Transfers of EU Personal Data to the Okta Service

Published: July 16, 2020

This document is provided for informational purposes only. It is not intended to provide legal advice. Please consult with your own legal counsel to determine how this applies to your specific situation. This information is provided as of the date of document publication and may not account for changes after the date of publication. Please visit Okta's Trust and Compliance website for the latest information.

This document provides information about transfers of EU personal data to the Okta Service in light of the July 16, 2020 decision of the Court of Justice of the European Union ("CJEU"). The CJEU confirmed the validity of the European Commission's Standard Contractual Clauses ("SCCs") as a legal mechanism for the transfer of EU personal data, but invalidated the EU-US Privacy Shield framework. This means that organizations may no longer rely on the EU-US Privacy Shield framework to transfer EU personal data to the US. However, Okta's customers may continue to use our services, relying on the SCCs, which are already included in our Data Processing Addendum. Okta has never self-certified to the now-invalidated Privacy Shield framework.

What Was this Case About?

The case was about whether the European Commission's Standard Contractual Clauses ("SCCs") are a lawful mechanism for transferring personal data outside of the EU. The Court of Justice of the European Union ("CJEU") also considered the validity of the EU-US Privacy Shield framework. Under European data protection law, organizations that transfer personal data outside of the EU must have a legal basis to ensure the continued protection of such data, and both the EU-US Privacy Shield framework and SCCs were considered legal bases in which to transfer such data.

- The EU-US Privacy Shield framework is an agreement between the European Commission and the US Department of Commerce and requires registered organizations to adhere to EU data protection requirements when receiving EU personal data.
- The SCCs are template contracts offered by the European Commission and entered into between the organization exporting personal data from the EU and the organization importing personal data from the EU, and similarly requires the organization importing personal data to adhere to EU data protection requirements.

What Was the Decision?

The CJEU **confirmed the validity of the SCCs** as a legal mechanism for the transfer of EU personal data, but **invalidated the EU-US Privacy Shield framework**. Okta's customers may continue to use the Okta Service by relying on the SCCs, which are already included in our Data Processing Addendum. Although the CJEU continues to consider the SCCs as valid, they opined that organizations relying on SCCs should conduct diligence to help ensure that all parties are in compliance with their respective obligations under EU data protection law, including with respect to any access by government authorities.

How Does the CJEU's Decision Impact Okta's Customers?

For most customers, no action is needed to comply with the CJEU's decision. Okta already relies on the European Commission's Standard Contractual Clauses ("SCCs") as its legal mechanism to transfer personal data outside of the EU, and the SCCs are included in our Data Processing Addendum. Thus, customers do not need to take any additional actions unless they revised our Data Processing Addendum to remove the SCCs. We encourage these customers to sign and return our latest Data Processing Addendum. If you are unsure if you have a Data Processing Addendum executed with Okta, please reach out to your Account Executive.

Furthermore, Okta's Trust and Compliance website provides many resources to assist our customers in performing diligence regarding compliance with EU data protection law, including our Data Processing Addendum, Security and Privacy Documentation, and Sub-processor Information.

Where is Customer Data Located?

Please visit our Trust and Compliance website to learn more about how we process Customer Data. Specifically, our Sub-processor Information addresses where data centers hosting Customer Data are located.

How Does Okta Handle Government Requests to Access Customer Data?

Okta will follow its Law Enforcement Data Request Policy (available via our Trust & Compliance website) if it receives a Customer Data request from a law enforcement or a government agency. In general, Okta will only disclose Customer Data in limited circumstances and only if required by law. Before Okta discloses Customer Data for such a request, it will first attempt to notify its customer and allow them to intervene.