Splunk’s Responses to the European Center for Digital Rights (noyb) questions regarding international data transfers

(“Schrems II Questionnaire”)

Splunk has reviewed the EDPB guidance and the specific questions raised by noyb in their questionnaire regarding international data transfers post-Schrems II. Splunk provides its responses below.

Information on Data Importer

Name of Data Importer: Splunk Inc. (“Splunk”)

Splunk Sub-processors

Splunk Privacy Policy

Splunk Protects (Splunk’s compliance story, including privacy and security)

Information on Provided Offerings

Splunk Cloud

Splunk Observability

Nature and Categories of Data

Splunk Products and Services (“Offerings”) process metadata generated by websites, applications, servers, networks, mobile and other devices, including clickstream and transaction information, network activity and other forms of metadata. This data is not easily readable on its own, however, Splunk Offerings can help you make sense of it.

Machine generated metadata can include personal data (e.g. an IP address or User ID). However, you control the extent to which personal data is processed in Splunk Offerings.

A. International Data Transfers

1. Processing of Personal Data in the United States of America

Does Splunk process personal data under Art. 4 EU General Data Protection Regulation (GDPR) that relates to data subjects located in the European Union, European Economic Area, United Kingdom or Switzerland or that is otherwise subject to the GDPR in the United States of America?

☒ Yes ☐ No

Splunk offers data hosting globally in select AWS and GCP regions. Customers have the ability to choose the region in which their data is hosted. As such, data hosting can be limited to within the EEA. However, processing (as defined by the GDPR) may still be performed in the United States for purposes of providing cloud operations or customer support.

2. Processing of Personal Data outside of EU/EEA

Does Splunk process personal data under Art. 4 GDPR that relates to data subjects located in the European Union, European Economic Area, United Kingdom or Switzerland or that is otherwise subject to the GDPR in a country outside the EEA, and outside any of the following countries: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, United States of America (see above question 1) and Uruguay?

☒ Yes ☐ No

Splunk processes personal data for purposes of providing cloud operations or customer support in Canada, India, Costa Rica, and Australia. Splunk controls access to support ticket information (which may include trace amounts of personal data) in these geographies, through a Virtual Desktop Infrastructure that allows Splunk to log, monitor, audit and terminate access immediately, if required. For the current list of Splunk Sub-processors, including their location, please see **Splunk's Sub-processor Page**.

3. What transfer mechanisms does Splunk rely on to facilitate the onward transfer of data in support of its operations?

☒ SCC ☐ Binding Corporate Rules

☒ Other (if applicable, please specify)

While it was recently invalidated in July, 2020, Splunk continues to adhere to the privacy principles of the Privacy Shield Framework, but no longer rely upon Privacy Shield as a valid transfer mechanism.

4. Is Splunk subject to any other law that could be seen as undermining the protection of personal data under the GDPR (Art. 44 GDPR)?

☐ Yes ☒ No

Please see our whitepaper "**A Risk Assessment of EU Cross-Border Data Transfers to the Splunk Cloud Service.**"

B. Government Access Requests

1. **Has Splunk received any requests from authorities for access (Access Requests) to personal data of data subjects in the EU/EEA in the past?**

   ☐ Yes ☒ No

2. **Does Splunk have a process and safeguards in place to verify the lawfulness of any such Access Requests?**

   ☒ Yes ☐ No

   Splunk evaluates any legal process that it receives and, if appropriate, challenges orders that it believes are beyond permissible scope of the legal authority relied upon or are otherwise unlawful. In addition, unless otherwise prohibited by law, Splunk notifies customers in advance of any legal process it receives prior to responding.

3. **Does Splunk have a process in place to promptly notify customer of any Access Requests, except where legally prohibited?**

   ☒ Yes ☐ No

4. **Does Splunk allow customer to determine the personal data to be disclosed in response to an Access Request in order to ensure that the disclosure does not go beyond what is strictly necessary and proportionate to comply with the Access Request?**

   ☒ Yes ☐ No

   Unless otherwise prohibited by law, Splunk notifies customers in advance of any legal process it receives prior to responding, so that its customer has the opportunity to determine the appropriate response.

5. **Does Splunk give customer the opportunity to object to Access Requests, except where legally prohibited?**

   ☒ Yes ☐ No

   Unless otherwise prohibited by law, Splunk notifies customers in advance of any legal process it receives prior to responding, so that its customer has the opportunity to determine the appropriate response, including any objection.

C. Data Transfers to the United States of America

1. Privacy Shield

Is Splunk certified under the EU-US and Swiss-US Privacy Shield Frameworks?

☒ Yes ☐ No

Splunk is certified to both Frameworks for the transfer of human resources and customer data to the United States. While these Frameworks were recently invalidated by the European Court of Justice in its decision of July 16, 2020, and the Federal Data Protection and Information Commissioner (FDPIC) of Switzerland in its position paper of September 8, 2020, Splunk remains committed to their underlying privacy principles. Splunk currently relies upon the Standard Contractual Clauses for the international cross-border transfer of personal data.

2. Executive Order 12333

Does Splunk cooperate in any respect with US authorities conducting surveillance of communications under EO 12333?

☐ Yes ☐ No ☒ Not Applicable

EO 12333 collection refers to collection of foreign intelligence that takes place under the inherent authority of the President of the United States as Commander-in-Chief, without statutory or judicial regulation. However, EO 12333 affords no compulsive power, and therefore the government would not have authority under EO 12333 to compel or require Splunk to produce a decryption key. For more details, please see our whitepaper "**A Risk Assessment of EU Cross-Border Data Transfers to the Splunk Cloud Service.**"

3. 50 USC § 1881a / sec. 702 of the Foreign Intelligence Surveillance Act (FISA)

Does Splunk fall under one of the following definitions in 50 United State Code (USC) § 1881 b (4) that could render Splunk directly subject to 50 USC § 1881a?

☐ Yes ☒ No

While the definition of an "electronic communication service (ECSP)" is broadly worded to include a "provider of an electronic communication service," a "provider of a remote computing service," or a "communication service provider," as a matter of practice and interpretation under U.S. law, Section 702 has historically been applied to a limited set of providers that offer these services to the general public for the reasons that: **1)** its far easier and more effective for the government to obtain this kind of information from telecommunications providers directly; and **2)** serving a Section 702 order on a company that merely provides email service to its employees would likely not be a particularly useful source of intelligence, because intelligence targets are unlikely to use employer-provided email to communicate.

a. Telecommunications Carrier (sec. 153 of title 47 USC)

Is Splunk a telecommunications carrier?

☐ Yes ☒ No

b. Provider of Electronic Communication Service (sec. 2510 of title 18 USC)

Is Splunk a provider of an electronic communication service?

☐ Yes ☒ No (see above)

c. Provider of a Remote Computing Service (sec. 2711 of title 18 USC)

Is Splunk a provider of a remote computing service?

☐ Yes ☒ No (see above)

d. Any other Communication Service Provider

Is Splunk any other service provider who has access to wire or electronic communications?

☐ Yes ☒ No (see above)

D. Data Transfers to Non-Adequate Third Countries (other than the U.S.)

Splunk relies on sub-processors to provide 24x7x365 availability for the Hosted Services (e.g. IT infrastructure, data centers and staffing for support and technical services). A current list of Splunk's sub-processors, including their location, can be found **here**. In addition, customers may sign up to receive notifications of changes to Splunk's sub-processors **here**.

1. **Is Splunk subject to any law, regulation or executive order in any of the above locations that is likely to have a substantial adverse effect on the level of protection of customer personal data, as required under EU data protection laws, including in relation, but not limited, to potential massive or disproportionate access to personal data by any public authority, or which could otherwise be seen as undermining the protection of customer personal data with a level of protection essentially equivalent to the EU?**

   ☐ Yes ☒ No

   More information about data protection laws of the applicable third party countries where Splunk's sub-processors are currently located can be found here:

   - **Canada**
   - **India**
   - **Costa Rica**
   - **Australia**

2. **Does Splunk limit the processing performed in the above locations?**

   ☒ Yes ☐ No

   Splunk's sub-processors in third countries access data using a Virtual Desktop Infrastructure that allows Splunk to control, monitor, audit and immediately terminate access, if required. For more information, please see our whitepaper "**A Risk Assessment of EU Cross-Border Data Transfers to the Splunk Cloud Service**."

3. **Are data subjects in the EU/EEA whose personal data is subject to Access Requests informed by the accessing public authorities on such access requests?**

   ☐ Yes ☐ No ☒ N/A

   Splunk's Hosted Services are used by businesses, not consumers, and therefore notification is provided to Splunk customers.

4. **Do data subjects in the EU/EEA whose personal data is subject to Access Requests have judicial remedies against such measures?**

   ☐ Yes ☐ No ☒ We do not know

   Unless otherwise prohibited by law, Splunk notifies customers in advance of any legal process it receives prior to responding. It is Splunk's customer's responsibility to determine the appropriate response on behalf of data subjects whose personal data may be processed by customer using the Hosted Services.

E. Technical and Organizational Measures

This section contains information on the safeguards (technical and organizational measures, e. g. encryption) Splunk uses to prevent unauthorized access to customers' data within the Hosted Service.

1. **Has Splunk taken appropriate technical and organizational measures for every step of the processing operations to protect personal data in transit against potential mass surveillance activities by or on behalf of public authorities?**

   ☒ Yes ☐ No

   Splunk's encryption standards currently include:

   Encryption in transit: Data in transit for Splunk Cloud is TLS 1.2+ encrypted. HTTP-based data collection is secured using token-based authentication.

   Encryption at rest: Splunk uses a minimum of AES 256-bit encryption at the infrastructure layer. Splunk Cloud customers can purchase additional encryption at rest at the application layer as a premium option.

   Details can also be found in the **Splunk Cloud service description** and the **Splunk Cloud Security Addendum**.

2. **Has Splunk taken appropriate technical and organizational measures to minimize the likelihood of direct access to personal data by any public authorities via the Internet (network of cables, switches, hubs, and routers)?**

   ☒ Yes ☐ No

   Splunk's encryption standards currently include:

   Encryption in transit: For security, data in transit for Splunk Cloud is TLS 1.2+ encrypted. HTTP-based data collection is secured using token-based authentication.

   Details can also be found in the **Splunk Cloud service description** and the **Splunk Cloud Security Addendum**.