Splunk Data Processing Addendum

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

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

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

1. between the Agreement and the DPA, the DPA will prevail;
2. between the DPA and the EU Clauses or the UK Addendum, the EU Clauses or the UK Addendum (as applicable) will prevail.

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

How and to Whom this DPA Applies

This DPA applies to Splunk as a Processor of Personal Data on behalf of the Customer, as follows:

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

For data not Processed by Splunk as a Processor; e.g., Usage Data, see Splunk's Privacy Policy.

This DPA is divided into two sections: Part I–Agreement for the Protection of Personal Data; Part II–European Data Protection Terms.

Part I – Applicable Terms for Protecting Personal Data

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

1. Processing Personal Data

1.1 Roles and Responsibilities. Customer is a Controller or a Processor and Splunk is a Processor. Customer grants a general authorization to: (i) Splunk to appoint any other Splunk Affiliate as a Sub-processor; and (ii) Splunk and any Splunk Affiliate to appoint third-party Sub-processors to support the performance of the Offerings as provided below.

1.2 Splunk Processing Activities. Splunk agrees that it (and its Sub-processors) will: (i) Process Personal Data only on the documented instructions from the Customer as set out in the Agreement and this DPA, unless required to do so by Data Protection Law to which Splunk is subject; (ii) ensure that only authorized personnel who are under written obligations of confidentiality have access to such Personal Data; and (iii) take appropriate technical and organizational measures to secure the Personal Data as set out in Section 7 (Technical and Organizational Measures).

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

1.4 Details of Processing Activities. The nature and extent of Processing Personal Data by Splunk to deliver the Offerings is determined and controlled solely by Customer. Annex I of the Appendix to this DPA sets out the duration, nature and purpose of the Processing of Personal Data. The categories of Personal Data and Data Subjects whose Personal Data may be Processed by Splunk are also set out in Annex I.

2. Sub-processing

2.1 **Current and New Sub-processors**. A list of Splunk's current Sub-processors by Offering is at: https://www.splunk.com/en_us/legal/privacy/privacy-policy/Sub-processors.html. To receive advance notification of new Sub-processors added to Offerings, subscribe to Splunk's Data Protection Notification Portal at: https://www.splunk.com/en_us/form/splunk-subprocessor-signup.html ("**Advance Notification**").

2.2 **Right to Object to New Sub-processors**. If Customer has a reasonable objection to any new Sub-processor, it will notify Splunk of that objection in writing at DPO@splunk.com within 10 business days of Splunk's Advance Notification. Within 30 days of receiving Customer's objection to a new Sub-processor, the parties will seek to resolve the matter in good faith. If Splunk is able to provide the Offerings to Customer under the Agreement without using the Sub-processor in question and decides in its discretion to do so, then Customer's objection to the Sub-processor will be deemed resolved. If Splunk requires the Sub-processor to provide the Offerings, within 60 days of Customer's written objection, Customer may terminate the Offerings that require the Sub-processor's services by providing written notice of termination to DPO@splunk.com.

2.3 **Obligations of and Liability for Sub-processors**. Splunk requires that any Sub-processor it engages to provide Offerings on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such Sub-processor terms no less protective of Personal Data than those imposed on Splunk in this DPA, including the necessary instruments to lawfully transfer Personal Data to a country outside the EU, EEA, UK or Switzerland ("third countries") or international organization in accordance with Data Protection Law. Splunk agrees to be fully liable for the acts or omissions of its third-party Sub-processors to the same extent as Splunk would be liable if performing the services of the Sub-processors under the Agreement.

3. Data Subject Requests

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

4. Assistance

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

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

5. Deletion or Return of Personal Data

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

6. Inspections and Audit

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

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

inspector selected by the Customer. Customer will promptly notify Splunk of any non-conformance discovered during an on-site audit.

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

7. Technical and Organizational Measures

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

8. Personal Data Breach

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

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

9. General

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

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

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

Part II – European Data Protection Terms

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 by reference into this 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 annexes to the EU Clauses, including the duly executed Annex I.A., are attached as an Appendix 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 will 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 will apply. Where Customer is a Processor, and Splunk a Processor, Module Three of the EU Clauses 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 7: The docking clause will not apply.

2.5.2 Clause 8.1: This DPA and the Agreement will be deemed to be Customer's final documented instructions as of the DPA Effective Date. Any further instructions must be consistent with this DPA and the Agreement.

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

2.5.4 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).

2.5.5 Clause 9(a): Option 2 will apply (general written authorization of Sub-processors) and the time period for change notifications will be 30 days. Customer's rights under Clause 9(a) may be exercised as set out in Section 2 of the DPA (Sub-processing).

2.5.6 Clause 11(a): The option to lodge a complaint with an independent dispute resolution body will not apply.

2.5.7 Clause 17: Option 1 will apply with the law of the Agreement if it is the law of an EU Member State, otherwise the law of the Netherlands will apply.

2.5.8 Clause 18(b): Any disputes arising from the EU Clauses will be resolved by the courts determined in the Agreement, if they are the courts of an EU Member State, otherwise the courts of the Netherlands will resolve such disputes.

2.6 The Appendix to the EU Clauses will be completed as follows:

2.6.1 **Annex I.A:** Annex I.A of the Appendix to this DPA contains the information required for Annex I.A of the EU Clauses.

2.6.2 **Annex I.B:** Annex I.B of the Appendix to this DPA contains the information required for Annex I.B of the EU Clauses.

2.6.3 **Annex I.C:** Annex I.C of the Appendix to this DPA contains the information required for Annex I.C of the EU Clauses.

2.6.4 **Annex II:** Annex II of the Appendix to this DPA contains the information required for Annex II of the EU Clauses.

3. Swiss Data Transfers

3.1 Where the FADP requires 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, the terms below will have the following substituted meanings for the purposes of the EU Clauses:

3.2.1 "GDPR" means the 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.

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 completed as follows:

4.2.1 **Table 1**: The information required for Table 1 is contained in Annex I.A of the Appendix to this DPA and the start date will be the DPA 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 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 the Appendix to this DPA, Splunk's technical and organisational measures are set in Annex II of the Appendix to this DPA, and the list of Splunk's Sub-processors is 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 **Annex II:** The full list of technical and organizational measures, including the links to Splunk's different security addenda are in Annex II.

5.2.2 **Splunk Data Request Guidelines:** Splunk's general practices for responding to requests by government agencies and other third parties is 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 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 at: https://www.splunk.com/en_us/form/splunk-subprocessor-signup.html. The variation will automatically apply as set out in Splunk's notification at the end of the notice period.

Definitions

Term	Meaning
Agreement	As defined in the preamble.
Controller	As defined under Data Protection Law.
Customer	The party which has entered into the Agreement with Splunk.
Data Protection Law	All laws and regulations of the EU, the EEA, the UK or Switzerland, applicable to Splunk in providing the Offerings under the Agreement and this DPA, that govern the Processing of Personal Data, including the GDPR, the UK Data Protection Act of 2018, the FADP and the Revised FADP, and all national legislation reflecting, implementing or supplementing the foregoing as updated, amended or replaced from time to time.
Data Subject	As defined under Data Protection Law.
Data Subject Request	A request from or on behalf of a Data Subject relating to access to, or rectification, erasure, or data portability in respect of that person's Personal Data or an objection from or on behalf of a Data Subject to the Processing of its Personal Data.
EEA	The European Economic Area.
EU	The European Union.
EU Clauses	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	The Swiss Federal Act on Data Protection of 19 June 1992 as revised 25 September 2020, in the version effective upon 1 September 2023.
FDPIC	The Swiss Federal Data Protection and Information Commissioner.
GDPR	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).
Personal Data	All data which is defined as 'personal data' under Data Protection Law, and which is provided by a Customer to Splunk (directly or indirectly), and accessed, stored, or otherwise Processed by Splunk as a Processor as part of its provision of the Offerings to a Customer.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data while being transmitted, stored or otherwise Processed by Splunk.
Process or Processing	As defined under Data Protection Law.
Processor	As defined under Data Protection Law.
Revised FADP	The revised version of the Swiss Federal Act on Data Protection of 25 September 2020, which is scheduled to come into force on 1 January 2023.
Splunk	Splunk Inc. and/or Splunk Services UK Limited, as applicable, and as explained on page 1.
Sub-processor	Splunk Affiliates, Splunk Inc. and third parties engaged by Splunk or Splunk Affiliates in connection with the Offerings that process Personal Data according to this DPA.
Supervisory Authority	As defined under Data Protection Law.
UK	The United Kingdom
UK Addendum	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	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	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	The Mandatory Clauses of the UK Addendum, as updated from time to time and/or replaced by the UK's Information Commissioner's Office.

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]*

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

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

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

   Activities relevant to the data transferred 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: per the Agreement

   Role (controller/processor): Controller or Processor

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

1. **Name:** Splunk Inc.

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

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

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

   Signature and date: per the Agreement

   Role (controller/processor): Processor

2. **Name:** Splunk Services UK Limited

   Address: 2 New Bailey, 6 Stanley Street, Salford, Greater Manchester, United Kingdom, M3 5GS

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

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

   Signature and date: per the Agreement

   Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Offerings, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

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

Categories of personal data transferred

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

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

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 (e.g., 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 and its 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 Offerings 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 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 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 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 Data Protection Law, as defined in the DPA, for the security of the Personal Data it processes as set out in the Agreement. The specific technical and organizational measures are listed in the applicable Security Addenda identified below and may contain, as applicable, measures reasonably designed for:

- Pseudonymisation and encryption of personal 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 management;
- Certification / assurance of processes and products;
- Allowing data portability and ensuring erasure.

Splunk's Security Exhibits for specific offerings: https://www.splunk.com/en_us/legal/splunk-security-exhibits.htmlConfiguration and Implementation Services Information Security Addendum 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 at: https://www.splunk.com/en_us/legal/privacy/privacy-policy/Sub-processors.html.