Privacy Alert
July 2020

EU Court Invalidates EU-U.S. Privacy Shield for Data Transfers

Key Takeaways

- The EU-U.S. Privacy Shield Framework is no longer a valid mechanism for transferring personal data from the European Union to the United States.
- Standard Contractual Clauses remain a valid transfer mechanism for the time being, but their continued validity for U.S. transfers also may be in doubt.
- European data exporters and U.S. data importers that had relied on the Privacy Shield as their transfer mechanism should revisit their processes for transatlantic data flows, including reviewing and updating any contracts related to data transfers to the U.S.

The Court of Justice of the European Union (CJEU) issued a ruling July 16 that struck down the EU-U.S. Privacy Shield framework as a mechanism for transferring personal data from the European Union to the U.S. In that same decision on Case C-311/18 (also known as *Schrems II*), the CJEU also upheld the validity of the European Commission's Standard Contractual Clauses (SCCs) as a valid transfer mechanism of personal data outside the EU.

The EU's General Data Protection Regulation (GDPR) is intended to guarantee respect for private and family life, personal data protection and the right to effective judicial protection. According to the CJEU's holding, U.S. surveillance programs are incompatible with the GDPR's privacy guarantees for EU data subjects. The CJEU held that U.S. surveillance programs are not limited in a way that would prevent interference with the fundamental rights of data subjects whose personal data is transferred to the U.S. To the contrary, the CJEU held that the U.S. government's broad powers to access personal data violate the GDPR principle of proportionality, because U.S. surveillance programs are not limited to what is "strictly necessary."

The GDPR also requires that data subjects be granted the ability to seek to legally enforce their privacy rights. In the view of the CJEU, however, the Ombudsperson mechanism of the Privacy Shield does not meet the requirements of the GDPR that EU data subjects be given the ability to bring a cause of action before a judicial body to guarantee their privacy rights. Notably, the *Schrems II* ruling holds that the U.S. Ombudsperson is not sufficiently independent and cannot adopt decisions that are binding on U.S. intelligence services. As a result, the Privacy Shield does not provide EU data subjects with an effective means to challenge the use of their personal data by U.S. intelligence services or to obtain access to, rectification of or deletion of their data. For these reasons, the CJEU struck down the Privacy Shield.

On the other hand, the CJEU upheld SCCs as a valid transfer mechanism of personal data. The court held that the SCCs should not be invalidated by the mere fact that their requirements and remedies are contractual rather than regulatory in nature. What saves the SCCs, according to the *Schrems II* decision, is that they obligate

the data exporter (i.e., the EU-based controller) to verify prior to making any transfer that the importing country maintains a satisfactory level of protection. Likewise, the data importer (i.e., the non-EU recipient of personal data) is obligated to notify the exporter if it is unable to comply with the SCCs, which would require the suspension of data transfers. Together, these contractual provisions of the SCCs create effective mechanisms to ensure compliance with the level of protection required by the GDPR. The CJEU places a heavy burden on data exporters wishing to use SCCs, however: data exporters must consider the law and practice of the country to which data will be transferred, especially if public authorities may have access to the data. Additional safeguards beyond the SCCs may be required, and for data transfers to the U.S., more thought may need to be given to what those additional safeguards are and how they will be documented.

What Should Your Organization Do Now?

The CJEU's ruling will impact any organization involved in data flows from Europe to the U.S., but the impact may be especially pronounced for adtech companies engaged in data processing via web cookies, since separate contracts are not usually executed in these arrangements. Rather, transatlantic data flows in the adtech context are often legitimized by relying on the Privacy Shield.

Whether they are data exporters from Europe or data importers in the U.S., organizations should immediately review their data transfer operations at all levels and stages. This requires data mapping and an inventory of all client/partner/vendor relationships involving transatlantic data flows (including a review of the contracts in place to formalize those relationships).

Organizations that have been relying on the Privacy Shield for personal data transfers from the EU to the U.S. should immediately suspend these transfers in order to avoid potential fines from EU data protection authorities. Once those data flows are suspended, organizations should work as quickly as possible to identify an alternative data transfer mechanism under which transfers of personal data to the U.S. can resume. The best alternative transfer mechanism might be SCCs in many instances, but for certain intracompany transfers, Binding Corporate Rules also may be an option. It is possible that organizations may be able to rely on certain GDPR derogations under specific circumstances for necessary data transfers.

Although SCCs remain valid after the *Schrems II* decision, organizations that currently rely on them for their data transfers are not entirely in the clear. Organizations should very closely consider whether the data arrangement provides an adequate level of protection for European personal data as required by the GDPR, particularly in light of the CJEU's concerns about U.S. surveillance activities. Where an adequate level of protection is not provided, organizations should assess what additional safeguards can be implemented to achieve that level of data protection in order to avoid having to choose between suspending data flows and risking regulatory fines.

Finally, as organizations consider new partnerships (or even new internal data-sharing initiatives) moving forward, they should engage in heightened due diligence regarding transatlantic data flows. Before starting any data flows, organizations should ask which country the data originates from, where it will be transferred, whether domestic law in the importing country would satisfy the concerns raised by the CJEU in *Schrems II* and what mechanism can be used to support the proposed data flow.

If your organization is involved in data flows from the EU to the U.S., now is the time to take immediate action in light of the CJEU's latest decision.

Related Professionals

Ieuan Jolly . . . . . ijolly@loeb.com
Kris Ekdahl . . . . . kekdahl@loeb.com

6382 REV2 07-20-2020