protiviti®
Face the Future with Confidence

European Court of Justice Invalidates the EU-US Privacy Shield Framework

July 17,
2020

On Thursday, July 16, the Court of Justice of the European Union (CJEU) implemented a landmark ruling in case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (more commonly referred to as "Schrems II"). While it concluded that Standard Contractual Clauses (SCCs) issued by the European Commission for the transfer of personal data to data processors established outside of the European Union (EU) are still valid, the court invalidated the EU-US Privacy Shield framework.

By way of background, Max Schrems is an Austrian privacy activist, commonly known for his objections to Facebook's cooperation with the U.S. federal government in conducting surveillance on individuals, which he alleged violated privacy rights granted under EU law. Looking back, revelations made in 2013 by Edward Snowden, a former U.S. Central Intelligence Agency contractor, publicly exposed numerous global surveillance programs administered by the U.S. National Security Agency. The inclusion of EU citizen data in these programs led to Schrems' first appearance in 2015 in front of the CJEU. Schrems successfully argued that Facebook's privacy practices did not provide "adequate protection" of fundamental privacy rights as required under Article 25 of the Data Protection Directive.

Finding in Schrems' favor, the CJEU invalidated the "Safe Harbor Principles," a set of 7 privacy principles that U.S. companies could self-certify that they follow in order to comply with the EU Data Protection Directive. After significant consultation and negotiation between the European Commission and the U.S. Federal Trade Commission and Department of Commerce, the EU-US Privacy Shield (Privacy Shield) was launched as a more robust framework to replace the Safe Harbor Principles. Its design was improved to strengthen, formalize and provide a certification mechanism for U.S. businesses and to provide adequate protection of EU data.

From its 2016 inception, Privacy Shield encountered uncertainty, even prior to its effective date. EU officials, public commentators and policymakers questioned whether the revamped framework, as architected, would now satisfy the data protection "adequacy" requirement of rapidly evolving EU privacy law. In 2019, Schrems once again found himself before the CJEU, this time to argue against the effectiveness of the new Privacy Shield. On July 16, the CJEU ultimately agreed with Schrems, invalidating the Privacy Shield framework, effective immediately.

In a statement addressing the decision dated July 17, the European Data Protection Board noted "While the SCCs remain valid, the CJEU underlines the need to ensure that these maintain, in practice, a level of protection that is essentially equivalent to the one guaranteed by the GDPR in light of the EU Charter."

What does the invalidation mean for U.S. businesses with EU interests?

There are 5,784 U.S. companies that have relied on their EU-US Privacy Shield certifications that can no longer use Privacy Shield as their mechanism for data transfers of personal information from the EU to the U.S. Moreover, no grace period has been officially established, so organizations relying on the Privacy Shield need to immediately consider alternative measures to ensure secure data transfers.

SCCs currently remain valid, but with conditions. Data controllers should examine the data protection laws of the receiving country to determine whether adequate protections are in place and align to the EU General Data Protection Regulation (GDPR) and Member State legal requirements; controllers should assess the likelihood that their processor(s) may share personal data with public authorities. Data protection officers (DPOs) and controllers should make risk-informed decisions on a case-by-case basis to protect the privacy rights of EU residents; supervisory authorities are "required to suspend or prohibit a transfer of personal data" in cases where the SCCs cannot be met and where neither the controller nor the processor have stopped the data transfer(s), in accordance with GDPR Article 58 (*Supervisory Authority Corrective Powers*).

Binding corporate rules and special derogations have not been affected by this decision. If a company relies on these mechanisms to enable data exports to the U.S., there is no need to alter them. However, like SCCs, each personal data export use case should be reviewed under the lens of protecting personal information with an increased focus on the "adequacy" of data protection.

How can organizations prepare?

1. Convene the privacy and data governance team to understand the impact of the ruling and set a new strategic course on EU-US data transfers.

2. Conduct an analysis to understand where Privacy Shield requirements have been in use, with specific emphasis on vendor relationships.

3. Review all data export/data import arrangements and storage locations (consider public cloud providers, who may retain data copies in jurisdictions without determinations of adequate protections).

4. Next, review and revise Standard Contractual Clauses to ensure stringent data protections considering the Schrems II decision. Consider implementing Binding Corporate Rules.

5. Review your current operational privacy practices. Does your organization really satisfy GDPR data protection and privacy requirements, or are Standard Contractual Clauses only used to fulfill a checkbox?

6. Finally, review the organization's privacy policies and public notices, particularly if the company has relied on EU-US Privacy Shield to date. Consult with legal counsel to update documents to reflect compliant terms. If the company maintains a data center presence in the EU or a country with a favorable adequacy decision (e.g., Canada, Japan, etc.) and processing is feasible in that environment, consider the possibility of moving the function into one of those jurisdictions.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of *Fortune* 1000 and 35% of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

How Can Protiviti Help?

Protiviti can assist companies with preparing for this major change in data management in a variety of ways. Our professionals can:

- Assess organizational privacy risks, using best-of-breed privacy frameworks.
- Define long-term privacy objectives and the strategic plans to implement and operationalize privacy practices.
- Elaborate personal data inventories and processing activities. Document data flows and Records of Processing Activities.
- Evaluate vendor risk programs and safeguards.
- Collaborate with Internal Audit departments to facilitate Privacy Program maturity assessments and organizational compliance with privacy laws and regulations.
- Identify and design process and technical solutions to remediate compliance gaps and enhance privacy operations.

protiviti®