GUNDERSON DETTMER

Privacy Alert: EU-U.S. Privacy Shield Is Invalidated in Landmark European Court of Justice Decision

Insights
July 17, 2020

What now? In the landmark *Schrems II* decision, the European Court of Justice invalidates the Privacy Shield; upholds the Standard Contractual Clauses (but only with additional scrutiny and safeguards).

Yesterday's Schrems II *decision, which invalidated the U.S.-EU Privacy Shield Framework and added complexity to the use of Standard Contractual Clauses, has major implications for international data transfers.*

Refresh: What is the meaning of the Privacy Shield and Standard Contractual Clauses?

The EU General Data Protection Regulation (GDPR) restricts transfers of EU personal data to a recipient outside the EU, unless the transfer is covered by an adequacy decision by the European Commission or a compliance mechanism set forth in the GDPR. To date, the most commonly used compliance mechanisms for transfers from the EU to the U.S. have been (i) participation in the EU-U.S. Privacy Shield Framework, and (ii) use of the Standard Contractual Clauses (SCCs), both of which were open to challenge in the *Schrems II* case.

What happened?

On July 16, 2020, the Court of Justice of the European Union (CJEU) issued its long awaited decision in the case of *Data Protection Commissioner v. Facebook Ireland*

Limited, Maximillian Schrems (Case C-311/18) ("*Schrems II*"). The *Schrems II* case follows the 2015 *Schrems* case which led to the invalidation of the Safe Harbor Program (the predecessor to the Privacy Shield).

In *Schrems II*, the CJEU was asked to consider whether law and practice in the U.S. relating to access to EU personal data by intelligence services should mean that either, or both, of the SCCs and Privacy Shield should be invalidated. In what many saw as a surprise twist, the CJEU decision invalidated the EU-U.S. Privacy Shield framework for data transfers, but upheld the validity of the SCCs as a transfer mechanism for exports of personal data from the EU (however, with additional scrutiny and safeguards, as further described below). ***As a result, most companies transferring EU personal data to jurisdictions outside the EU (including U.S.-based companies receiving EU personal data from customers or end users) will need to revisit the mechanism they use to comply with GDPR.***

What does this mean for companies using the Privacy Shield?

As of July 16, 2020, the Privacy Shield is no longer a valid compliance mechanism for exports of EU personal data to the U.S. under the GDPR. However, the U.S. Department of Commerce, the agency tasked with the administration of the Privacy Shield, promptly issued a statement confirming that it will continue to administer the Privacy Shield program, including processing applications for self-certification and re-certification, and maintaining the Privacy Shield List. The U.S. Department of Commerce also confirmed that the decision does not relieve participating organizations of their Privacy Shield obligations, which are enforceable by the Federal Trade Commission as binding public commitments under the program. Therefore, in the near term, participating companies are advised to continue to honor their commitments under the Privacy Shield program while they evaluate alternative mechanisms. If you decide to withdraw from the Privacy Shield or let your certification lapse, you will need to remove all references to the Privacy Shield in your privacy policy and other public documentation and materials.

If you are a Privacy Shield certified company, we recommend that you consult with your Gunderson Dettmer attorney to explore alternative compliance options. For companies receiving EU personal data from an exporting controller in the EU, consider using the SCCs instead of the Privacy Shield, but note that use of the SCCs is more complex following the *Schrems II* decision, and you may need to amend your current Data Processing Agreements (DPAs).

If you are a consumer-facing company which receives personal data directly from end users, for the time being, there may be no feasible way to comply with GDPR for transfers of data to the U.S. If you do not have an EU subsidiary, the SCCs may not

be available since there is no exporting company in the EU with which to contract. A global compliance mechanism such as the Binding Corporate Rules is a possibility, although it can be expensive and time-consuming program to implement. Relying on GDPR derogations such as consent or necessity for contract may also be possible, but we recommend that you consult with your attorney and approach these derogations with caution, since they are narrowly applied and generally not favored by EU regulators for large scale or routine transfers of personal data.

What is the impact on companies using the SCCs?

The CJEU decision did not invalidate the SCCs as a compliance mechanism. However, following the judgment, use of the SCCs will require greater scrutiny, self-assessment and documentation. Companies will need to assess transfers on a case-by-case basis according to the level of risk and sensitivity of the data, as well as the level of protection (including the risk of surveillance) for the data in the recipient country. Additional safeguards may be required.

Data importers may be required to provide additional confirmation of their ability to safeguard data, and we expect to see expanded contractual and technical security requirements. In some cases, the conclusion may be to keep the data within the EU. Note that the "new" SCC requirements apply not only to transfers from the EU to the U.S., but to all transfers to a jurisdiction outside the EU under the SCCs. ***As always under the GDPR, documentation of your processes, procedures and decisions is important*.**

The current versions of the SCCs pre-date the GDPR and are due for an update, which we expect to see now that the *Schrems II* decision has been finalized. Once the European Commission issues and endorses new SCCs, companies will need to update their DPAs to include the new SCCs.

Was the Swiss-U.S. Privacy Shield Framework impacted?

Switzerland is not required to follow judgments of the CJEU, and currently the Swiss-U.S. Privacy Shield Framework remains valid. However, Switzerland follows the EU closely on data protection matters, and we expect to see a renegotiation of the Swiss-U.S. Privacy Shield Framework if and when the EU-U.S. Privacy Shield is renegotiated or replaced.

What are some steps companies should take now?

At a minimum, we recommend that all companies who process EU personal data in a non-EU jurisdiction (whether as a controller or as a processor on behalf of your

customers) take the following steps:

1. **Evaluate your data collection and data flows**: Revisit your GDPR processing records and assess what types of data you collect and process, and how and where data is transferred. It is now more important than ever to map which jurisdictions you transfer data to, and to assess the sensitivity of the data and the risk of surveillance in each non-EU jurisdiction. If you are a U.S.-based processor and receive data from EU customers, prepare to answer detailed questions from your customers on these matters.

2. **Consider alternative compliance mechanisms if you currently rely on the Privacy Shield**. If you are a Privacy Shield certified company and you can change your compliance mechanism to using the SCCs, we recommend that you do so. If you are a consumer-facing company, assess with your attorney whether an alternative compliance mechanism or derogation is available.

3. **Consider whether DPA amendments and additional safeguards are needed if you rely on the SCCs**. Review your DPAs with your customers and vendors. If you are moving from the Privacy Shield to the SCCs, you will likely need to amend your DPAs. Also consider whether your customers will require additional assurances and safeguards from you to use the SCCs as a transfer mechanism.

What happens next?

There are currently more than 5,400 companies certified under the Privacy Shield, and the *Schrems II* decision has major ramifications for transatlantic trade. We expect the U.S. Department of Commerce to promptly engage in discussions with its European Commission counterparts to assess next steps and discuss an updated tool (a Privacy Shield 2.0?) for compliance. However, as we saw after the Safe Harbor invalidation, negotiating and implementing a new compliance tool is a complex, politically sensitive and lengthy process. We also expect to see further guidance from EU data protection regulators and the European Data Protection Board. As always, we are following these developments closely and will keep our clients updated.

Related People

Anna C. Westfelt
PARTNER
P +1 650 463 5367

Katherine S. Gardner
PARTNER
P +1 212 430 3188

Featured Insights

CLIENT NEWS

Brazilian Carbon Capture Company Mombak Announces $30M Financing

CLIENT NEWS

Africa B2B OmniRetail Announces $20M Financing

CLIENT NEWS

Glacier Announces Series A Financing to Expand Robot Recycling Fleet

CLIENT NEWS

Dataminr Announces $100M Investment Led by Fortress Investment Group

CLIENT NEWS

Omnidian Announces $87M Series C for Renewable Energy Performance

INSIGHTS

Splitting the Pie: How Savvy Founders Divide Ownership and Navigate Other Founder Equity Decisions

CLIENT NEWS

Chainguard Announces $356 Million Series D Led by Kleiner Perkins and IVP

INSIGHTS

Client Insight: California AI Transparency Act

INSIGHTS

Client Insight: Prepare for BE-10 Benchmark Survey of US Direct Investment Abroad

INSIGHTS

Tech Brew Interviews Aaron Rubin in “Where the legal battle stands around copyright and AI training”

CLIENT NEWS

Latin America Fintech Belvo Announces $15M Funding

INSIGHTS

Legal 500 Country Comparative Guides 2025: Venture Capital (Singapore)