified in an Order, Customer agrees to not transmit or store within the Offerings any data that it is not otherwise entitled to transmit or store under the Agreement.

1.4 Details of Processing Activities. The nature and extent of Processing Personal Information by Splunk to deliver the Offerings is determined and controlled solely by Customer. Annex I of the Appendix to this DPA sets out the duration,

nature and purpose of the Processing of Personal Information. The categories of Personal Information and Consumers whose Personal Information may be Processed by Splunk are also set out in Annex I.

2. Sub-processing

2.1 **Current Sub-processors**. A list of Splunk's current Sub-processors by Offering is at: https://www.splunk.com/en_us/legal/privacy/privacy-policy/Sub-processors.html.

2.2 **New Sub-processors.** To receive advance notification of new Sub-processors added to Offerings, subscribe to Splunk's Data Protection Notification Portal at: https://www.splunk.com/en_us/form/splunk-subprocessor-signup.html ("**Advance Notification**").

2.3 **Obligations of and Liability for Sub-processors**. Splunk requires that any Sub-processor it engages to provide Offerings on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such Sub-processor terms no less protective of Personal Information than those imposed on Splunk in this DPA. Splunk agrees to be fully liable for the acts or omissions of its third-party Sub-processors to the same extent as Splunk would be liable if performing the Offerings of the Sub-processors under the terms of the Agreement.

3. Consumer Requests

If Splunk receives a Consumer Request from Customer's Consumer, it will promptly notify Customer. Splunk will refrain from responding to the Consumer except to acknowledge receipt of the Consumer Request, to which Customer hereby agrees. Customer can address Consumer Requests within the Offering in accordance with the applicable Documentation. Upon Customer's request, Splunk will provide reasonable assistance to help Customer fulfil a Consumer Request. Splunk reserves the right to charge a mutually agreed fee for assistance rendered upon Customer request. Requests for assistance from Splunk should be made to DPO@splunk.com.

4. Assistance

Splunk will provide assistance to Customer as Customer reasonably requests (taking into account the nature of Processing and the information available to Splunk) in relation to Customer's obligations under Data Protection Law with respect to: (a) data protection impact assessments or similar privacy assessments required under Data Protection Law); (b) Customer's compliance with its obligations under Data Protection Law with respect to the security of Processing; and (c) any prior consultations required with a regulatory authority.

Requests for assistance from Splunk as provided herein should be made to DPO@splunk.com or such other location as Splunk may make available on its website from time to time.

5. Deletion or Return of Personal Information

Upon termination of the Hosted Service, Customer may at its sole discretion and expense, delete or retrieve Customer Content, including any Personal Information contained therein, from the Hosted Services as provided in the Agreement. For On-Premises Products, Splunk does not Process or store Customer Content, except to the extent it may be included in diagnostic files submitted in connection with Splunk's Support Program, which are deleted in accordance with Splunk's Data Retention Policy at: https://www.splunk.com/en_us/legal/splunk-retention-policy.html. In the event Splunk is required under applicable law to retain Personal Information Processed under this DPA after termination of the Agreement, Splunk will protect the Personal Information as set out in Section 7 (Technical and Organizational Measures).

6. Inspections and Audit

6.1 Splunk will contribute to audits requested by Customer, not more than once annually (except in the event of a Personal Information Breach or request from a regulatory authority) to demonstrate Splunk's compliance with its obligations under this DPA by: (i) in the case of Hosted Services, providing to Customer (or Customer's independent third-party auditor that is not a competitor of Splunk) a copy of the relevant and most recent third-party audit reports or certifications, or such other written documentation generally provided by Splunk if the Hosted Services are not audited by a third-party; (ii) in the case of On-Premises Products, providing such information generally provided to similarly situated customers to demonstrate Splunk's compliance with its obligations as a Service Provider; and (iii) such additional information in Splunk's possession or control requested or required by a regulatory authority to demonstrate its compliance with the Personal Information Processing activities carried out by Splunk under this DPA.

6.2 If a Customer who purchased Hosted Services is required under Data Protection Law to request any further information to confirm Splunk's compliance with its obligations under this DPA, such additional information (including any on-site inspections) will be provided and/or conducted in accordance with Splunk's fee-based Customer Audit Program. Splunk's Customer Audit Program terms are available upon request by email to DPO@splunk.com. Customer and Splunk will mutually agree upon the scope, timing and duration of any on-site inspection, including with respect to any third-party inspector selected by the Customer. Customer will promptly notify Splunk of any non-conformance discovered during an on-site audit.

6.3 Requests or inquiries regarding audit services provided herein should be made to DPO@splunk.com or such other location as Splunk may make available on its website from time to time.

7. Technical and Organizational Measures

Splunk provides the technical and organizational measures required under Data Protection Law for the security of the Personal Information it Processes as set out in the Agreement and Annex II of the Appendix to this DPA.

8. Personal Information Breach

8.1 **Personal Information Breach Notification**. Splunk will notify Customer without undue delay after becoming aware of a Personal Information Breach. Where appropriate in respect of any Personal Information which has been the subject of a Personal Information Breach, Splunk will provide reasonable assistance to Customer to the extent required for Customer to comply with Data Protection Law, which may include assistance in notifying Consumers and the relevant regulatory authority, providing a description of the Personal Information Breach, including where possible: (i) the nature of the Personal Information Breach and the categories and approximate number of Consumers and/or Personal Information records concerned; (ii) the name and contact details of Splunk's data protection officer or other contact point; (iii) a description of (a) the likely consequences of the Personal Information Breach and (b) measures to mitigate its possible adverse effects. If it is not possible to provide the above information simultaneously, additional information will be provided without undue delay as it becomes available.

8.2 **Cooperation in case of Personal Information Breach**. If Customer determines that a Personal Information Breach must be notified to a regulatory authority, Consumer, or the public under Data Protection Law, to the extent such notice makes reference to Splunk, whether or not by name, Customer agrees to consult with Splunk in good faith and in advance to consider any clarifications or corrections Splunk may reasonably request to the notification consistent with Data Protection Law.

9. General

9.1 Splunk will inform Customer, immediately upon becoming aware, if in Splunk's opinion any instructions provided by Customer under this DPA infringe Data Protection Law.

9.2 Splunk's aggregate liability to Customer arising out of or related to the DPA will be subject to the same limitations and exclusion of liability as apply under the Agreement, whether liability arises under the Agreement or this DPA.

9.3 This DPA will be governed by and construed in accordance with the governing law provisions set out in the Agreement.

9.4 Splunk will notify Customer within five (5) business days if it determines that it can no longer meet its obligations under Data Protection Law.

Definitions

Term	Meaning
Agreement	As defined in the preamble.
Business	As defined under Data Protection Law.
Business Purpose	As defined under Data Protection Law.
Consumer	As defined under Data Protection Law.
Consumer Request	As defined under Data Protection Law.
Customer	The party which has entered into the Agreement with Splunk.
Data Protection Law	The California Consumer Privacy Act of 2018, including as amended by the California Privacy Rights Acts, and all legislation revising, pre-empting, or supplementing the foregoing as updated, amended, or replaced from time to time.
Personal Information	All data which is defined as 'personal information' or 'personal data' under Data Protection Law and which is provided by a Customer to Splunk (directly or indirectly), and accessed, stored, or otherwise Processed by Splunk as a Service Provider as part of its provision of the Offerings to a Customer.
Personal Information Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information while being transmitted, stored or otherwise Processed by Splunk.
Process or Processing	As defined under Data Protection Law, as applicable.
Processor	As defined under Data Protection Law.
Revised FADP	The revised version of the Swiss Federal Act on Data Protection of 25 September 2020, which is scheduled to come into force on 1 January 2023.
Sale or **Sell**	As defined under Data Protection Law.
Service Provider	As defined under Data Protection Law.
Share or **Sharing**	As defined under Data Protection Law.
Sub-processor	Another Service Provider engaged by Splunk in Processing of Personal Information for a Business Purpose, or in other words, a sub-Service Provider.
US	The United States of America.

APPENDIX

ANNEX I

A. LIST OF PARTIES

1. **Name:** Customer's name, as noted in the introductory paragraph of the DPA

   Address: Customer's address, as noted in the introductory paragraph of the DPA

   Contact person's name, position and contact details: As determined by the "Notices" section of the Agreement

   Activities relevant to the data transferred: Customer determines the subject-matter of the processing and Splunk processes data as required to deliver the Offerings

   Role (controller/processor): Business or Service Provider

1. **Name:** Splunk Inc.

   Address: 250 Brannan St., San Francisco, CA 94107 U.S.A.

   Contact person's name, position and contact details: Splunk Data Protection Officer, DPO@splunk.com

   Activities relevant to the data transferred: Processing operations as required to deliver the Offerings to the Customer.

   Role (controller/processor): Service Provider

B. DESCRIPTION OF PROCESSING

Categories of Consumers whose Personal Information is Processed

Customer may submit Personal Information to the Offerings, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to, Personal Information relating to the following categories of Consumers:

- Prospects, customers, business partners, vendors and their respective employees or contractors (who are natural persons)
- Customers' assigned users of the Offerings
- Customers' employees, agents, contractors or advisors (who are natural persons)

Categories of Personal Information Processed

Customer may submit Personal Information to the Offerings, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Information:

- First and last name
- Title
- Position
- Employer
- Business contact information (e.g., company email, phone, physical business address)
- Personal contact information (e.g., email, mobile phone, address)
- ID data
- Connection data
- Location data
- File and message content

Sensitive Information Processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The Customer and Splunk do not envisage that sensitive categories of Personal Information will be Processed under this Agreement.

The frequency of the Processing.

Continuous.

Nature of the processing

Customer determines the subject-matter, nature and duration of the Processing and Splunk and its Sub-processors Process Personal Information as required to deliver the Offerings.

Purpose(s) of Processing

Customer is requesting, and Splunk will provide, the Offerings to the Customer pursuant to the Agreement.

The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period

Customer determines the retention periods applicable to Customer Content (including any Personal Information therein).

For transfers to Sub-processors, also specify subject matter, nature and duration of the Processing

A current list of data importer's Sub-processors is at: https://www.splunk.com/en_us/legal/privacy/privacy-policy/Sub-processors.html. Customer determines the subject-matter, nature and duration of the Processing and Splunk's Sub-processors Process Personal Information as required to deliver the Offerings.

ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the Splunk (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Splunk provides the technical and organizational measures required under Data Protection Law, as defined in the DPA, for the security of the Personal Information it processes as set out in the Agreement. The specific technical and organizational measures are listed in the applicable Security Addenda identified below and may contain, as applicable, measures reasonably designed for:

- Pseudonymisation and encryption of personal information;
- Ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal information in a timely manner in the event of a physical or technical incident;
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- User identification and authorization;
- Protection of data during transmission;
- Protection of data during storage;
- Physical security of locations at which personal information are processed;
- Event logging;
- System configuration, including default configuration;
- Internal IT and IT security governance and management;
- Certification / assurance of processes and products;
- Allowing data portability and ensuring erasure.

Splunk's Security Exhibits for specific offerings: https://www.splunk.com/en_us/legal/splunk-security-exhibits.html

Configuration and Implementation Services Information Security Addendum at: https://www.splunk.com/prof-serv-isa

Splunk requires that any Sub-processor it engages to provide the Offerings on its behalf in connection with the DPA does so only on the basis of a written contract which imposes on such Sub-processor terms no less protective of Personal Information than those imposed on Splunk in the DPA, including the transfer of Personal Information to a third country or international organization in accordance with Data Protection Law.

A current list of data importer's Sub-processors is at: https://www.splunk.com/en_us/legal/privacy/privacy-policy/Sub-processors.html.