Auth0

November 15, 2020

EU Customer Toolkit: International Data Transfers

Where is your data stored and processed?

General position:

- Personal data input into the Auth0 platform by the customer is primarily stored and processed in the AWS region selected by the customer when they create an Auth0 tenant.

- Auth0's European customers are able to select the AWS EU region, which has a primary data center in Frankfurt (Germany) with failover to a second data center in Dublin (Republic of Ireland). Aside from the limited exceptions outlined below, if a customer selects the EU region, then all processing of personal data by Auth0 will take place within the EU.

Exceptions:

(1) Use of the Auth0 Management Dashboard: For public cloud customers, Auth0 may temporarily process tenant data in the US for display on the Auth0 Management Dashboard. Dashboard web servers are located in the US. This data is not automatically transferred but is only served up when the Customer's dashboard administrator requests it for viewing. When this occurs, the data itself is ephemeral, is not permanently stored on our systems, is encrypted during transit, and is only used to display information on the dashboard to the requesting customer administrator.

This data can include any information that can be viewed through the Auth0 Management Dashboard, which typically includes the user's e-mail address or other UID and basic metadata about that user, such as creation date, last login time, user agent, and the identity provider used. The dashboard exception does not apply to Private Cloud. For customers on Auth0's private cloud deployment all dashboard processing occurs within the AWS region the customer has selected for its tenant for private cloud customers e.g. if the customer selects the EU region, then dashboard processing will remain in the EU.

(2) Customer Support Operations: If a customer includes personal data in a support ticket, then this may be viewed by Auth0 support personnel outside the EU. Also, In order to resolve a support ticket Auth0 personnel may review activity logs to help understand the underlying error. Personal data in those logs typically consists of a user ID (e.g., e-mail) and IP addresses that are voluntarily stored by the customer in Auth0's database using the user and application metadata fields. There is no need for customers to include user personal data in their support tickets.

When would Auth0 personnel access and view customers' personal data?

- Access to logs for support purposes: Auth0 minimizes its personnel's access to personal data processed with the Auth0 platform. However, Auth0 may occasionally access and view personal data to resolve support issues. For example, Auth0 personnel may need to review logs to examine why user X (usually an email address or other uid) was unable to authenticate from IP address Y to IP address Z. If resolution of the issue requires escalation, then the logs may also be viewed by other members of the support team, or by members of the applicable engineering teams.

- Access to logs for security purposes: Member's of Auth0's security team may also require access to logs to investigate and address security issues. If log data needs to be analysed at scale, then selected members of Auth0's data team may also be engaged.

Safeguarding Access: Auth0 Controls

- Auth0 logs access to customer personal data by Auth0 personnel. Access privileges are allocated by the Auth0 security team, operated under the principle of least privilege, and reviewed quarterly. All Auth0 employees are subject to criminal and background checks.

What safeguards does Auth0 have in place to protect customer data when transferred from the AWS region selected by a customer?

Legal Safeguards for transfers of personal data from the EEA and Switzerland: EU Model Clauses apply

European Union

On July 16, 2020 in the so-called *Schrems II* decision, the European Court of Justice (ECJ) invalidated the EU-US Privacy Shield framework, which was a safeguard relied upon by many companies (like Auth0) when transferring personal data from the EEA to the United States.

Although Auth0 relied on the Privacy Shield framework, we'd anticipated and planned for its possible invalidation. As a result our then-current version of the Auth0 DPA automatically defaulted to the Standard Contractual Clauses in ("SCCs" or "Model Clauses") when *Schrems II* occurred, which is another safeguard approved by the European Commission with respect to EU-US personal data transfers.

Following the Schrems II decision, we updated our DPA to include a signed set of SCCs. A pre-signed version of the new Auth0 DPA is available at www.auth0.com/legal together with a helpful reviewer's guide.

Switzerland

Although not a member of the EU, Switzerland had its own version of Privacy Shield that applied specifically to transfers of personal data from Switzerland to the US. Following *Schrems II*, the Swiss Data Privacy Regulator (FDPIC) followed the position of the ECJ and invalidated this Swiss-US Privacy Shield regime, so that it could no longer be used to transfer personnel from Switzerland to the US. The FDPIC also followed the ECJ by reaffirming the validity of SCCs as an approved mechanism for such transfers, and will be covered by our new previous and current form DPA (as outlined above).

Technical Safeguards:

Data in transit: Auth0 applies Internet Engineering Task Force (IETF) encryption standard TLS 1.2 to all data that it transfers on behalf of customers. Auth0 retains control of the decrypt key for such data in transit. Customer data being processed in the US or otherwise transferred by Auth0 from the AWS region in which the customer's Auth0 tenant is hosted to another location is subject to this encryption standard.

Data at rest: Auth0 applies encryption standard AES 256 to all customer data it holds at rest on the Auth0 platform. This encryption standard also applies to log data processed in connection with support tickets (but not the support tickets themselves) and dashboard data stored in cache (prior to deletion). Reminder: there is no need for customers to include user personal data in their Auth0 support tickets.

What additional encryption controls do Auth0 customers have?

The Auth0 platform is extensible when it comes to the encryption architecture it can integrate with on the customer end. Auth0 platform functionality allows customers to structure their Auth0 services with a number of complementary measures to ensure a more more robust encryption framework:

- Auth0 allows its customers to configure its Auth0 services so that its Administrative Users are prevented from using a lower standard than TLS 1.2 in respect to the customer's interoperability code integrating with the Auth0 platform. This allows customers to set a high encryption baseline standard for its own interoperability code.

- Auth0 automatically configures its services so that certain customer data fields are subject to additional encryption using unique customer keys. This enhanced encryption is applied to customer rules, signing keys, enterprise connectors and end user passwords. The AES-256 encryption standard is used with the unique customer keys stored in a Key Management System (KMS).

- Customers can choose to apply their own private encryption standards to data before it is uploaded to the Auth0 platform. This would mean that even if Auth0 or a third party directing Auth0 wanted to access such customer data, it would only be able to access encrypted data for which it does not control the decryption keys.