November 15, 2020

FAQ for EU Data Transfers to the US and Applicable US Laws

In light of the Schrems II decision in July 2020, Auth0 understands that some of its European customers may have questions surrounding personal data transfers to the US via the Auth0 Platform, particularly the applicability of certain US surveillance laws, such as the Foreign Intelligence Surveillance Act ("**FISA**") and Executive Order 12333 ("**EO 12333**") to access such personal data in the US. We would like to proactively answer some of those questions and provide reassurances to our EU customers about the personal data they process via the Auth0 Platform.

When is it possible for EU Personal Data to be transferred to the US via the Auth0 Platform?

There are two very limited circumstances in which Auth0 may transfer a customer's EU personal data to the US: (1) if a customer includes personal data in a request or communications with Auth0 for customer support or (2) on a temporary, ephemeral basis when public cloud customers use our management dashboard tool. For more detailed information, please review our "EU Customer Toolkit: International Data Transfers" document found on the Auth0 Legal page under the "Resources for Privacy and Data Protection" sidebar.

Aside from those two circumstances, and assuming that a customer selects the AWS "EU region" when setting up its Auth0 tenant, Auth0 will only store and process the customer's personal data in the European Union.

What Legal Basis is there to Transfer EU data to the US via the Auth0 Platform in those Limited Circumstances?

Even though the US-EU Privacy Shield Framework has been invalidated by Schrems II, the European Commission's Standard Contractual Clauses ("**SCCs**") are contractual terms that have been pre-approved by the European Commission and still serve as a legal basis to transfer personal data outside of the EU/EEA. SCCs are included as a data transfer mechanism in the Data Processing Addendum ("**DPA**") that Auth0 offers to customers. We incorporate the SCCs into our subscription agreement when you sign our DPA in order to enable safe and legal transfers of personal data outside of the EU.

Does Auth0 Use Technical and Organizational Measures to Safeguard Personal Data Transferred to US?

Auth0 has implemented a variety of technical and organizational measures to safeguard EU personal data that is transferred to the United States, including the execution of the SCCs and encryption of your data while in transit and at rest. You can find more details on these technical and organizational measures in our "EU Customer Toolkit: International Data Transfers" document on the Auth0 Legal page under the "Privacy and Data Protection" sidebar.

How does Auth0 Respond to Government and other Third Party Requests for Customer Data?

Auth0 has established and is committed to complying with certain principles when responding to government and other third-party requests for customers' personal data. These principles are outlined in our "Principles Regarding Responding to Third-Party Requests for Customer Data" document found on the Auth0 Legal page under the "Resources for Privacy and Data Protection" sidebar.

Has Auth0 ever received an Information Request from the US Government?

No. As of the publication date of this document, Auth0 has not received any user information requests from the US Government. We also now publish a Transparency Report and will update that report on a yearly basis. That report can be found on the Auth0 Legal page under the "Resources for Privacy and Data Protection" sidebar.

What About US Laws that Could Allow the US Government to Access EU Personal Data Transferred to the US?

FISA 702

What is Section 702 of FISA?

Section 702 of FISA ("**FISA 702**") outlines the specific legal procedures that US government agencies must follow in order to compel assistance from electronic service communication providers ("**ESCPs**") in the collection of foreign intelligence information from non-U.S. persons located outside of the United States. For information on the legal process that is required for a US government agency to establish a FISA 702 surveillance program, please review the DNI's Section 702 Overview.

The US government has engaged in two foreign surveillance programs under FISA 702, both of which were raised as specific concerns by the European Court of Justice ("**ECJ**") when invalidating the EU-US Privacy Shield framework:

- PRISM or downstream surveillance, which involves the direct 'downstream' collection of information from US online providers that provide individual accounts; and
- Upstream surveillance, which involves the indirect 'upstream' collection of information via US telecommunications providers that provide the backbone of the internet.

Is it likely for Auth0 to receive a FISA 702 request for Customer Data in the US?

Auth0 may technically be considered as an ESCP and therefore theoretically in scope of FISA 702. However, given the two limited circumstances in which Auth0 transfers EU personal data to the US described above, **we believe it is unlikely that Auth0 would receive a request under FISA 702,** primarily because this kind of data is only temporarily stored in the US, and/or is not the kind of data that we believe would be relevant to US foreign intelligence activities.

The US government must restrict information collection under FISA 702 to **only what is required for foreign intelligence purposes**. The personal data processed by Auth0 for its customers is unlikely to be of any interest to US intelligence agencies. As highlighted by the US government in a white paper published in September 2020, most companies "do not deal in data that is of any interest to U.S. intelligence agencies, and have no grounds to believe they do."

Is individual redress available for FISA 702 violations?

Yes. As part of its reasoning for invalidating the EU-US Privacy Shield framework, the ECJ expressed concerns over the lack of individual redress for FISA 702 violations. However, individuals (including EU citizens) do have redress under the following US statutes for FISA violations:

- Section 1810 of FISA – allows an individual to seek compensatory damages, punitive damages and attorneys' fees.
- Section 2712 of the Electronic Communications Privacy Act – allows an individual to seek compensatory damages and attorneys' fees.

- Section 702 of the Administrative Procedure Act – allows an individual to challenge unlawful government access to personal data, including under FISA.

EO 12333

What is Executive Order 12333?

EO 12333 was raised as a concern by the ECJ when invalidating the Privacy Shield Framework. EO 12333 is the foundational authority for organizing US intelligence activities and specifies the circumstances, parameters and principles under which different US intelligence agencies can engage in foreign intelligence surveillance **outside of the US**. Unlike FISA 702, EO 12333 does not authorize the US government to require any company to disclose data, though it may be used to authorize clandestine intelligence activities involving overseas access to data without the involvement of the company in question.

Can the US Government compel Auth0 to disclose EU Personal Data in the US under EO 12333?

No. Under EO 12333, the **US government does not have the ability to compel Auth0 to assist in intelligence surveillance.** Under US law, any government information request to a company for intelligence purposes must be authorized by FISA or a national security letter statute. As a result, Auth0 cannot be ordered by the US government to participate in a bulk surveillance program under EO 12333, nor would Auth0 provide such assistance voluntarily.