Whitepaper: International Data Transfers & the EU-U.S. Data Privacy Framework

A. Is Splunk certified under the EU-U.S. Data Privacy Framework?

Yes. Splunk is a certified organization under the EU-U.S.Data Privacy Framework (EU-U.S. DPF) for all data transfers from the EU to the United States. Splunk is proud to be among the first organizations to obtain certification under the EU-U.S. Data Privacy Framework. Additional details about Splunk's participation can be found in Splunk's Data Privacy Framework Notice located here.

B. Does Splunk use the EU-U.S. DPF for international data transfers?

Yes. While Splunk's current default transfer mechanism for customer data transfers from the EU to the United States are the Standard Contractual Clauses (SCCs), Splunk offers customers the option to rely on the EU-U.S. DPF for such data transfers. .

For customers with an existing Data Processing Agreement (DPA), the SCCs incorporated by reference into your DPA will continue to be your data transfer mechanism. At the time of your next renewal, you can request to update your DPA to adopt the EU-U.S.DPF as your data transfer mechanism.

For those customers that want to rely on the EU-U.S. DPF to legitimize data transfers from the EU to the United States, the DPA will be updated to leverage the EU-U.S. DPF as the data transfer instrument for customer data transfers from the EU to the United States, with language that incorporates the SCCs by reference and a condition that the SCCs will take immediate effect in the event that the EU-U.S. DPF is invalidated.

C. What is the EU-U.S. DPF and how does it address Schrems II concerns?

On July 10, 2023, the European Commission gave the green light for the new EU-U.S. DPF by adopting its adequacy decision for the EU-U.S. DPF. This adequacy decision officially confirms that the United States ensures an adequate level of protection - compared to that of the EU - for personal data transferred from the EU to the U.S. under the new framework. The effect of the adequacy decision is that personal data can flow freely from the EU (and Norway, Liechtenstein and Iceland) to U.S. companies participating in the EU-U.S. DPF without additional data protection safeguards.

The adequacy decision follows President Biden's Executive Order on 'Enhancing Safeguards for United States Signals Intelligence Activities' in October 2022, which introduced new safeguards to address the points raised by the Court of Justice of the European Union in its Schrems II decision of July 2020. Notably, the new safeguards were designed to ensure that data can be accessed by U.S. intelligence agencies only to the extent of what is necessary and proportionate, and to establish an independent and impartial redress mechanism to handle and resolve complaints from Europeans concerning the collection of their data for national security purposes.

D. How does Splunk's EU-U.S. DPF certification benefit Splunk's customers?

Companies like Splunk that self-certify under the EU-U.S. DPF are publicly committed to comply with the EU-U.S. DPF Principles and this commitment is enforceable under U.S. law. Our certification to the EU-U.S. DPF signals that we have an adequate level of protection for transfers between the EU and U.S. All the safeguards put in place by the US Government in the area of national security under the EU-U.S. DPF (including the redress mechanism) apply to all data transfers under the GDPR to companies in the U.S., regardless of the transfer mechanism utilized. This eases the burden on companies currently attempting to document that appropriate safeguards are in place such that data transfers are appropriate via their data transfer impact assessments. These obligations can now be met by referencing Splunk's DPF certification(s).

E. What about data transfers from Switzerland to the U.S.?

Similar to the prior data transfer framework, there is a separate Data Privacy Framework specific to data transfers from Switzerland to the U.S. known as the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF). Splunk is self-certified under the Swiss-U.S. DPF, but cannot use the framework as a data transfer mechanism until the Swiss Federal Administration recognizes the adequacy of protection provided by the Swiss-U.S. DPF.

F. What about data transfers from the United Kingdom to the U.S.?

Organizations that already participate in the EU-U.S. DPF were permitted to extend their participation to also cover personal data received from the United Kingdom and, as applicable, Gibraltar. As of October 12, 2023, the date the UK adequacy decision takes effect, data transfers from the United Kingdom and Gibraltar can be based on the UK Extension to the EU-U.S. DPF.

G. Where can I find additional details on Splunk's data transfer practices?

While no longer strictly required, Splunk will continue to provide information on its data transfer practices for companies seeking additional details to ensure trust and transparency on our practices. This information is outlined below.

Additional Details on Splunk's Data Transfers

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 Platform**
- **Splunk Observability**

H. Natures 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, GCP and/or Microsoft Azure 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, Australia, and Singapore. 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)

The EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework

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

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. **Data Privacy Framework**

   Is Splunk certified under the EU-U.S. and Swiss-US Data Privacy Frameworks?

   ☒ Yes ☐ No

   Splunk is certified to both Frameworks for the transfer of human resources and customer data to the United States.
   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.

2. **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 versus to those companies that merely provide email services to its employees. This is because: **1)** it's 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 with incidental service offerings like the provision of email services to its employees would likely be an unfruitful exercise (i.e., it’s unlikely that intelligence targets 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

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**
   - **Singapore**

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. **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 ☒ We do not know

   Please note Splunk's Hosted Services are used by businesses, not consumers. Unless otherwise prohibited by law, Splunk notifies customers of any legal process it receives.**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 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 Platform is TLS 1.2+ encrypted. HTTP-based data collection is secured using token-based authentication.

   Encryption at rest: Splunk Cloud Platform customers that select Amazon Web Services (AWS) to host their Splunk Cloud Platform service can purchase encryption at rest (AES 256 standard) at the application layer as a premium option. For customers that select Google Cloud Platform (GCP) to host their Splunk Cloud Platform service, encryption at rest at the application layer is included.

   Details c**an also be fou**nd in the **Splunk Cloud Platform service description** and the **Splunk Cloud Platform Secuurity Addendm**.

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 Platform is TLS 1.2+ encrypted. HTTP-based data collection is secured using token-based authentication.

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