GODFREY & KAHN S.C.

July 2020

Major blow for US businesses that process EU personal data: ECJ strikes down Privacy Shield

Sarah A. Sargent
414.287.9450
ssargent@gklaw.com

Zachary R. Willenbrink
414.287.9463
zwillenbrink@gklaw.com

On July 16, 2020, the European Court of Justice (ECJ) struck down the EU-US Privacy Shield (Privacy Shield), an important program that provided US businesses with a legal mechanism for transferring personal data from the EU to the US in compliance with the General Data Protection Regulation (GDPR). This new ruling has major implications for US businesses that have depended on Privacy Shield to process EU personal data. Those businesses must now re-evaluate and leverage a different legal mechanism to transfer personal data into the US

The US Department of Commerce designed Privacy Shield in conjunction with the European Commission, which in July 2016 determined the program adequately protected EU personal data and therefore approved it. Privacy Shield enabled US-based organizations to both self-certify and publicly commit to compliance with the program's requirements and, in exchange, receive assurance that their transfer of EU data would comply with EU law. However, by joining the Privacy Shield program, US businesses committed to the US government's enforcement of the program. In other words, although the US does not have nationally-applicable standards that reach the same level as Privacy Shield, any businesses joining the program agreed that US authorities could punish them for breaching the program's requirements.

Despite Privacy Shield's heightened requirements, including the requirement that businesses voluntarily subject themselves to US enforcement, the program was successful: more than 5,000 businesses joined, including social media giants Facebook and Twitter. Additionally, many large European businesses, such as Eaton Corporation, Ingersoll-Rand and SAP, joined primarily to ensure that their transfers of human resource data were protected. But adoption wasn't limited to large multinationals, as approximately 65 percent of participants are considered small to medium enterprises and 41 percent have a revenue of below $5 million.

The ECJ, however, just threw a wrench into the plans of any business relying on Privacy Shield for protection. In *Schrems II* (the "II" being necessary because an earlier *Schrems* decision struck down a previous EU/US cooperation program called "Safe Harbor"), the ECJ decided that US national security and law enforcement requirements—essentially, government surveillance, with Section 702 of FISA being of particular concern (FNs 54-58)—interfere with the fundamental rights of EU citizens whose data is transferred to the US. Specifically, the ECJ found that EU citizens did not have the required legal recourse in the US for a violation of their rights under GDPR. The US Secretary of Commerce, Wilbur Ross, issued a statement that the US Department of Commerce would continue to enforce Privacy Shield obligations despite the ruling. He also indicated that the Department of Commerce would work with the European Commission and European Data Protection Board to limit negative impacts on US businesses.

Additionally, the ECJ upheld the validity of the Standard Contractual Clauses (SCCs) as a legal method for transferring personal data. The SCCs are non-negotiable legal contracts created by the EU to allow for the transfer of personal data to countries without an adequacy decision. While some businesses praised the ECJ's decision to uphold the SCCs, others are concerned that the ECJ laid the groundwork for a future conclusion that the SCCs will not work with US businesses. The ECJ questioned whether businesses could comply with the SCCs provisions if the business was subject to laws inconsistent with the GDPR. The ECJ stated that controllers must determine on a case-by-case basis whether a processor can meet the requirements of the SCCs considering the level of protection afforded to data in the processor's country. The ECJ stated that parties to the SCCs could potentially agree to additional protections above and beyond the SCCs but did not outline what those additional protections would be.

This decision has immediate ramifications for any US business that processes EU personal data pursuant to Privacy Shield and may have future impacts on US businesses relying on the SCCs if controllers determine that US processors cannot comply with the SCCs due to applicable law. Because Privacy Shield no longer provides a legal method for transferring personal data to the US, data controllers now have a legal obligation to suspend personal data transfers that do not comply with EU law. If your business processes EU personal data, you should immediately:

- Ensure that your data transfers and processing comply with GDPR requirements
- Implement another legal method for transferring personal data from the EU, such as the SCCs, Binding Corporate Rules or consent
- Before ceasing to comply with the Privacy Shield requirements, ensure that you follow all necessary guidelines for withdrawing

If you need any assistance ensuring GDPR compliance, evaluating SCCs, devising Privacy Shield alternatives, or other data privacy and security matters, contact our Data Privacy & Cybersecurity Practice Group.