DataRobot FAQ on International Transfer of Personal Data

What is Schrems II?

Schrems II is a case that was heard before the Court of Justice of the European Union ("CJEU") that challenged the validity of the Standard Contractual Clauses ("SCCs") to provide adequate safeguards to personal data that is transferred out of the EU. On July 16, 2020, the CJEU reaffirmed that the SCCs were a valid transfer mechanism, but said that in some cases, depending on the nature of the transfer, additional supplementary measures may be required. The European Data Protection Board ("EDBP") subsequently issued guidance describing what supplementary measures might be sufficient.[1]

What is FISA 702 and EO 12333?

Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702") is a US statute that authorizes the collection, use and dissemination of electronic communications content that is stored or processed by US internet service or telecom providers by the US government for national security and foreign intelligence purposes.

Executive Order 12333 ("EO 12333") is a general directive that assigns US intelligence agencies responsibilities for different types of intelligence collection activities. Unlike FISA 702, it doesn't authorize any US government agencies to require any company to disclose data. Any such requirement must be authorized by a specific statute, such as FISA 702.

In the Schrems II decision, the CJEU found that US surveillance conducted under FISA 702 and EO 12333 didn't meet the requirement for an adequate level of protection of personal data that is required for the transfer of data under the General Data Protection Regulation ("GDPR").

How does the Schrems II ruling affect DataRobot?

DataRobot is unlikely to be targeted by FISA 702. It applies to "electronic communications service providers" which are commonly understood to be internet service and storage providers. The US government has confirmed that "most US companies do not deal in data that is of any interest to US intelligence agencies, and have no grounds to believe they do. They are not engaged in data transfers that present the type of risks to privacy that appear to have concerned the ECJ in Schrems II."[2]

[1] Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
[2] Information on US Privacy Safeguards Relevant to SCCs and other EU Legal Bases for EU-US Data Transfers after Schrems II, September 2020.

In line with the US government guidance, the data processed within the DataRobot product is unlikely to be of interest to US intelligence agencies. FISA 702 is only authorized for the collection of foreign intelligence that is important to US national security.

What actions has DataRobot taken in response to Schrems II?

In response to the Schrems II ruling and the resulting EDBP guidance, we performed a review of its data transfers and the controls in place to protect our customers' personal data. We have performed transfer impact assessments for all transfers of customer data to our subprocessors and to DataRobot entities located in third countries without adequacy agreements.

What supplementary measures does DataRobot have in place to protect personal data transferred from the EU?

The EDBP identified three types of supplementary measures that enable transfer mechanisms to provide equivalent protection to what the data would receive in the EU – technical, contractual, and organizational. DataRobot has the following supplementary measures in place:

Technical Measures

Our Information Security Policy details the technical measures that are in place to protect customer data in our managed cloud. This includes:

- **Encryption.** All data residing in, or transiting to or from the DataRobot managed cloud product, is encrypted. Data in transit is encrypted using HTTP (TLS1.2/AES-256). Data at rest is encrypted with SSE-S3 object level data encryption (AES-256).
- **Logging and Monitoring.** We maintain logs of administrator and operator activity and data recovery events.
- **Access Management.** We monitor repeated failed login attempts, and will lock out a user account after five failed attempts[3]. Two factor authentication is available for user accounts, as well as unique user API tokens and Single Sign On (SSO) authentication.
- **Password Management.** Users must set complex passwords with length, character complexity, and non-repeatability requirements. Passwords are encrypted and salted using PBKDF2 (SHA512+128bit salt).
- **Secure Development Lifecycle.** We have policies for secure development and change control and follow industry best practices for change management. For each major release, static and dynamic analysis scans and container environment scans are performed, and any weaknesses found are remediated as deemed necessary.

[3] For all DataRobot software except for Zepl.

- **Penetration Testing**. On an annual basis, we engage a third party to perform pen tests to detect corporate infrastructure and network vulnerabilities. Any found vulnerabilities are remediated as deemed necessary.

Contractual Measures

Our Master Subscription Agreement automatically incorporates an Information Security Policy and a Data Processing Policy to protect any personal data that a customer might upload to the managed cloud. The Data Processing Policy is aligned to the Article 28 Model Clauses published by the European Commission for the transfer of data to a processor, and includes GDPR, UK GDPR, and CCPA compliant provisions. It also includes the new version of the EU Standard Contractual Clauses for transferring personal data to third countries, published on June 4, 2021, as well as the older version of the Standard Contractual Clauses adopted under Data Protection Directive 95/96/EC for transfers from the UK.

We enter into Data Protection Agreements and Standard Contractual Clauses with all subprocessors that impose substantially the same data protection obligations as those imposed on us.

Organizational

- **Data Residency.** For most DataRobot products on our managed cloud, customers located in the EU or in countries with an adequacy decision are hosted on AWS servers located in Ireland.[4]
- **Government Access Requests.** We have published a Government Data Request Policy that describes how any requests from government entities or law enforcement officials will be managed. We publish bi-annual Transparency Reports but to date have never received a government access request.
- **Internationally recognized standards.** We have achieved ISO27001 certification for information security, as well as SOC 2 Type 2 certification for the management of customer data safeguards based on security, availability, confidentiality, and privacy.

Where is customer data processed?

Customer data uploaded to the DataRobot managed cloud is hosted on AWS servers located in either the United States, or Ireland. Customers located in the EU or in countries with an adequacy decision are hosted on the Ireland installation.[5]

Customers may also send data to our Support and Success teams for help in troubleshooting issues or optimizing their AI predictive models. In that scenario, customers may use either a designated Support Portal AWS S3 bucket, Zendesk support ticket, or Box folder to provide their data to our employees. In each of those cases the data is transferred to the US. Alternatively and more preferably, customers can provide remote access to enable us to assist if necessary.

[4] For all DataRobot software except for Zepl and Algorithmia.
[5] For all DataRobot software except for Zepl and Algorithmia.

As a global company, we have employees worldwide to provide round the clock support and product maintenance to our customers. As discussed above, customers may specifically request assistance from our Support and Success teams, in which case data may also be shared with our Engineering team to help troubleshoot. Our employees may be located in any of our subsidiary countries that are listed here.

What subprocessors does DataRobot use?

Our subprocessor list is available on our website. Customers can subscribe to receive updates when a new subprocessor is added.

Where can I get more information on DataRobot's processing of personal data?

Please visit our Trust Center to learn more about how we are working to keep our customers' data private and secured. From there, you can also request a copy of our Trust Package that contains further details and evidence of our security certifications. If you have any other questions, please contact your DataRobot representative or email privacy@datarobot.com.