Paragon's Data Transfer Impact Assessment

Current as of January 4, 2023

Please note that this document is for informational purposes only, and that Paragon's customers are responsible for making their own independent assessment of the information presented below. All of Paragon's obligations and liabilities to our customers are outlined in our agreements, and this document does not form part of, or modify, any agreement between Paragon and our customers.

1. **Overview**
   In July 2020, the Court of Justice of the European Union issued a decision in Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems ("Schrems II"), holding that (1) the U.S.-EU Privacy Shield program could no longer be used for data transfers to the United States, and (2) the transfer mechanisms identified in the GDPR — including the European Commission-issued Standard Contractual Clauses ("SCCs") — could only be used where the laws and practices in the data importer's country do not impinge on the protections provided by the transfer mechanism.
   As a result of the decision, organizations are required to carry out assessments of the laws and practices in the countries they transfer data to. And if you use Paragon as a vendor, that means assessing transfers to Paragon in the U.S. We put together this Data Transfer Impact Assessment to provide you with all the information you need to perform a transfer assessment of Paragon.
2. **Definitions**
   The most important terms you should know as you review this Assessment are the following:
   1. "Customer Data" means the data sent from your IT environment to Paragon for processing by the Services (e.g., app events, data flowing through workflows, etc).
   2. "Customer Personal Data" means Customer Data that consists of personal data (e.g., Logs events that include things like an individual's full name or an IP address).
   3. "Data Processing Addendum" and "DPA" mean the contract we sign with customers that governs how we process Personal Data; for instructions on how to request our DPA, please visit this page.

4. “EEA” means the European Economic Area.
5. “GDPR” means Europe’s General Data Protection Regulation.
6. “Personal Data” means data related to an identified or identifiable natural person (e.g., a full name, an IP address, or a photograph of someone).
7. “Services” means the hosted or on premise products we provide to our customers.
8. “Standard Contractual Clauses” and “SCCs” mean the European Commission-approved contracts used to safeguard Personal Data when transferred out of the EEA.
9. “Subprocessor” means a vendor that processes Customer Personal Data on Paragon’s behalf.

3. **Paragon’s Services**
   Paragon’s Services include its web-based application and workflow integration service, among others. Because these products can be used in unique ways, many kinds of data may be sent to Paragon for processing. As a result, it’s possible that you may configure and use our Services in a way that results in the collection of Personal Data, including Personal Data that is governed by data protection laws like the GDPR.
4. **Transfers of Your Personal Data**
   1. Transfer Mechanisms in General
      The GDPR prohibits the transfer of Personal Data outside of the EEA unless the transfer is made using an approved transfer mechanism: (1) the transfer is made to a country that the European Commission has determined provides an adequate level of data protection; (2) the transfer is subject to appropriate safeguards; or (3) the transfer is made in accordance with specific derogations.
      First, an organization may transfer Personal Data out of the EEA when the transfer is to a country that the European Commission has determined provides an adequate level of data protection. The European Commission maintains a list of the countries that have been deemed adequate. While the U.S. used to be on the list (scoped to the organizations who were part of the Privacy Shield program), that decision was revoked as a result of the Schrems II decision. Second, an organization may transfer Personal Data out of the EEA when the transfer is subject to appropriate safeguards under Article 46 of the GDPR. There are a few specific mechanisms that provide appropriate safeguards, the most popular of which is the European Commission-approved Standard Contractual Clauses — a form contract signed by the data exporter

and the data importer. Third, an organization may transfer Personal Data out of the EEA in specific (and limited) cases, including where the data subject (whose Personal Data will be transferred) has explicitly consented to the transfer. More information about these derogations is available in Article 49 of the GDPR.

2. Transfers to Paragon
   When choosing a hosting solution for Paragon, you may have the option of choosing where your Customer Data is hosted. For cloud hosting, all data is hosted in the US. For on-premise, it can be anywhere of your choosing. You can read more about this here on our documentation. When you select a hosting region, we commit not to host your Customer Data anywhere else.
   In order to ensure that all transfers of Personal Data to Paragon are made under a GDPR-compliant transfer mechanism, we will sign a Data Processing Addendum with you that incorporates the European Commission-approved Standard Contractual Clauses. *If you haven't yet signed a DPA with us and believe that you need one, you can request a copy from your customer success manager or from Support*.
3. Paragon's Onward Transfers
   In order to provide our best-in-class Services, including support, we may disclose your Customer Data to certain of our affiliates and trusted vendors (our Subprocessors). These onward transfers are only made as necessary to deliver our Services as outlined in our agreements with you. A full list of our current Subprocessors is maintained on our Subprocessors List. In our Subprocessors List, we identify for each Subprocessor the specific service that they provide to us, such as infrastructure provision by our cloud services providers or support ticketing systems, and each Subprocessor's location.
   Before we engage a new Subprocessor, we subject it to a rigorous vendor-review and -onboarding process to ensure that we can safely provide it with the Customer Personal Data we receive from our customers. This includes reviewing each vendor's security and privacy practices to ensure that they meet our strict requirements, as well as requiring them to sign a DPA with us that (1) provides protections for Customer Personal Data at least as protective as those in our DPA with you, and (2) includes the SCCs for any onward transfers of Customer Personal Data. After we vet a new Subprocessor and feel confident that Customer Personal Data will be fully protected when shared with the Subprocessor, we send a notice to each of our

customers who has signed a DPA so that it has an opportunity to review the new Subprocessor.

4. Analysis of the Transfer Mechanisms

   Once your transfer mechanism has been determined, you need to assess your transfers under the guidelines provided by the Court of Justice of the European Union and the European Data Protection Board. According to the European Data Protection Board, you must assess whether "there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer." To assist you with this assessment, we've provided information below related to the laws and practices in the U.S., with an emphasis on those that were of concern to the Schrems II court.

   - FISA 702

     Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702") permits a specific U.S. court to authorize the federal government to issue orders to certain types of companies in the U.S. These orders usually require companies to disclose the communications they have of certain individuals located outside of the U.S. Under FISA, these orders may only be issued to "electronic communication service providers," which includes providers of "electronic communication service[s]" and providers of "remote computing service[s]."

     We have analyzed the scope of FISA 702, and we do not believe that we are subject to government orders for communications under the statute. Specifically, based on the Services that we provide to our customers, it is our opinion that we do not constitute a provider of "electronic communication service[s]," a provider of "remote computing service[s]," or an entity that would otherwise be considered an "electronic communication service provider" that is subject to orders under FISA 702 and we believe that nature of the data we collect would not be the type that would be of the interest of any law enforcement agency. As a result, we don't believe that we would ever be in scope to receive an order under FISA 702.

   - Executive Order 12333

     Executive Order ("EO") 12333 applies to U.S. government intelligence activities, and outlines how different U.S. intelligence agencies are responsible for certain intelligence and

counterintelligence operations, including how they can collect the communications of non-U.S. individuals. According to the U.S. government, any disclosure requirement directed at companies under EO 12333 must be "authorized by statute and must be targeted at specific persons or identifiers." Moreover, "bulk collection is expressly prohibited."

We do not believe that EO 12333 introduces a substantial risk to our customers with respect to their use of the Services. As a general matter, the kinds of data that our customers send to us as part of their use of the Services would not constitute the types of communications that are relevant for the U.S. government during intelligence and counterintelligence operations — compare, for example, the content of an individual's emails with the logged events of when the individual logged into her email service provider's website (this being the type of data that could be sent to Paragon); while intelligence agencies might be interested in collecting the former, it is unlikely that they would collect the latter under EO 12333. Moreover, because we encrypt data when in transit across public networks, we believe we are at little risk of having any customer Personal Data in the clear intercepted under EO 12333.

- The CLOUD Act

The Clarifying Lawful Overseas Use of Data ("CLOUD") Act is another statute that companies may be concerned with in assessing whether they are permitted to send Personal Data to us. While the CLOUD Act broadens the U.S. government's ability to access data stored abroad, we believe that it has no effect on Paragon.

The CLOUD Act has two parts. The first allows the U.S. to enter into agreements with other countries that grant them reciprocal access to certain data stored in each country. We understand that, as of the date of this Assessment, the U.S. has not entered into any such agreement with the EU or any of its member states.The second expands the geographical scope of the Stored Communications Act ("SCA"), the federal law that allows U.S. law-enforcement agencies to require the disclosure of information held by certain organizations. Specifically, the CLOUD Act clarifies that the SCA applies to data stored outside of the U.S. But the CLOUD Act does not expand the scope of entities subject to the SCA — and the SCA only applies to

providers of “electronic communication service[s]” and providers of “remote computing service[s].”As noted in the “FISA 702” section above, we do not believe that we would constitute either a provider of “electronic communication service[s]” or a provider of “remote computing service[s]” and again the nature of our data is unlikely to be of interest to law enforcement. As a result, Paragon would not be subject to the SCA, and so the CLOUD Act’s expansion of the SCA’s geographical scope has no effect on us.

- Government Access Requests in General
  Taken together, we think it is highly unlikely that any of the features of U.S. law that the Schrems II court was worried about would apply to Paragon’s processing of your Personal Data as part of our provision of the Services. We also note that the United States and the European Union have entered into a understanding that allows for transatlantic personal data flows in compliance with European Union data protection regulations.
- Moreover, if we ever were to receive any kind of request from a governmental body requesting the Personal Data you have submitted to our Services, to the extent permitted by applicable laws, we would (1) attempt to fight or quash the request by raising nonfrivolous objections; (2) provide you with reasonable notice of the request so that you have the opportunity to seek a protective order or other appropriate remedy; (3) attempt to redirect the governmental body to request the information from you directly; and (4) if ultimately required to disclose your Personal Data to the government, limit the disclosure to the minimum amount of data legally necessary to comply with the request.

5. **Supplementary Measures**
   Even though we believe that we are technically out of scope of the laws and practices in the U.S. that caused the Schrems II court to question data transfers to the U.S., we take the privacy and security of your Personal Data seriously. In order to ensure that we meet state-of-the-art practices for privacy and security, we have implemented the following technical, contractual, and organizational measures in order to protect your Personal Data. You can review those measures on our Trust Center.
6. **Reevaluation**
   We know that the global privacy landscape is in constant flux, and that new risks are routinely uncovered. Accordingly, we do not view this as a static Assessment —

instead, we are committed to continuously analyzing our policies and practices in order to ensure that we can process Customer Personal Data in a way that complies with all applicable privacy and data protection laws. We're always willing to work with you if you have specific concerns not covered in the Assessment above. You can reach out to Paragon's privacy team, at privacy@useparagon.com.