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 our customers operate, including but not limited to the EU General Data Protection Regulation 2016/679 (the "**GDPR**"). We have closely reviewed the decision by the European Court of Justice in the "*Schrems II*" case, and as the European Commission and the US Department of Commerce engage in workable solutions to support EU-US personal data transfers, we have made it a priority to provide our customers with these Frequently Asked Questions to assist in their analysis of Juniper's processes and procedures in conducting applicable EU-US transfers of personal data.

In July 2020, the European Court of Justice (the "**CJEU**") considered whether privacy protections in US law relating to intelligence agencies' access to data meet EU legal standards. The CJEU determined that the EU-US Privacy Shield was invalid and 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. We have provided the following information to assist our customers with information relating to the CJEU's *Schrems II* decision. While Juniper does not rely on the EU-US Privacy Shield to facilitate the lawful transfer of personal data between the EU and the US, the CJEU's decision has created general legal and operational uncertainty regarding international data transfers from the EU to the US. It is important to note that the data Juniper receives is predominantly technical and related to network devices.

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

- No, Juniper does not rely on the EU-US or Swiss-US Privacy Shield to facilitate the lawful transfer of personal data between the EU or Switzerland and the US. Juniper relies on SCCs for all data transfers outside the EEA.
- While the Privacy Shield agreement has been invalidated by the *Schrems II* decision, SCCs haven't been annulled. The *Schrems II* decision does permit the use of SCCs provided the data importer implements certain supplementary measures - whether legal, technical or organisational - in order to provide adequate levels of protection that a data subject would have in the EU.

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

- The CJEU highlighted concerns it had with US surveillance laws, which it argued can cause recipients of personal data in the US 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 as concerning:

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

  and

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

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

- United States government requests under FISA apply to "electronic communications services" (ECS) providers, which is specifically defined statutorily and also includes "remote computing services" (RCS) providers. While it is conceivable that Juniper could theoretically be interpreted to be a provider of ECS or RCS, the main thrust of FISA 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, whether for free or for a fee. Juniper, however, provides networking solutions, equipment, and software to enterprises in a business-to-business context.
- In the unlikely event that Juniper cloud services are determined to be "electronic communication services" or "remote computing services," certain data Juniper processes may be interpreted to be within the scope of FISA. However, since 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, it is improbable that the data Juniper processes would be relevant to a government request.
- It is important to understand how FISA impacts both technology providers like Juniper and enterprise customers. We encourage our customers to assess their cloud service providers and take into account the nature of the data being processed and the controls the provider uses to protect such data.
- To assist customers in their analysis of FISA with respect to Juniper, as of the publishing date of this FAQ, Juniper has not received any US national security demands, including FISA orders, and we are not currently voluntarily cooperating with any program authorized by EO 12333.

4. Does Section FISA 702 or EO 12333 apply to other US cloud service providers?

- All companies in the U.S. are required to comply with applicable laws, but this does not mean that the U.S. government can leverage FISA and EO 12333 to obtain unfettered access to data processed by U.S. companies. In fact, data access laws in the U.S. are not dissimilar from those in many other countries (including those in the EU), such that any government access to data is subject to rigorous review and approval processes. Such laws also recognize the right of companies to challenge requests for data, for example because the requests may conflict with another country's laws or national interests.
- In response to *Schrems II*, the U.S. Department of Justice issued a White Paper, stating that U.S. privacy safeguards would "ensure 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." *See Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*. The Department of Justice has also explained that for most companies, the data these companies handle is of no interest to the U.S. intelligence community.

5. Does Juniper transfer data outside the EEA?

- Juniper provides technical support globally to meet customer requirements for expanded 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.
- For certain Juniper cloud services, such as Mist, Juniper has implemented its cloud environment in an EU-based data center. Mist customers may at their election discontinue sharing personal data with Juniper technical support personnel outside of the EEA. Other cloud services, such as ATP Cloud, permit customers to select the data center location they prefer between Europe, United States, Canada, or Japan.

6. Can I still use Juniper's cloud 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 November 10, 2020, the European Data Protection Board adopted recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ("Supplemental Measures"). See here.
- Juniper is actively reviewing the Supplemental Measures and, where necessary, implementing and refining safeguards as applicable. We welcome an open dialogue with customers regarding our implementation of such measures

7. 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 the customer. 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 we will 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 cloud services that will store customer data are required to abide by the requirements in this Question 7, as applicable.
- If we do receive a governmental 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 absolutely necessary for us to meet our obligations under applicable law.
- In addition to complying with our US legal obligations, we have also implemented the technical and organisational measures set out below to protect the data that you share with Juniper.

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

- We understand that data protection requires a robust and technically secured environment. Juniper has implemented appropriate data protection and security measures throughout the company and requires our third-party suppliers to commit to high standards of data security. For example, for our Mist cloud service, we encrypt device data processed as part of the service, including using HTTPS with AES-128 for communication between network devices and the Mist service and block level encryption with AES-256 for data at rest in the cloud service. Contrail Service Orchestration hosts servers in an ISO 27001-certified data center, which also provides SOC 2 attestation reports over its security controls and across multiple availability zones.

- Any theoretical government access to customer data processed by Juniper would be protected by the above security measures – which make it improbable that any government disclosure without our consent would result in the deciphering or meaningful disclosure of data.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Dr.
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: 31.0.207.125.700
Fax: 31.0.207.125.701

4000026-001-EN Jan 2021