

**Featured Professionals**

Sten-Erik Hoidal, CIPP

**Related Services**Data Protection &  
Cybersecurity

Technology &amp; Data

## Personal Data Drama—EU's Highest Court Invalidates EU-U.S. Privacy Shield

**Legal Update**

07.20.2020

By Sten-Erik Hoidal

The European Union's sweeping privacy law, the General Data Protection Regulation (GDPR), prohibits transfers of personal data to the United States unless the company transferring the data has provided legally-appropriate safeguards. One mechanism that many companies—over 5,000 in total—have relied upon to safeguard such transfers is the EU-U.S. Privacy Shield framework (the Privacy Shield). That safeguard is no longer valid.

On July 16, the Court of Justice for the European Union (CJEU) issued a decision in *Data Protection Commission v. Facebook Ireland and Maximilian Schrems* invalidating the Privacy Shield and prohibiting further transfers under the Privacy Shield, effective immediately. This leaves many companies scrambling to implement alternative mechanisms to safeguard personal data transfers to the U.S.

The CJEU's decision is based on concerns about the impact of U.S. government surveillance programs on the privacy of EU residents' personal data. Specifically, the CJEU found:

- the access and use of personal data by the U.S. government through surveillance programs were not restricted in a way that comports with EU law; and
- EU residents lack actionable judicial redress as to personal data accessed through such programs.

The most common mechanism used to safeguard such transfers—standard contractual clauses approved by the European Commission (SCCs)—were not entirely unscathed by the decision. While the CJEU upheld SCCs as a valid mechanism to safeguard personal data transfers from the EU, it indicated that companies should examine on a case-by-case basis whether the law in the country to which the personal data is exported (e.g., the U.S.) ensures adequate protection of personal data consistent with EU law. If protection is inadequate, companies should implement additional safeguards for the transfer or suspend the transfer.

# Personal Data Drama—EU’s Highest Court Invalidates EU-U.S. Privacy Shield

For its part, the U.S. Department of Commerce decried the ruling. Secretary Wilbur Ross commented the U.S. is “deeply disappointed” by the ruling, but it will remain in close contact with the European Commission and hopes “to limit the negative consequences to the \$7.1 trillion (trans-Atlantic) economic relationship that is so vital to our respective citizens, companies and economies.”

The consequences of this decision are just starting to be felt by U.S. companies. In the near term, there are three practical implications for U.S. businesses.

- First, businesses that directly rely on the Privacy Shield need to find an alternative mechanism for personal data transfers from the EU. There is no grace period in the decision, so alternative mechanisms must be implemented as soon as possible. Potential mechanisms could include SCCs, binding corporate rules for intra-company transfers, or the narrow derogations available under Article 49 of the GDPR.
- Second, businesses using third-party vendors to manage data transfers that rely on the Privacy Shield need to understand what alternative mechanism the vendor will put in place to safeguard the transfers.
- Third, businesses that receive personal data in the U.S. through SCCs can expect increased scrutiny from transferring entities in the EU. To that end, U.S. businesses should carefully consider whether the personal data they receive from the EU is subject to the surveillance concerns flagged by the CJEU and, if so, begin identifying additional safeguards to address the concerns (e.g., encryption of data in transit).

We will continue to monitor the impact of this decision for our clients and will provide further updates and guidance over the coming weeks and months.