Schrems II: EU-US Privacy Shield Struck Down, but European Commission Standard Contractual Clauses Survive

07 / 17 / 20

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Eve-Christie Vermynck
Counsel / London
44.02.0751.9709
eve-christie.vermynck@skadden.com

Daniel Millard
Associate / London
44.02.7519.7201
daniel.millard@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

40 Bank St., Canary Wharf
London, E14 5DS, UK
44.20.7519.7000

On July 16, 2020, the Court of Justice of the European Union (CJEU) struck down the EU-U.S. Privacy Shield as a valid mechanism for transferring personal data from the European Economic Area (EEA) to the United States (*Schrems II*). The European Commission Standard Contractual Clauses (SCCs) for data transfers remain valid but are subject to increased due diligence on the part of data exporters to ensure that the privacy laws of the importing country are adequate. Below, we discuss the background to *Schrems II*, the judgment itself and key takeaways.

Background

In 2013, Austrian privacy activist Max Schrems filed a complaint with the Irish Data Protection Commission (DPC) against Facebook, alleging that Facebook had allowed U.S. authorities to access his personal data in violation of the Data Protection Directive 1995 (Directive 95/46/EC), the predecessor of the General Data Protection Regulation (2016/679) (GDPR). In 2015, the CJEU held in Schrems' favor and, more broadly, found that the Safe Harbor framework, the transfer mechanism by which the personal data transfer had been effected, was invalid (*Schrems I*). The Safe Harbor, which thousands of U.S. companies had been relying on, allowed such companies to self-certify adherence to various privacy principles and then transfer data from the EEA to the U.S. in compliance with the Data Protection Directive. The CJEU decision was based, in part, on the access that U.S. authorities had to the personal data of EEA-based individuals, the scale of which had been unearthed by the former National Security Agency contractor Edward Snowden.

The EU and the U.S. subsequently negotiated and implemented the Privacy Shield as the data transfer mechanism to replace the Safe Harbor framework. While the Privacy Shield sought to address the issues the CJEU had raised with the Safe Harbor, the basic mechanism remained the same; companies could self-certify adherence to various privacy principles and then transfer data from the EEA to the U.S. Over 5,000 U.S. companies took advantage of the Privacy Shield.

After *Schrems I*, Facebook decided to rely on the European Commission-approved SCCs as the data transfer mechanism by which to transfer personal data to the U.S. SCCs are approved data contracts that two parties can enter into to transfer data from the EEA to other countries. Schrems submitted another complaint to the Irish DPC, relying on similar arguments to those made in *Schrems I*, alleging that the SCCs are also inadequate.[1] In its *Schrems II* judgment, the CJEU addressed both the SCCs and the Privacy Shield.

CJEU Decision

SCCs

The CJEU held that SCCs remain a valid mechanism to transfer personal data outside the EEA since they provide sufficient protection for EEA personal data. However, the court held that it is for the data exporter (*i.e.*, the EEA-based party) to ensure that, in practice, an adequate level of data protection is provided in the country where the data importer is based: "it is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses."

[1] The validity of the Privacy Shield was separately challenged by La Quadrature du Net, a French advocacy group that promotes digital rights; that challenge to the Privacy Shield had been put on hold by the CJEU pending the outcome of *Schrems II*.

Where a country falls short, the CJEU also encouraged parties to enter into "additional safeguards" to those offered by the SCCs, but it did not elaborate on the form such safeguards could take.

The SCCs refer to the Data Protection Directive 1995. The CJEU did not comment on the need for the SCCs to be updated for alignment purposes with GDPR requirements.

Privacy Shield

The CJEU held that the Privacy Shield is not a valid mechanism for transferring personal data from the EEA to the U.S. The CJEU's decision was based on (i) the limitations on the protection of personal data under U.S. law, and (ii) the disproportionate access and use of EEA personal data by U.S. authorities with no effective redress mechanism for data subjects. In particular, the access to personal data under U.S. surveillance programs could not be regarded as being limited to what is "strictly necessary," and the Privacy Shield also does not grant individuals based in the EEA actionable rights before U.S. courts against U.S. authorities. According to the CJEU, the Privacy Shield therefore cannot ensure a level of protection essentially equivalent to that arising from the GDPR as supplemented by national data protection laws across EEA countries.

Key Takeaways

- If an organization's data transfers from the EEA to the U.S. are currently based on the Privacy Shield, it should begin to consider alternative data transfer mechanisms. We note that when the Safe Harbor was held to be invalid in 2015, EEA supervisory authorities allowed a grace period during which organizations could implement alternative transfer mechanisms. This grace period, coupled with the subsequent absence of enforcement action from supervisory authorities, was long enough for organizations to move over to the newly negotiated Privacy Shield. It remains to be seen whether a similar approach may be adopted for the Privacy Shield, although a grace period was offered when the Safe Harbor was held to be invalid because the EEA was keenly aware of the disruptive effect on U.S. organizations. The EEA may have the same view now. In addition, a statement by European Commission Vice President for Values and Transparency Věra Jourová and Justice Commissioner Didier Reynders suggested that plans to modify the Privacy Shield to address the CJEU decision are already underway.
- If an organization relies on, or is considering relying on, the SCCs to transfer data out of the EEA, it will need to assess whether the country to which the personal data will be transferred has an adequate level of protection. At a minimum, this might involve developing a written due diligence process to assess adequacy whenever a data transfer outside the EEA occurs — including consideration of the importing country's privacy laws — the level of access and/or surveillance that the importing country's authorities may have to the exported EEA personal data, and the rights that data subjects have in relation to their exported EEA personal data. EEA supervisory authorities are expected to issue guidance in due course as to how companies are to comply with this new requirement. It remains unclear what would happen if different organizations drew different conclusions about what constituted adequate compliance.
- EEA supervisory authorities, the European Commission and the European Data Protection Board, will likely comment on *Schrems II*, providing organizations with further guidance on next steps.