EEA International Data Transfers FAQs

These FAQs answer some of the most common questions Datadog receives relating to how we support our customers’ sending of personal data out of the EEA in light of the Schrems II decision, and subsequent EDPB recommendations.

What customer data does Datadog have access to?

Datadog provides its customers with SaaS-based tools to collect, view, manage, and analyze a wide variety of data relating to their own computing infrastructure and software applications. Datadog customers determine what data from their IT environment are sent to the Datadog services, typically through deployment of either an API or installation of an open-source software agent. Accordingly, the only data that we have of our customers is the data that our customers choose to send to our service through the establishment of one-way data flows. Whether the data submitted to our service by our customers contains personal data is dependent on each customer’s use case. Further, we provide our customers the ability to configure our agent, which can be used to mask, filter, or obfuscate data before it reaches our service environment.

How does Datadog support its customers’ sending of data from the European Economic Area to the United States?

We have ensured that every transfer of personal data from the EEA to the U.S. has been lawfully made since the General Data Protection Regulation (GDPR) went into effect by enabling all of our customers who intend to send personal data to our service to sign data processing addenda (DPAs) that include the European Commission’s Standard Contractual Clauses (SCCs). If a customer has not already signed a DPA with us and believes that they should, they can request a copy as outlined in our online DPA.

Where does Datadog store data that is submitted to the service by its customers?

Datadog customers can choose to have their data stored in the U.S. or in the EU. Data that is stored in the EU is backed up only in EU locations.

How has the Schrems II decision impacted Datadog’s support for its customers sending of data outside of the EEA?

After the Schrems II decision invalidated the EU-U.S. Privacy Shield framework, Datadog performed a transfer assessment to ensure that we could continue to transfer personal data to the U.S. consistent with the GDPR. As part of this assessment, we reviewed our supplementary measures and onward transfers of personal data, including our transfers of customer personal data to our subprocessors.

Because Datadog has always included the SCCs in all our DPAs with customers, no changes were needed with respect to our contracts with current customers. We have also always included the SCCs in our DPAs with our subprocessors, which require that our subprocessors notify us in the event they are unable to comply with the terms of the SCCs, meaning that no changes were needed with respect to our contracts with our subprocessors. Today, all of our transfers of personal data from the EEA to the U.S. are made on the basis of the SCCs.

Can Datadog ensure that the data submitted to it by its customers never leaves the EEA?

While our customers can ensure that data stored in the EEA is never stored in another location (including the U.S.) by choosing to subscribe to our EU-hosted service instance, the data that our customers share with our service may be accessed by organizations or individuals outside of the EEA. This is necessary for two reasons. First, we utilize a number of subprocessors that operate outside of the EEA. For a full list of our subprocessors, please refer to our Subprocessor List. Second, our best-in-class support team utilizes a follow-the-sun model, whereby our customers’ data may be accessed by our support engineers from outside of the EEA.

Is Datadog subject to Section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA) and does Datadog otherwise cooperate with government requests for access to personal data?

Based on our analysis, we do not believe that we are subject to government directives under FISA § 702. Specifically, we do not believe that we are a provider of electronic communication services, a provider of remote computing services, or otherwise an entity that meets the definition of “electronic communication service provider” under 50 U.S.C. § 1881(b)(4).

Nonetheless, if we were to receive a directive under FISA § 702, we would not disclose a customer’s data unless we were required to do so to comply with the law or a binding order of a government body, and we would make reasonable efforts to redirect the government body to request that data directly from our relevant customer. Unless we were legally prohibited from doing so, we would also give the impacted customer reasonable notice of the demand to allow the customer to seek a protective order or other appropriate remedy.

Is Datadog subject to other governmental surveillance, including under Executive Order (EO) 12333, that would result in a government agency accessing customer personal data or that would otherwise prevent the enforceability of data subject rights?

EO 12333 applies to U.S. government intelligence activities and does not include any authorization to compel disclosures from companies like Datadog. Accordingly, we do not believe that EO 12333 introduces a substantial risk to our customers with respect to their use of Datadog services. Further, because we encrypt data when in transit across public networks, we believe we are at little risk of having customer personal data in the clear intercepted under EO 12333. We are not aware of any other U.S. laws that would involve the access to our customers’ instance or personal data.

What supplementary measures does Datadog have in place for international data transfers?

We have implemented a number of supplementary measures to adequately protect personal data that is transferred internationally. First, all data sent to the Datadog platform uses Transport Layer Security (TLS) with HTTP Strict Transport Security (HSTS) by default and can be configured by our customers to use TLS 1.2 where supported.

Second, we encrypt customer data, including backups, at rest using FIPS 140-2-compliant encryption standards, and we use FIPS 140-2-approved cryptographic devices for the generation, storage, and revocation of encryption keys. For more information about how we encrypt data, please refer to our Data Protection page.

Third, we rely on the principle of storage minimization to ensure that personal data is not retained for longer than is strictly necessary. For more information on our default retention periods, please refer to our Data Collection, Resolution, and Retention page.

Fourth, we enforce strict access controls to ensure that only the people who need to have access to a customer’s information have access to that customer’s information, and we log all access to customer data.