Splunk Data Processing Addendum

This DPA is incorporated into and forms part of the Splunk General Terms and applicable Order, or such other written or electronic agreement between Splunk and Customer for the purchase of Splunk Offerings ("**Agreement**").

THIS DATA PROCESSING ADDENDUM ("**DPA**") is made as of the Effective Date (defined below)

BETWEEN

(1) _____, a company incorporated in _____ with a principal place of business at _____ , together with any Affiliates, as defined in the Agreement, which are authorized to use the Splunk Offerings under the Agreement (and provided an Affiliate is not subject to a separate Agreement with Splunk), collectively referred to as "**Customer**"; and

(2) **Splunk Inc.**, whose principal place of business is at 270 Brannan St., San Francisco, CA 94107 ("**Splunk**").

Each a "**Party**" and together, the "**Parties**."

Instructions

This DPA has been pre-signed on behalf of Splunk.

To execute this DPA, Customer must:

(a) complete the information in the section above;

(b) verify that the information is accurate, complete and is the same as the information about Customer provided in the Agreement; and

(c) submit the validly completed, signed and unmodified DPA to Splunk by email at: dpacontracts@splunk.com or execute the DPA online.

This DPA will become effective as of the date the Offerings start as listed in the applicable Order ("**Effective Date**"). This DPA will be deemed legally binding upon receipt by Splunk of a fully executed copy pursuant to the instructions above and supersedes any prior agreements between Customer and Splunk concerning the processing of Personal Data.

How This DPA Applies

In the event of any conflict or inconsistency between the Agreement and this DPA, the latter shall prevail, but only to the extent of the conflict or inconsistency. Any terms which are not defined in this DPA are as defined in the Agreement.

Splunk DPAs are not available for and do not apply to Trials, Evaluations, Beta and Free Licenses. A DPA executed in connection with any such licenses will be deemed null and void.

This DPA is divided into two sections: Part I—European Data Protection; Part II—California Data Protection.

Part I—European Data Protection

Subject to the terms of the Agreement, the below terms and conditions apply to the Processing of Personal Data.

1. Processing of Personal Data

1.1 **Roles and Responsibilities**. Customer is the Data Controller and Splunk is the Data Processor. Customer grants a general authorization to: (a) Splunk to appoint any other Splunk Affiliate as a sub-processor; and (b) 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: (a) Process Personal Data only on the documented instructions from the Customer as set forth in the Agreement and this DPA; (b) ensure that only authorized personnel who are under written obligations of confidentiality have access to such Personal Data; and (c) take appropriate technical and organizational measures to secure the Personal Data as set forth in Section 7 (Technical and Organizational Measures). Splunk further agrees that it will comply with the Data Protection Law applicable to Splunk in the provision of Offerings under the Agreement and this DPA.

1.3 **Customer Processing Activities.** Customer agrees that if it uses the Offerings to submit Personal Data to Splunk, it will: (a) do so in accordance with the requirements of Data Protection Law, including, if applicable, providing notice to Data Subjects of the use of Splunk as a Processor; and (b) provide documented instructions for the Processing of Personal Data that comply with Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer or any relevant third-party acquired Personal Data. Unless specifically identified in an Order, Customer agrees to not transmit or store within the Offerings any restricted Personal Data as set forth in the Agreement.

1.4 **Details of Processing Activities.** The nature and extent of Personal Data processed by Splunk to deliver the Offerings is determined and controlled solely by Customer. Appendix A sets out the duration, nature and purpose of the processing of Personal Data. The categories of Data and Data Subjects whose Personal Data that may be processed by Splunk are also set forth in Appendix A.

2. Sub-processing

2.1 **Current Sub-processors**. Customer gives its general authorization to engage sub-processors. A list of Splunk's current sub-processors by Offering is available on Splunk's Privacy Policy and is attached as Appendix B. To receive advance notification of new sub-processors added to Splunk Offerings, subscribe to Splunk's Notification Portal.

2.2 **Right to Object to New Sub-processors**. If Customer has a reasonable objection to any new sub-processor, it shall notify Splunk of such objection in writing within ten (10) business days of Splunk's notice as provided in Section 2.1 above (Current Sub-processors). Within thirty (30) days after receipt of Customer's objection to a new sub-processor, the parties will seek to resolve the matter in good faith. If Splunk can provide the Offerings to Customer under the Agreement without using the sub-processor and decides in its discretion to do so, then Customer will have no further rights to object the sub-processor under this Section 2.2.

If Splunk requires the sub-processor to provide the Offerings, within sixty (60) days of Customer's written objection Customer may terminate the Offerings that require the sub-processor's services by providing written notice of termination to Splunk as provided under the Agreement.

2.3 **Obligations of and Liability for Sub-processors**. Splunk will require that any sub-processor it engages to provide Splunk 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 Data than those imposed on Splunk in this DPA, including the transfer of Personal Data to a third country or international organization in accordance with Data Protection Law. 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 services of the sub-processors under the terms of the Agreement.

3. Subject Access Requests

If Splunk receives a Data Subject Request from Customer's Data Subject, it will promptly notify Customer. Splunk will refrain from responding to the Data Subject except to acknowledge receipt of the Request, to which Customer hereby agrees. Customer can address Data Subject Requests within the Offering in accordance with the applicable Documentation. Upon request, Splunk will provide reasonable assistance to help Customer facilitate a Data Subject Request. Splunk reserves the right to charge for such assistance. Requests for assistance from Splunk hereunder 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 (as such term is defined in 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 Supervisory Authority.

5. Deletion or Return of Personal Data

Upon termination of the Hosted Service, Customer may at its sole option and expense, delete or retrieve Customer Content, including any Personal Data contained therein, from the Hosted Services as provided in the Agreement. For On-Premise 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 Retention Policy.

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 Data Breach or request from a Supervisory Authority) to demonstrate Splunk's compliance with its obligations under this DPA by: (a) 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 audits or certifications, or such other written documentation generally provided by Splunk if the Hosted Services are not subject to a third-party audit or certification; (b) in the case of On-Premises Products, providing such information in its possession or control as Customer may reasonably request to demonstrate Splunk's compliance with its obligations as a Data Processor; and (c) such additional information in Splunk's possession or control requested or required by a Supervisory Authority to demonstrate its compliance with the data processing activities carried out by Splunk under this DPA.

6.2 If Customer 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 at Splunk's then-current Configuration and Implementation Services rates, taking into account the amount of resources and time required. 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 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.

7. Technical and Organizational Measures

Splunk provides the technical and organizational measures required under applicable Data Protection Law for the security of the Personal Data it processes as set forth in the Agreement.

8. International Data Transfers

8.1 The standard contractual clauses (processors) pursuant to European Commission Decision 2010/87/EU ("C2P Clauses"), attached hereto as Appendix C, are incorporated into this DPA and apply where the application of the C2P Clauses, as between the Parties, is required under applicable Data Protection Law for the transfer of Personal Data. Customer acknowledges that Splunk will process Personal Data outside the EEA (and the U.K.) including in the United States in compliance with this DPA, the C2P Clauses, the Agreement, and applicable Data Protection Law. Splunk will notify Customer if it determines that it can no longer meet its obligations under the C2P Clauses.

8.2 For the purposes of the C2P Clauses: (a) Customer is the "data exporter"; (b) Splunk is the "data importer"; (c) the governing law at Clause 9 is the Member State in which the Customer is established or the law of England & Wales (if the Customer is established in the UK or if the Customer is not established in any Member State or in the UK); (d) the law referred to at Clause 11(3) is the Member State in which the Customer is established or the law of England & Wales (if the Customer is established in the UK [or if the Customer is not established in any Member State or in the UK), and (e) the process for obtaining the consent of the data exporter for sub-processors under the C2P Clauses is as set out above in Section 2 (Sub-processing) of this DPA.

8.3 Splunk reserves the right to adopt an alternative compliance standard to the C2P Clauses for the lawful transfer of Personal Data, provided it is recognized under Data Protection Law. Splunk will provide 30 days' advance notice of its adoption of an alternative compliance standard to customers who subscribe to its Notification Portal.

9. Personal Data Breach

9.1 **Personal Data Breach Notification.** Splunk will notify Customer without undue delay after becoming aware of a Personal Data Breach. Where appropriate in respect of any Personal Data which has been the subject of a Personal Data 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 Data Subjects and the relevant Supervisory Authority, providing a description of the Personal Data Breach, including where possible: (a) the nature of the Personal Data Breach and the categories and approximate number of Data Subjects and/or Personal Data records concerned; (b) the name and contact details of Splunk's data protection officer or other contact point; (c) a description of the likely consequences of the Personal Data Breach; and (d) the measures taken or proposed to be taken by Splunk to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.2 **Customer Notification to Splunk.** If Customer determines that a Personal Data Breach must be notified to any Supervisory Authority, Data Subject, 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 and consider any clarifications or corrections Splunk may reasonably request to the notification consistent with Data Protection Law.

10. General

10.1 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.

10.2 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.

10.3 The Parties agree that Splunk will be a Data Controller of: (a) Customer business contact information that is Personal Data required to administer the Offerings; and (b) any Personal Data contained within Usage Data as described in the Agreement, and terms of this DPA will not apply.

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

Part II—California Data Protection

1. Roles and Responsibilities

1.1 Splunk is a "service provider," for the purposes of the services it provides to Customer pursuant to the Agreement, according to the meaning given to that term in Section 1798.140(v) of the California Civil Code, as of the date of execution of this DPA.

1.2 Splunk agrees that, to the extent that Customer discloses a Consumer's Personal Information to Splunk, Splunk will Process that Personal Information only on behalf of Customer and pursuant to the Agreement and this DPA.

2. Splunk Processing of Personal Information of Consumers

2.1 Splunk certifies that it shall not Process, retain, use, or disclose a Consumer's Personal Information for any purpose other than for the specific purpose of performing the Offerings specified in the Agreement.

2.2 Splunk agrees that it shall not Sell a Consumer's Personal Information.

2.3 Splunk certifies that it understands the restrictions set forth in Section 1798.140(w)(2)(A) of the California Civil Code, as of the date of execution of this DPA, and will comply with them.

Definitions

"CCPA" means the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq., as updated, amended or replaced from time to time;

"**Consumer**" as defined in Section 1798.140(g) of the CCPA;

"Data Controller" as defined under Data Protection Law;

"**Data Processor**" as defined under Data Protection Law;

"**Data Protection Law**" means all applicable laws and regulations of the European Union, the European Economic Area, their member states, and the United Kingdom, applicable to the Processing of Personal Data including the General Data Protection Regulation (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)("**GDPR**"), the UK Data Protection Act of 2018 and all national legislation reflecting, implementing or supplementing the foregoing as updated, amended or replaced from time to time;

"Data Subject" as defined under Data Protection Law;

"Data Subject Request" means a request from or on behalf of a Data Subject relating to access to, or rectification, erasure or data portability in respect of that person's Personal Data or an objection from or on behalf of a Data Subject to the processing of its Personal Data;

"Supervisory Authority" as defined under Data Protection Law;

"**Personal Data**" means all data which is defined as '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 Data Processor as part of its provision of the Offerings to a Customer and to which Data Protection Law applies from time to time;

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data while being transmitted, stored or otherwise processed by Splunk;

"Personal Information" as defined in Section 1798.140(o) of the CCPA;

"**Process**" or "**Processing**" as defined under Data Protection Law or the CCPA, as applicable; and

"**Sell**" as defined in Section 1798.140(t) of the CCPA.

The Parties' authorized signatories have duly executed this DPA:

CUSTOMER		**SPLUNK INC.**	
By:	_____	By:	DocuSigned by: Jaime Hildebrand F52A29DF2C46470...
Name:	_____	Name:	**Jaime Hildebrand**
Title:	_____	Title:	**Senior Director, Revenue**

Appendix A

Data Subjects

Customer may submit Personal Data to the Splunk 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 Data relating to the following categories of Data Subjects:

- Prospects, customers, business partners, vendors and their respective employees or contractors (who are natural persons)

- Customers' assigned users of the Splunk Offerings

Customers' employees, agents, contractors or advisors (who are natural persons)

Categories of Data

Customer may submit Personal Data to the Splunk 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 Data:

- 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

Subject-Matter

Customer determines the subject-matter of the processing and Splunk processes Personal Data as required to deliver the Offerings.

Duration

Personal Data will be processed for the duration of the Offerings as determined by the Customer and as required by Splunk to administer the Offerings to the Customer.

Nature and Purpose

Customer determines the nature and purpose of the processing and Splunk handles Personal Data as required to deliver the Offerings.

Appendix B

General Splunk Offerings Sub-processor List

Entity	Type of Service	Location
Blue Ocean Contact Centers Inc.	Support	Canada
Salesforce.com, Inc.	Enterprise Services	U.S.
Spencer Rose Limited	Staffing Services and Support	U.K.
P.S. Computer Services Ltd.	IT Staffing Services	U.K.
iOPEX Technologies, Inc.	Technical Support Services	U.S., India
The Kinney Group	IT Infrastructure and Data Center Solution Services	U.S.
TEKsystems, Inc.	Technical Support	U.S.
Crest Data Systems, Inc.& Private LTD	Technical Support	U.S., India
Gary D. Nelson Associates, Inc.	Staffing Services	U.S.
Praecipio Consulting	Support Services	U.S.
Sykes Enterprises, Inc. Sykes Latin America, S.A.	Technical Support	U.S., Costa Rica

General Hosted Services Sub-processor List

Entity	Type of Service	Location
Amazon Web Services, Inc.	Infrastructure-as-a-Service	Splunk On-Call: U.S. (East & West Coast) Splunk Cloud Platform, Splunk Observability Cloud: Location selected by Customer
Google, LLC (GCP)	Infrastructure-as-a-Service	Splunk On-Call: U.S. Splunk Cloud Platform, Splunk Observability Cloud: Location selected by Customer

Offering-Specific Sub-processor List

Splunk Cloud Platform

Entity	Type of Service	Location
Mulesoft, Inc.	Software Orchestration Services	U.S.
Postmark (Wildbit, LLC)	Email Processing	U.S.

Splunk Enterprise (On-prem)

Entity	Type of Service	Location
Mixpanel, Inc.	Mobile Analytics	U.S.
Crashlytics/Firebase (Google, LLC)	Mobile Analytics	U.S.

Splunk Observability Cloud

Entity	Type of Service	Location
Zuora, Inc.	Billing and Account Services	U.S.
Snowflake, Inc	Infrastructure-as-a-Service	U.S.

Appendix B (continued)

Splunk On-Call

Entity	Type of Service	Location
Twilio, Inc.	Customer Messaging Service	U.S.
Mailgun, Inc.	Customer Messaging Service	U.S.
Sendgrid, Inc.	Customer Messaging Service	U.S.
Intercom R&D Unlimited Co.	Customer Communication Service	U.S.
Free Conferencing Corp.	In-Product Calling Functionality	U.S.
Instabug, Inc.	Customer Feedback and Bug Reporting	U.S., Egypt
Zuora, Inc.	Customer Billing	U.S.
Fivetran, Inc.	Software Orchestration Services	U.S.
Jitterbit, Inc.	Software Orchestration Services	U.S.
Periscope Data	Data Analytics	U.S.
New Relic, Inc.	Product Analytics	U.S.
Crashlytics (Google, LLC)	Mobile Analytics	U.S.
Pardot (Salesforce.com, Inc.)	Marketing Automation	U.S.
Pushy, LLC	Customer Messaging Service	U.S.

Appendix C

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: **The entity identified as "Customer" on page 1 of the DPA**

Address: **The address identified for Provider on page 1 of the DPA**

Tel.: .....; fax: ..... ; e-mail: .....

Other information needed to identify the organisation: **None.**

……
(the data **exporter**)

And

Name of the data importing organisation: **Splunk Inc.**

Address: **270 Brannan St., San Francisco, CA 94107**

Tel.: **(415) 848-8400**; fax:..... ; e-mail: **DPO@splunk.com**

Other information needed to identify the organisation: **None.**

……
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): _____

Position: _____

Address: **The address identified for Provider on page 1 of the DPA**

Other information necessary in order for the contract to be binding (if any):

Signature _____

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Jaime Hildebrand

Position: Senior Director, Revenue

Address: **270 Brannan St., San Francisco, CA 94107**

Other information necessary in order for the contract to be binding (if any):

Signature DocuSigned by: Jaime Hildebrand F52A29DF2C46470...

(stamp of organisation)

Appendix 1 to the Standard Contractual Clauses

Data Exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Customer is requesting Services from Splunk pursuant to the Agreement.

Data Importer

The data importer is (please specify briefly your activities relevant to the transfer):

Splunk Inc. will provide the Services to the Customer pursuant to the Agreement.

Data Subjects

The personal data transferred concern the following categories of data subjects (please specify):

Please refer to data subjects as set out in Appendix A of the DPA.

Categories of Data

The personal data transferred concern the following categories of data (please specify):

Please refer to categories of data as set out in Appendix A of the DPA.

Special Categories of Data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

The data importer and data exporter do not envisage that special categories of data will be processed under these clauses.

Processing Operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Processing operations as required to deliver the Services to the Customer.

Appendix 2 to the Standard Contractual Clauses

Splunk provides the technical and organizational measures required under applicable Data Protection Law, as defined in the DPA, for the security of the Personal Data it processes as set forth in the Agreement.