INVALIDATION OF THE PRIVACY SHIELD: WHAT THE REGULATORS ARE SAYING

Hodgson Russ Cybersecurity & Privacy Alert
August 11, 2020

Transfers of personal data from the European Union into the United States require that certain protections are in effect. With the recent invalidation of the Privacy Shield Framework by the Court of Justice of the European Union (CJEU), it is now more difficult to make such transatlantic transfers because reliance on the Privacy Shield is no longer a viable option.

More specifically, on July 16, 2020, the CJEU invalidated the E.U.-U.S. Privacy Shield, one of the methods for transfers of personal data into the U.S. The court found that under U.S. surveillance laws, the U.S. government has access to personal data that does not provide Europeans with privacy protections equivalent to those in the E.U. The CJEU's judgment, however, did not invalidate transfers based on Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), neither of which is nearly as convenient as the Privacy Shield as a basis to justify personal data transfers. The SCCs and BCRs, which are subject to the same defects as the Privacy Shield, probably escaped greater scrutiny by the CJEU because they are expressly contemplated by the General Data Protection Regulation (GDPR). But, given the court's reasons for invalidating the Privacy Shield, transfers of personal data into the U.S. based on SCCs and BCRs may also be problematic.

Following this landmark ruling by the CJEU, U.S. and E.U. regulators have issued statements giving some preliminary guidance on the judgment's immediate impact. Below is a brief background on the GDPR, Privacy Shield, and the CJEU's recent judgment, as well as a brief summary of the statements issued by the relevant regulators.

Background – GDPR, Privacy Shield, and CJEU's Judgment

The GDPR was adopted into E.U. law in April 2016 and became effective in May 2018. It provides a set of rules that ensure a high standard of protection for personal data, increases legal certainty for organizations processing data, and offers a high degree of protection for individuals. Generally speaking, personal data transfers from the E.U. to non-E.U. countries are prohibited under the GDPR unless certain standards are met by the receiving country or certain safeguards are adopted by the receiving party to ensure protection of the transferred data. (GDPR can be found here).

Attorneys

Jane Bello Burke
William Ciszewski III
Alfonzo Cutaia
Reetuparna Dutta
Patrick Fitzsimmons
Michael Flanagan
Michelle Merola
R. Kent Roberts
Gary Schober
Amy Walters

Practices & Industries

Cybersecurity & Privacy

The E.U.-U.S. Privacy Shield was designed by the U.S. Department of Commerce and the European Commission to help facilitate the transfer of data from the E.U. to the U.S. in compliance with data protection requirements under the GDPR. Participants in the program could self-certify their compliance with the E.U.-U.S. Privacy Shield Framework by registering with the Department of Commerce. (Privacy Shield information can be found here).

The recent CJEU judgment (case C-311/18), which invalidated the E.U.-U.S. Privacy Shield, stems from a complaint filed with the Irish Data Protection Commissioner (DPC) by Max Schrems, an Austrian privacy advocate, who challenged Facebook Ireland's reliance on SCCs as the legal basis for transferring personal data to Facebook Inc. located in the U.S. (Schrems II). After investigating the Schrems' complaint, the DPC brought a proceeding before Ireland's High Court which not only bore on the validity of the SCCs, but also indirectly on the validity of the Privacy Shield. The case made its way to the CJEU which found that U.S. public authorities have access to and use of transferred data in a manner that does not provide E.U. citizens a level of protection essentially equivalent to those protections guaranteed within the E.U. by the GDPR. The CJEU also found that E.U. citizens whose data is transferred to the U.S. do not have actionable rights before the courts against U.S. authorities. As a result, the CJEU found the Privacy Shield invalid. The CJEU did not, however, invalidate transfers based on SCCs or BCRs. Instead, it found that businesses relying on them must assess, prior to any transfer, whether there is an adequate level of protection for personal data in the country where the data is to be transferred. If an adequate level of protection cannot be ensured, then the parties are required to suspend the transfer. Since the E.U. previously ruled that the U.S. does not offer an adequate level of protection, the SCCs and BCRs may not be available to justify transfers of E.U. personal data to the U.S.

Department of Commerce and EDPB Statements Following Schrems II

The U.S. Department of Commerce and the European Data Protection Board (EDPB) both issued statements in the form of FAQs following Schrems II. The Department of Commerce FAQs are found here, and the EDPB FAQs are found here. Below are a few highlights.

- The Department of Commerce said that "the E.U.-U.S. Privacy Shield Framework is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States."
- However, the Department of Commerce also made clear that Schrems II does not relieve E.U.-U.S. Privacy Shield Framework participants of their ongoing obligations and that annual re-certification is still required. It is the Department's position that "organizations' continued participation in the E.U.-U.S. Privacy Shield demonstrates a serious commitment to protect personal information in accordance with a set of privacy principles that offer meaningful privacy protections and recourse for EU individuals."
- The EDPB said that, in light of the CJEU's ruling, transfers done solely on the basis of the Privacy Shield are now considered illegal, and there is no grace period following the Privacy Shield's invalidation.
- The EDPB also said the legality of transfers made on another basis, such as in reliance on SCCs, will depend on a case-by-case assessment taking into account the circumstances of the transfer and supplemental measures that businesses may put into place. The EDPB did not elaborate on what supplemental measures may be taken, but said that any supplemental measures along with the SCCs "would have to ensure that U.S. law does not impinge on the adequate level of protection" guaranteed within the E.U. by the GDPR. If the assessment is that the transfer would not ensure an

essentially equivalent level of protection, then the transfer must not take place.

- On August 10, 2020 the U.S. Department of Commerce and the European Commission issued a joint statement indicating that they have "initiated discussions to evaluate the potential for an enhanced E.U.-U.S. Privacy Shield framework to comply with the July 16 judgment of the Court of Justice of the European Union in the Schrems II case." The U.S. Department of Commerce statement can be found here, and the European Commission statement can be found here.

Now What?

Businesses can no longer lawfully transfer data into the U.S. solely on the basis of the Privacy Shield. Privacy Shield participants, however, should continue to recertify and maintain compliance with their ongoing obligations for the time being. Businesses should also conduct an individualized assessment before making any transfers pursuant to SCCs or BCRs, but given the CJEU's findings regarding U.S. surveillance laws, not to mention the E.U.'s having designated the data protection laws of the U.S. as inadequate, such transfers to the U.S. will be difficult, if not impossible, to justify. A careful analysis must take place, and businesses are encouraged to seek counsel's advice.

Importantly, the CJEU's judgment does not invalidate the Swiss-U.S. Privacy Shield Framework, which "remains a valid mechanism to comply with Swiss data protection requirements when transferring personal data from Switzerland to the United States." (Department of Commerce, FAQs – Swiss-U.S. Privacy Shield). The Federal Data Protection and Information Commissioner of Switzerland (FDPIC) issued a statement saying that the "FDIC has taken note of the CJEU ruling. This ruling is not directly applicable to Switzerland. The FDIC will examine the judgment in detail and comment on it in due course." (FDIC statement).

While we await further guidance on the impact of the CJEU's judgment, many businesses are taking a wait-and-see approach. But given the uncertainty surrounding transatlantic transfers following this landmark ruling, businesses should consult with counsel to determine the best course of action moving forward.

Further alerts will be issued regarding next steps as we gather more information and receive further guidance from regulators. If you have immediate questions, please contact Gary Schober (716.848.1289), Michelle Merola (518.736.2917) or Patrick Fitzsimmons (716.848.1710).

If you received this alert from a third party or from visiting our website, and would like to be added to our Cybersecurity & Privacy alert mailing list or any other of our mailing lists, please visit us **HERE**.