splunk®>

Amendment to Splunk Data Processing Addendum

This Amendment dated as of Created Date, ("**Amendment**") hereby amends the Splunk Data Processing Addendum ("**DPA**") entered into between Splunk LLC ("**Splunk**") and Account Name ("**Customer**").

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

Instructions

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

To execute this Amendment, Customer must:

(a) complete the information in the section above;

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

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

How This Amendment Applies

Any terms which are not defined in this Amendment are as defined in the DPA or Agreement.

Order of Precedence. In the event of any conflict between the following documents, and only to the extent of such conflict, the order of precedence will be as follows:

(a) between the Agreement and the DPA as amended via this Amendment, the amended DPA will prevail;
(b) between this amended DPA and the EU Clauses or UK Clauses (both as defined below), the EU Clauses or UK Clauses (as applicable) will prevail;
(c) In the event the International Data Transfers section of theDPA was previously amended this Amendment supersedes and replaces any such prior amended section between the Parties.

This Amendment will be deemed legally binding upon receipt by Splunk of a fully executed copy pursuant to the instructions above.

This Amendment is not available for and does not apply to trial, evaluation, beta, free, donated, test, or development licenses. An Amendment executed in connection with any such licenses will be deemed null and void.

Substitution of EU Clauses

The Parties hereby agree to replace the standard contractual clauses ((European Commission Decision 2010/87/EU), previously annexed to the DPA, with the standard contractual clauses pursuant to European Commission Decision 2021/914/EU ("**EU Clauses**"), attached to this Amendment as Exhibit 1 and Exhibit 2

International Data Transfers

The Parties further agree to replace the International Data Transfers section of the DPA in its entirety with the following provisions:

1. Data Transfers to Third Countries

Customer acknowledges that its use of the Offerings will involve the transfer of Personal Data to, and Processing of Personal Data in, locations outside of the EU, the EEA, the UK and/or Switzerland from time to time, including Processing in the United States.

2. Data Transfers under the EU Clauses

2.1 The EU Clauses are incorporated into the DPA and apply where the application of the EU Clauses, as between the Parties, is required under Data Protection Law for the transfer of Personal Data. The EU Clauses are attached as Exhibit 1 and Exhibit 2 to this DPA.

2.2 For transfers to the UK, the EU Clauses are not required due to the UK Adequacy Decision. However, in the event that the UK Adequacy Decision is revoked, the EU Clauses shall immediately apply to transfers of Personal Data to the UK.

2.3 Where Customer is a Controller, and Splunk a Processor, Module Two of the EU Clauses (Exhibit 1) will apply. Where Customer is a Processor, and Splunk a Processor, Module Three of the EU Clauses (Exhibit 2) will apply.

2.4 For the purposes of the EU Clauses, Customer is the "data exporter" and Splunk is the "data importer."

2.5 For the application of the EU Clauses, the Parties agree on the following:

2.5.1 Clause 8.1: The DPA, as amended via this Amendment, and the Agreement will be deemed to be Customer's final documented instructions as of the Effective Date.

2.5.2 Clause 8.5: Splunk's obligations in respect of erasure are supplemented by Section 5 of the DPA (Deletion or Return of Personal Data).

2.5.3 Clause 8.9(c): Customer's rights under Clause 8.9(c) may be exercised as set out in Section 6 of this DPA (Inspections and Audit).

2.5.4 Clause 9(a): Customer's rights under Clause 9(a) may be exercised as set out in Section 2 of the DPA (Sub-processing).

3. Swiss Data Transfers

3.1 Where the FADP or the Revised FADP require sufficient safeguards for the adequate protection of Personal Data transferred to a third country, the EU Clauses will apply.

3.2 In case of a transfer from Switzerland subject to the FADP or the Revised FADP, the terms below will have the following substituted meanings for the purposes of the EU Clauses:

3.2.1 "GDPR" means the FADP and the Revised FADP.

3.2.2 "European Union", "Union" or "Member States" means Switzerland, provided that the term "member state" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence, provided it is in Switzerland in accordance with Clause 18 c.

3.2.3 "Supervisory Authority" means the FDPIC.

3.3 The EU Clauses will also protect the data of legal entities until the entry into force of the Revised FADP.

4. UK Data Transfers

4.1 To the extent Personal Data is transferred to Splunk and Processed by or on behalf of Splunk outside the UK in circumstances where such transfer would be prohibited by the UK Data Protection Act 2018 in the absence of a transfer mechanism, the parties agree that the EU Clauses subject to the UK Addendum will apply. The UK Addendum is incorporated by reference into this DPA.

4.2 The tables of the UK Addendum are filled-in as follows:

4.2.1 **Table 1**: The information required for Table 1 is contained in Annex I.A of Exhibit 1 and 2 to this Amendment and the start date shall be the Effective Date.

4.2.2 **Table 2:** The versions of the EU Clauses to which the UK Addendum applies are Module Two (Controller to Processor) and/or Module Three (Processor to Processor).

4.2.3 **Table 3:** The list of parties and description of the transfer are as set out in Annex I.A and I.B of Exhibit 1 and 2 to this Amendment, Splunk's technical and organizational measures are set in Annex II of Exhibit 1 and 2 to this Amendment, and the list of Splunk's sub-processors is located on Splunk's website at: https://www.splunk.com/en_us/legal/privacy/privacy-policy/sub-processors.html.

4.2.4 **Table 4:** Neither party will be entitled to terminate the UK Addendum in accordance with clause 19 of the UK Mandatory Clauses.

5. Supplementary Measures

5.1 This section supplements but does not modify the EU Clauses or the UK Addendum.

5.2 In the event that Personal Data is transferred to a country where the EU Clauses or the UK Addendum are required, and the third country does not ensure an essentially equivalent level of protection to Personal Data as the European Union or the UK, Splunk has put in place the following supplementary measures:

5.2.1 **Technical and organizational measures:** The full list of technical and organizational measures, including the links to Splunk's different security exhibits, are laid out in Annex II **of** Exhibit 1 and 2 to this Amendment.

5.2.2 **Splunk Data Request Guidelines:** Splunk's general practices for responding to requests by government agencies and other third parties is published on Splunk Protects at https://www.splunk.com/en_us/pdfs/legal/splunk-data-request-guidelines.pdf.

6. Notification

Splunk will promptly notify Customer if it determines that it can no longer meet its obligations under the EU Clauses or the UK Addendum.

7. Variations

Splunk reserves the right to adopt an alternative compliance standard to replace the EU Clauses or the UK Addendum for the lawful transfer of Personal Data, provided it is recognized under Data Protection Law. Splunk will provide thirty (30) days' advance notice of its adoption of the alternative compliance standard to customers who subscribe to its Data Protection Notification Portal (available at: https://www.splunk.com/en_us/form/splunk-subprocessor-signup.html) and by email to customers who do not subscribe to the portal. The variation will automatically apply as set out in Splunk's notification at the end of the notice period.

Definitions

"**EEA**"	is the European Economic Area.

"**EU**"	is the European Union.
"**EU Clauses**"	is the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
"**FADP**"	is the Swiss Federal Act on Data Protection of 19 June 1992.
"**FDPIC**"	is the Swiss Federal Data Protection and Information Commissioner.
"**GDPR**"	is the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
"**Revised FADP**"	is 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.
"**UK**"	is the United Kingdom.
"**UK Addendum**"	is the template international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (VERSION B1.0) issued by the UK's Information Commissioner's Office and laid before Parliament in accordance with S119A(1) UK Data Protection Act 2018.
"**UK Adequacy Decision**"	is the Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.
"**UK Data Protection Act 2018**"	is the United Kingdom Act of Parliament of 23 May 2018 as updated by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 laid on 14 October 2020.
"**UK Mandatory Clauses**"	means the Mandatory Clauses of the UK Addendum, as updated from time to time and/or replaced by the UK's Information Commissioner's Office.

Execution of this Amendment includes deemed execution of the EU Clauses and the UK Addendum by both Parties. The Parties' authorized signatories have duly executed this Amendment:

Account Name By: _____ Name: _____ Title: _____ Date: _____	**SPLUNK LLC** By: _____ Name: **Amy Solus** Title: **VP, Deal Strategy and Execution** Date: _____
	SPLUNK SERVICES UK LIMITED By: _____ Name: **Leo Heinze**

	Title: **DSE, Deal Engagement Manager**
	Date: _____ _____

EXHIBIT 1 to the Amendment

STANDARD CONTRACTUAL CLAUSES

(Controller to Processor Module)

SECTION I

Clause 1

Purpose and scope

(a)   The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b)   The Parties:

(i)   the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

(ii)   the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c)   These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d)   The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a)   These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(e)   These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a)   Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

6

(ii)   Clause 8.1(b) and Clause 8.9(a), (c), (d) and (e);

(iii)   Clause 9(a), (c), (d) and (e);

(iv)   Clause 12(a), (d) and (f);

(v)   Clause 13;

(vi)   Clause 15.1(c), (d) and (e);

(vii)   Clause 16(e);

(viii)   Clause 18(a) and (b).

(b)   Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a)   Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b)   These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c)   These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

(Intentionally left blank)

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1   Instructions

(a)   The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b)   The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2   Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3   Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4   Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5   Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6   Security of processing

(a)   The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission,

where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b)   The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c)   In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d)   The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7   Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8   Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i)   the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii)   the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii)   the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv)   the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9   Documentation and compliance

(a)   The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b)   The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c)   The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d)   The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e)   The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a)   The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b)   Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c)   The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d)   The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e)   The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a)   The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b)   The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall

set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c)   In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a)   The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(a)   In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(b)   Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

    (i)   lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

    (ii)   refer the dispute to the competent courts within the meaning of Clause 18.

(d)   The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e)   The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f)   The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a)   Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b)   The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c)   Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d)   The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e)   Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f)   The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g)   The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a)   The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b)   The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a)   The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b)   The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

    (i)   the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

    (ii)   the laws and practices of the third country of destination -including those requiring the disclosure of data to public authorities or authorising access by such authorities -relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

    (iii)   any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c)   The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d)   The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e)   The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third

country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f)   Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1   Notification

(a)   The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

  (i)   receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

  (ii)   becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b)   If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)   Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d)   The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)   Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2   Review of legality and data minimisation

(a)   The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)   The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation

available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c)   The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)   The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)   In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)   The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

     (i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

     (ii)   the data importer is in substantial or persistent breach of these Clauses; or

     (iii)   the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d)   Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e)   Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18

Choice of forum and jurisdiction

(a)   Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b)   The Parties agree that those shall be the courts of the Netherlands.

(c)   A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d)   The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

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 under these Clauses: data exporter determines the subject-matter of the processing and data importer processes data as required to deliver the Offerings

Signature and date:

CUSTOMER
Signature: _____
Date: _____

Role (controller/processor): Controller

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Splunk LLC

Address: 3098 Olsen Drive, San Jose, California 95128 U.S.A.

Contact person's name, position and contact details: Chief Privacy Officer, Cisco Systems, Inc. 170 West Tasman Dr., San Jose, CA 95134 USA

Americas Privacy Officer, Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134 USA

Europe, Middle East, and Africa (EMEA) Privacy Officer, Cisco Systems International BV, Haarlerbergweg 13-19, 1101 CH Amsterdam-Zuidoost, Netherlands

Asia Pacific, Japan, and China (APJC) Privacy Officer, Cisco Systems (USA) Pte Ltd, 80 Pasir Panjang Road, Level 25, Maple Tree Business City 2, Singapore 117372

Activities relevant to the data transferred under these Clauses: Processing operations as required to deliver the Offerings to the data exporter.

Signature and date:

SPLUNK LLC
DocuSigned by: *Amy Solus* F61B9082F650472...

16

Signature: _____

Date: _____

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Please refer to the categories of Data Subjects as set forth in Appendix A of the DPA.

Categories of personal data transferred

Please refer to the categories of Personal Data as set forth in Appendix A of the DPA.

Sensitive data transferred (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 data importer and data exporter do not envisage that special categories of data will be Processed under these clauses.

The frequency of the transfer (eg. whether the data is transferred on a one-off or continuous basis).

Continuous.

Nature of the processing

Data exporter determines the subject-matter, nature and duration of the Processing and data importer's sub-processors Process Personal Data as required to deliver the Offerings.

Purpose(s) of the data transfer and further processing

Data exporter is requesting, and data importer will provide, the Services to the data exporter pursuant to the Agreement.

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

Data exporter determines the retention periods applicable to Customer Content (including any Personal Data 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 located on Splunk's website at: https://www.splunk.com/en_us/legal/privacy/privacy-policy/sub-processors.html. Data exporter determines the subject-matter, nature and duration of the Processing and data importer's sub-processors Process Personal Data as required to deliver the Offerings.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The Supervisory Authority is determined as follows:

Where Customer is established in an EU Member State, the Supervisory Authority with responsibility for ensuring compliance by Customer with the GDPR as regards the data transfer will act as the competent Supervisory Authority.

Where Customer is not established in an EU Member State but falls within the territorial scope of application of the GDPR, in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR, the Supervisory Authority of the Member State in which the representative is established willact as the competent Supervisory Authority.

Where Customer is not established in an EU Member State, but falls within the territorial scope of application of the GDPR through its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), PO Box 93374, 2509 AJ DEN HAAG, Netherlands, will act as the competent Supervisory Authority.

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

Description of the technical and organisational measures implemented by the data importer(s) (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.

Data importer 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. The specific technical and organizational measures are listed in the applicable Security Exhibits identified below and may contain, as applicable, measures reasonably designed for:

- Pseudonymisation and encryption of personal data;

- Ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- The ability to restore the availability and access to personal data 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 authorisation;

- Protection of data during transmission;

- Protection of data during storage;

- Physical security of locations at which personal data are processed;

- Event logging;

- System configuration, including default configuration;

- Internal IT and IT security governance and managements;

- 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 Exhibit located at: https://www.splunk.com/prof-serv-isa

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller, and, for transfers from a processor to a sub-processor, to the data exporter

Data importer 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 Data than those imposed on data importer in the DPA, including the transfer of Personal Data to a third country or international organization in accordance with Data Protection Law.

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

EXHIBIT 2 to the Amendment

STANDARD CONTRACTUAL CLAUSES

(Processor to Processor Module)

SECTION I

Clause 1

Purpose and scope

(f)   The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(g)   The Parties:

(i)   the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

(ii)   the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(h)   These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(i)   The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(b)   These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(j)   These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(c)   Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

      (i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

      (ii)   Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

      (iii)   Clause 9(a), (c), (d) and (e);

      (iv)   Clause 12(a), (d) and (f);

      (v)   Clause 13;

      (vi)   Clause 15.1(c), (d) and (e);

      (vii)   Clause 16(e);

      (viii) Clause 18(a) and (b).

(d)   Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(d)   Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(e)   These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(f)   These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

(Intentionally left blank)

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1   Instructions

(a)   The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b)   The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c)   The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d)   The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2   Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3   Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4   Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5   Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6   Security of processing

(a)   The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b)   The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c)   In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d)   The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7   Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8   Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([ii]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i)   the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii)   the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii)   the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv)   the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9   Documentation and compliance

(a)   The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b)   The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c)   The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d)   The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e)   Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f)   The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g)   The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a)   GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b)   Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([i]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c)   The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d)   The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e)   The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a)   The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b)   The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c)   In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a)   The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b)   In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c)   Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i)   lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii)   refer the dispute to the competent courts within the meaning of Clause 18.

(d)   The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e)   The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f)   The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a)   Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b)   The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c)   Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d)   The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e)   Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f)   The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g)   The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a)   The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b)   The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a)   The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed

what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination -including those requiring the disclosure of data to public authorities or authorising access by such authorities -relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii)   becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller

(b)   If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)   Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d)   The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)   Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2   Review of legality and data minimisation

(a)   The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)   The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c)   The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

<div align="center">

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

</div>

(a)   The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)   In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)   The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii)   the data importer is in substantial or persistent breach of these Clauses; or

(iii)   the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d)   Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e)   Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18

Choice of forum and jurisdiction

(e)   Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(f)   The Parties agree that those shall be the courts of the Netherlands.

(g)   A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(h)   The Parties agree to submit themselves to the jurisdiction of such courts.

<u>APPENDIX</u>

ANNEX I

A.   LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

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 under these Clauses: data exporter determines the subject-matter of the processing and data importer processes data as required to deliver the Offerings

Signature and date:

CUSTOMER
Signature: _____
Date: _____

Role (controller/processor): Processor

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Splunk LLC

Address: 3098 Olsen Drive, San Jose, California 95128 U.S.A.

Contact person's name, position and contact details: Chief Privacy Officer, Cisco Systems, Inc. 170 West Tasman Dr., San Jose, CA 95134 USA

Americas Privacy Officer, Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134 USA

Europe, Middle East, and Africa (EMEA) Privacy Officer, Cisco Systems International BV, Haarlerbergweg 13-19, 1101 CH Amsterdam-Zuidoost, Netherlands

Asia Pacific, Japan, and China (APJC) Privacy Officer, Cisco Systems (USA) Pte Ltd, 80 Pasir Panjang Road, Level 25, Maple Tree Business City 2, Singapore 117372

Activities relevant to the data transferred under these Clauses: Processing operations as required to deliver the Offerings to the data exporter.

Signature and date:

SPLUNK LLC

Signature: _____

Date: _____

Role (controller/processor): Processor

B.   DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Please refer to the categories of Data Subjects as set forth in Appendix A of the DPA.

Categories of personal data transferred

Please refer to the categories of Personal Data as set forth in Appendix A of the DPA.

Sensitive data transferred (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 data importer and data exporter do not envisage that special categories of data will be Processed under these clauses.

The frequency of the transfer (eg. whether the data is transferred on a one-off or continuous basis).

Continuous.

Nature of the processing

Data exporter determines the subject-matter, nature and duration of the Processing and data importer's sub-processors Process Personal Data as required to deliver the Offerings.

Purpose(s) of the data transfer and further processing

Data exporter is requesting, and data importer will provide, the Services to the data exporter pursuant to the Agreement.

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

Data exporter determines the retention periods applicable to Customer Content (including any Personal Data 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 located on Splunk's website at: https://www.splunk.com/en_us/legal/privacy/privacy-policy/sub-processors.html. Data exporter determines the subject-matter, nature and duration of the Processing and data importer's sub-processors Process personal data as required to deliver the Offerings.

C.   COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The Supervisory Authority is determined as follows:

Where Customer is established in an EU Member State, the Supervisory Authority with responsibility for ensuring compliance by Customer with the GDPR as regards the data transfer will act as the competent Supervisory Authority.

Where Customer is not established in an EU Member State but falls within the territorial scope of application of the GDPR, in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR, the Supervisory Authority of the Member State in which the representative is established willact as the competent Supervisory Authority.

Where Customer is not established in an EU Member State, but falls within the territorial scope of application of the GDPR through its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR, the Dutch Data

Protection Authority (Autoriteit Persoonsgegevens), PO Box 93374, 2509 AJ DEN HAAG, Netherlands, will act as the competent Supervisory Authority.

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

Description of the technical and organisational measures implemented by the data importer(s) (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.

Data importer 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. The specific technical and organizational measures are listed in the applicable Security Exhibits identified below and may contain, as applicable, measures reasonably designed for:

- Pseudonymisation and encryption of personal data;

- Ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- The ability to restore the availability and access to personal data 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 authorisation;

- Protection of data during transmission;

- Protection of data during storage;

- Physical security of locations at which personal data are processed;

- Event logging;

- System configuration, including default configuration;

- Internal IT and IT security governance and managements;

- 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 Exhibit located at: https://www.splunk.com/prof-serv-isa

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller, and, for transfers from a processor to a sub-processor, to the data exporter

Data importer 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 Data than those imposed on data importer in the DPA, including the transfer of Personal Data to a third country or international organization in accordance with Data Protection Law.

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