Post-Schrems II International Personal Data Transfers Frequently Asked Questions

Introduction

Strong relationships are built on trust. Here at Juniper, earning our customers' trust is of paramount importance. Protecting our customers' data is integral to building trust, and it is a top Juniper priority.

Juniper and our customers operate in a number of jurisdictions, including the US and the EU, and we appreciate the importance of ensuring that we provide customers with the information they need to evaluate whether our products and services align with requirements of the regulatory landscapes in which they operate, such as the EU General Data Protection Regulation 2016/679 (the "**GDPR**").

We have reviewed the decision by the European Court of Justice (the "**CJEU**") in Schrems II, and as the European Commission and the US Department of Commerce engage in workable solutions to support EU-US personal data transfers, such as the EU-US and Swiss-US Data Privacy Framework ("**DPF**") we have made it a priority to provide our customers with these Frequently Asked Questions ("**FAQs**") to assist in their analysis of Juniper's processes and procedures in conducting applicable EEA-US transfers of personal data.

Background

In Schrems II, the CJEU considered whether privacy protections in US law relating to intelligence agencies' access to data meet EU legal standards. In its July 2020 judgment, the CJEU invalidated the EU-US Privacy Shield and determined that the Standard Contractual Clauses ("**SCCs**") approved by the European Commission for the transfer of personal data outside the European Economic Area ("**EEA**") would need to be reviewed in light of its concerns regarding certain privacy protections under US law. As discussed within Question 5 of this FAQ, the European Data Protection Board ("**EDPB**") subsequently adopted recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

In response to Schrems II, the U.S. Department of Justice issued a whitepaper stating that U.S. privacy safeguards would "[e]nsure that U.S. intelligence agencies' access to data was based on clear and accessible legal rules, proportionate access to data for legitimate purposes, supervision of compliance with those rules through independent and multi-layered oversight, and effective remedies for violations of rights."[1] The U.S. Department of Justice also explained that for most companies, the data that is processed is of no interest to the U.S. intelligence community because it involves ordinary commercial information like employee, customer, or sales records and is unrelated to matters such as potential hostile acts of a foreign power or the proliferation of weapons of mass destruction.

In July 2023, the European Commission adopted an adequacy decision that concluded there is an adequate level of protection for personal data transferred from the EEA to the US, provided that the data importer participates

1. *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU -U.S. Data Transfers after Schrems II*

in the DPF. A data importer that relies on the DPF does not need to rely on the SCCs as an appropriate safeguard under Article 46 of the GDPR for EEA-US data transfers.

1. Does Juniper rely on Data Privacy Framework for data transfers to the US from the EEA?

- At this time, Juniper has chosen not to rely on the DPF to facilitate the lawful transfer of personal data between the EU or Switzerland and the U.S. Juniper will continue to rely on the SCCs, which is permitted under the GDPR and Schrems II, and which requires data importers to implement certain supplementary measures – whether legal, technical, or organizational – to ensure that a data subject would have similar protections in the US (as in the EEA).
- Unlike the DPF, which is only applicable to data transfers from the EEA to the US, the SCCs are relevant to transfers of personal data to non-U.S. countries that have not been granted an adequacy decision by the European Commission.

2. Which US Laws concerned the CJEU in Schrems II and why?

- The CJEU highlighted its concerns that certain US surveillance laws can cause US recipients of personal data to breach their obligations with respect to personal data relating to individuals in the EEA, whether such obligations are contractual or owed directly through the extra-territorial scope of the GDPR.
- In particular, the CJEU identified the following US laws and orders:

  (a) Section 702 of the Foreign Intelligence Surveillance Act (50 U.S.C. § 1881a) ("**FISA 702**"); and

  (b) Executive Order 12333 ("**EO 12333**").

3. Does FISA 702 or EO 12333 impact Juniper's services?

- United States government requests under FISA 702 apply to "Electronic Communications Service Providers" which includes: (i) "electronic communications services" ("**ECS**") providers; (ii) "remote computing services" ("**RCS**") providers; and (iii) as of April 20, 2024, any other service providers with access to equipment used to transmit or store wire or electronic communications ("**SP**").
- While Juniper could be interpreted to be a provider of ECS or RCS, FISA 702 is aimed at telecommunications and other electronic communications providers, which Juniper is not. Without duplicating the detailed analysis of these definitions undertaken by publicly-available government, academic, legal, and research publications, ECS and RCS providers are generally found to provide communication services to the general public. In contrast, Juniper provides networking solutions, equipment, and software to enterprises in a business-to-business context.
- In the unlikely event that Juniper is determined to be a provider of ECS or RCS, then certain data Juniper processes may be interpreted to be within the scope of FISA 702. However, because the type of data Juniper processes and has access to is not communication data between individuals but is rather technical communication data between network devices in a business-to-business context, it is improbable that the data Juniper processes would be relevant to a government request.
- Under the April 2024 amendment to FISA 702, Juniper is unlikely to be considered an SP with respect to its provision of technical support services and any on-site services we provide to telecommunications, cloud, and enterprise customers. Juniper technical support and on-site personnel only access customer equipment and systems under the direction and supervision of Juniper's customers for the purposes of providing those services, and therefore this amendment has limited applicability to Juniper's services.

Similarly, the data that would be available to Juniper is unlikely to be relevant to the aim of FISA 702 given such information would predominantly be data between network devices in a business-to-business context, rather than the communications between individuals that are the focus of FISA 702.

- EO 12333 provides authority for US intelligence agencies to collect non-US personal data from communications and other data passed or accessible by radio, wire and other electromagnetic means, also known as "signals intelligence" information. EO 12333 does not, itself, authorize the US Government to compel any company or person to disclose data to the US Government. Any such orders must rely on another statute, such as FISA 702.
- As of the publishing date of this FAQ, Juniper has not received any FISA 702 orders, and we are not participating in any program authorized by EO 12333.

4. Does Juniper transfer data outside the EEA?

- Juniper provides technical support globally to meet customer requirements for worldwide support coverage. This provision of support services requires data, such as technical network device data, from the EEA to be transferred outside of the EEA.
- Depending on the Juniper service, customers may elect a cloud environment in an EEA-based data center and may choose to share their personal data with specific Juniper technical support personnel outside of the EEA. Juniper has data center options in locations that may include but are not limited to: Australia, Canada, Europe, Japan, United Kingdom, and the United States.

5. Can I still use Juniper's services after Schrems II?

- Schrems II affirmed the validity of SCCs provided that supplementary measures are applied to such transfers to provide for an equivalent level of protection for individuals. On June 18, 2021, the EDPB adopted recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ("**Supplemental Measures**"). See here.
- In connection with Juniper's reliance on the SCCs, Juniper has reviewed the Supplemental Measures and, where necessary, has implemented certain safeguards. For more information on those Supplemental Measures implemented, please see Question 7 of this FAQ.

6. In light of Schrems II, what is Juniper's position on government demands for data?

- Juniper will evaluate and scrutinize government demands for data and seek to appropriately narrow or challenge requests which, among other reasons, are not necessary and proportionate or are otherwise legally insufficient. We will also seek to challenge requests that prohibit notification to you. Juniper's standard practice – which predates Schrems II – is to only produce information to an agency with appropriate authority under applicable law to demand the information, and to only provide the information within the specific scope of the request. Every government request, however received, goes through this evaluation process. Juniper also employs a rigorous supplier due diligence and contracting process designed to ensure any suppliers who provide Juniper with services that will store customer data are required to abide by the requirements in this Question 6, as applicable.
- If we do receive a government request to disclose personal data, we will notify you in accordance with our obligations under our agreements with you, including the SCCs incorporated into our data processing agreement (unless we are prohibited from doing so under applicable law), to give you an opportunity to limit or prevent disclosure.

- If we are unable to notify you of such requests, we will, unless we are prohibited from doing so under applicable law, notify your applicable supervisory authority to seek feedback regarding suggested best practices or EU legal requirements on complying with the disclosure request.
- In any event, we will seek to minimize the information we disclose in response to a disclosure request to what is necessary for us to meet our obligations under applicable law.

7. What technical measures does Juniper have in place to protect customer data in its services?

- Juniper has implemented appropriate data protection and security measures throughout the company and Juniper requires its third-party suppliers to commit to high standards of data security. For example, for Juniper's Mist offerings, we encrypt device data processed as part of the service, including using HTTPS with AES-128 for communication between network devices and block level encryption with AES-256 for data at rest in the cloud service. For more information on the Supplemental Measures Juniper has implemented, please see Schedule 2 to Juniper's **Customer Data Protection and Privacy Exhibit for Juniper Products and Services**.
- The above security measures would make it improbable that any theoretical government access to customer data without our consent would result in the deciphering or meaningful disclosure of data.

8. What if I have further questions regarding Juniper's compliance with Schrems II?

- If you have further questions, please contact **privacy@juniper.net** or your Juniper account manager.

About Juniper Networks

Juniper Networks believes that connectivity is not the same as experiencing a great connection. Juniper's AI-Native Networking Platform is built from the ground up to leverage AI to deliver exceptional, highly secure, and sustainable user experiences from the edge to the data center and cloud. Additional information can be found at www.juniper.net or connect with Juniper on X (formerly Twitter), LinkedIn and Facebook.

JUNIPER NETWORKS | Driven by Experience™

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000 | Fax: +1.408.745.2100
www.juniper.net