BLANKROME

Cybersecurity & Data Privacy

JULY 16, 2020 • NO. 13

Privacy Shield Invalidated and Standard Contractual Clauses Called into Question by EU High Court Decision

The European Union's ("EU") highest court has struck down the EU-U.S. Privacy Shield, which allowed transfers of personal data from the EU to companies in the United States that had certified to the Privacy Shield. Further, the court's decision has called into question whether the standard contractual clauses used by so many companies will remain a viable mechanism for transfer of personal data from Europe to the United States. At a minimum, data exporters and data importers that rely on standard clauses will need to demonstrate that they have done a case-by-case assessment for each contract and determined that they have sufficient protections in place to address the concerns raised by the court with respect to transfers to the United States.

Transferring personal data from the EU to the United States in compliance with the General Data Protection Regulation ("GDPR") just got more difficult. In a surprising decision, the European Court of Justice struck down the adequacy determination regarding the protection provided by the EU-U.S. Privacy Shield framework. In the same decision, the Court also called into question the use of standard contractual clauses for data transfers between the EU and the United States, or any country with similar government surveillance powers. The case, that many refer to casually as "Schrems II," concerned the transfer of personal data by Facebook from the EU to the United States, and the U.S. government's largely unfettered collection of that data for national security surveillance purposes. The Court found that the bulk collection and surveillance of data by the U.S. government is inconsistent with the fundamental rights of EU residents.

PRIVACY SHIELD INVALIDATED

The Court of Justice has invalidated the Privacy Shield Framework, which more than 5,000 organizations in the United States have certified their adherence to and relied on since 2016 to receive personal data from organizations in the EU in compliance with the GDPR. The Court determined that the level of protection afforded by the United States for personal data of EU residents transferred under the Privacy Shield does respect an individual's right to an effective judicial remedy for breach of his or her data

privacy rights guaranteed under Article 47 the EU Charter of Fundamental Rights. With respect to national security surveillance, the Court said that the law in the United States "does not provide for the necessary limitations and safeguards with regard to the interferences authorised by its national legislation and does not ensure effective judicial protection against such interferences." There is no grace period—the Privacy Shield Framework is invalidated as of the date of the decision.

UNCERTAIN FUTURE FOR STANDARD CONTRACTUAL CLAUSES

In addition, the Shrems II decision creates uncertainty around the use of standard contractual clauses for data transfers between the EU and the United States, or any country where the government has broad surveillance powers. Over the years, the European Commission has issued standard contractual clauses that the Commission determined offered sufficient safeguards of personal data to allow the data to be transferred internationally between a data exporter and data importer who signed the clauses. Many EU companies have put these clauses in place covering the transfer of personal data to their vendors and business partners in the United States. It is common for companies to rely on these clauses to transfer employee personal data to affiliates or parent companies in the United States. Now, the Court has said that these clauses require that data exporters and data importers ensure that data subjects whose data are transferred are afforded a level of protection essentially equivalent to that guaranteed under EU regulation, taking into consideration any access by public authorities in the country to which the personal data are transferred. If it is determined that the clauses cannot be complied with in the transferee country, then the Court says that data protection authorities are required to suspend or prohibit transfer of personal data to that country. Given that the Court has already found that EU data subjects do not have equivalent protection in the United States with respect to information that is subject to government surveillance, it is not clear how organizations that rely on Standard Contractual Clauses will bridge the gap.

WHAT NOW?

Data exporters in the EU and data importers in the United States, as of today, must reconsider the personal data that they are transferring pursuant to the Privacy Shield framework and standard contractual clauses.

For each company relying on the Privacy Shield to receive EU Personal Data in the United States, the company must either stop receiving the personal data from the EU or identify another GDPR-compliant mechanism for the transfer. Privacy Shield certified companies in the United States are still bound by their commitment to the Privacy Shield for all EU personal data in their possession. Accordingly, if such companies do not have another GDPR-compliant mechanism to process the data in the United States, they must determine how to return, destroy, or anonymize that data. Other GDPR compliant mechanisms for processing data in the United States include express consent of the data subject, necessity to perform a contract, binding corporate rules, and (perhaps) standard contractual clauses.

For companies relying on Standard Contractual Clauses, the data exporter and importer will need to decide on a case by case basis if there are safeguards that can be used to limit the potential for government surveillance of personal data transferred to the United States under the Clauses. For example, perhaps encryption of EU personal data could be used as such a safeguard. Data exporters and data importers should document their determination. Companies will need to keep an eye on developments to see if the data protection authorities in Europe make a determination that standard contractual clauses cannot be complied with in the United States.

For additional information, please contact:

Jennifer J. Daniels, Pittsburgh Office
Partner, Cybersecurity & Data Privacy
412.932.2754 | daniels@blankrome.com