Kilpatrick

OCTOBER 5, 2020

The Privacy Shield Sunk, but Is There a Life Raft for the Standard Contractual Clauses? Strategies for Transferring Personal Data Across the Atlantic from a Post-Schrems II Europe

1. *Schrems II* requires parties relying on the SCCs to implement additional measures ensuring that transferred personal data is adequately protected.

The *Schrems II* decision did not affirmatively invalidate the SCCs, but also made clear that the SCCs alone, without additional measures, often do not sufficiently protect transferred personal data. The Court of Justice of the European Union ("CJEU") noted that "depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller" may be necessary "in order to ensure compliance with" the level of protection required under the laws of the European Union ("E.U."). The decision notes that the GDPR "states that 'the possibility for the controller… to use standard data-protection clauses adopted by the Commission… should [not] prevent [it]… from adding other clauses or ***additional safeguards' and states, in particular, that the controller 'should be encouraged to provide additional safeguards… that supplement'*** the SCCs.

With respect to personal data transferred to the United States, the CJEU found that data subjects have no actionable rights against U.S. authorities with respect to certain surveillance programs, FISA 702 and Executive Order 12333, such that data subjects lack enforceable rights and judicial redress under U.S. law.

Given that public authorities engage in lawful surveillance under E.U. law, additional safeguards implemented to match the level of protection required by E.U. law should not require eliminating the possibility that transferred personal data might be subject to collection by U.S. intelligence or law enforcement agencies. After all, Sections 5(d)(i) of the SCCs affirmatively permits sharing personal data pursuant to law enforcement requests.

No specific additional safeguards are required for any particular transfer, as the CJEU clarified that parties must identify additional safeguards on a case-by-case basis. Given that uncertainty, to address the CJEU's concerns regarding data subjects' lack of enforceable rights and judicial redress, parties should consider implementing supplemental measures such as those listed below to establish arguments that transferred personal data remains adequately protected:

- enhanced notice requirements under which the data importer must notify the data exporter, and the data subject to the extent practical and permitted by law, of law enforcement or surveillance

requests;

- contractual commitments to challenge law enforcement or surveillance requests and disclose only the minimum amount of personal data required by law;
- publishing transparency reports describing FISA requests to the extent permitted by federal law (i.e., delaying reporting by 6 months from the request date and reporting in bands of 500); and
- enhanced encryption requirements.

2. European Regulatory Guidance

Many European Data Protection Authorities ("DPAs"), such as those in France and Spain, have acknowledged the *Schrems II* decision, but offered little substantive guidance regarding what parties should do to protect transferred personal data. Other DPAs, such as Norway's DPA, have suggested that organizations should stop transferring personal data until DPAs can identify adequate safeguards. The Berlin DPA has taken an even more extreme view in that it has interpreted the *Schrems II* ruling to mean that no data may be transferred to the U.S., even using SCCs that include additional safeguards. Similarly, proceedings in Ireland could lead to a prohibition on data transfers from Ireland to the U.S.

In September 2020, the Baden-Württemberg, Germany DPA proposed edits to the SCCs that increase data exporter obligations with respect to law enforcement requests for personal data. The draft included revised SCCs that require the data importer to inform both the data exporter and the data subject (if feasible) of a request. Moreover, the draft rules would require data importers to take legal action against responding to surveillance requests, but the draft SCCs would allow data importers to disclose personal data pursuant to a legally binding order. Therefore, although those draft rules set forth some of the most restrictive of proposed safeguards following *Schrems II*, the proposal does not create an affirmative requirement to obtain data exporter consent for personal data disclosures to law enforcement.

3. The U.S. Department of Commerce

On September 28, the Department of Commerce released a white paper outlining privacy safeguards regulating and establishing oversight of U.S. intelligence agencies' use of personal data. The white paper does not bear directly on whether law enforcement agencies will treat personal data differently if the personal data has been transferred from the E.U. to the U.S. However, the white paper emphasizes that US intelligence agencies share personal information with E.U. Member States, including information relating to foreign operatives, suggesting that the agencies remain committed to collecting the personal data of E.U. citizens, even after the *Schrems II* decision.

The white paper also states that companies transferring personal data to the E.U. under the SCCs may argue that US law, at least in 2020, satisfies many of the CJEU's concerns. The *Schrems II* court evaluated an E.U. Commission decision from 2016 that described U.S. law as in force at that time, instead of evaluating current U.S. law. The white paper therefore points out that the Schrems II court did not consider several safeguards privacy safeguards currently in place with respect to FISA 702 requests and US government access to personal data under 12333.

As such, the white paper suggests that companies may argue that transferring personal data from the E.U. to the U.S. under the SCCs may be permissible following *Schrems II*. Since that decision did not consider many US privacy safeguards, data transfer to the US under the SCCs should not require as many additional safeguards to ensure adequate protections as the CJEU may suggest.

Although the white paper may not be a sea change for E.U. regulators' understanding of data transfer, the white paper cuts against regulators' potential argument that transfers under the SCCs are impermissible without significant additional protective measures.

We note, in conclusion, that the law of personal data transfer after *Schrems II* remains fluid and many European regulators have not issued substantive or final guidance (including the European Data Protection Board ("EDPB"). Given that lack of guidance requiring any specific compliance solutions, companies should be cautious about implementing any specific additional protection safeguards that create significant legal or operational burdens.