Kilpatrick

JULY 21, 2020

Lower Your Privacy Shield, But Max Out Your Options for Maintaining Transatlantic Data Flow

by Jon Neiditz

Any organization that relies on certification under the EU-U.S. Privacy Shield framework and/or entering into the Standard Contractual Clauses ("SCCs" or "Model Clauses") to effectuate personal data transfers from the European Economic Area ("EEA") to the United States ("U.S.") should reevaluate the organization's data transfer strategy. On July 16, 2020, the Court of Justice of the European Union ("CJEU"), in a case evaluating the validity of data transfers from the EEA to the U.S. ("case C-311/18" or "Schrems II"), invalidated the Privacy Shield and significantly restricted the SCCs' effectiveness. So far, regulators across Europe have signaled mixed responses to the decisions, so the countries from which an organization transfers personal data may shape the organization's response.

A. The Pen is Mightier than the Shield

Schrems II arises from a complaint made by Austrian Max Schrems to the Irish Data Protection Commission ("DPC") challenging personal data transfers from the EEA to the U.S. Schrems voiced concern that the SCCs insufficiently protect personal information transferred to the U.S. The DPC referred the case to Irish courts, which passed the complaint, and additional questions regarding the Privacy Shield (not at issue in Schrems' complaint), to the CJEU.

The CJEU found that the Privacy Shield cannot establish an adequate basis for data transfers since (i) data subjects lack the right to seek an adequate legal redress against U.S. authorities in a legal tribunal and (ii) U.S. law does not effectively limit government authorities' access to personal data. With respect to rights over personal data, whether a third country's legal regime adequately protects personal data depends on whether that regime "provides effective and enforceable rights and effective administrative and judicial redress." The CJEU found that data subjects have no actionable rights against U.S. authorities with respect to certain surveillance programs, such that data subjects lack enforceable rights and judicial redress. Moreover, the CJEU reiterated that a government authority's access to personal data must be limited and proportionate to the authority's need to access personal data. The CJEU found that U.S. law lacks such limitations and proportionality. These findings are similar to those previously made in striking down the "Safe Harbor" in 2015 and – unless we begin to include government in publicly-accountable and visible "privacy law" – probably similar to those to be made in several years in striking down "Privacy Mask."

B. CJEU Puts a Chink in the Model Clauses' Armor

The CJEU found that the SCCs are a valid data transfer mechanism for providing some level of data

protection, but without additional safeguards, may be insufficient for ensuring that a personal data transfer sufficiently protects personal data. Under the GDPR, parties must implement adequate safeguards to ensure data protection, including to ensure effective remedies for data subjects. The SCCs, as a contract between private parties, cannot bind government authorities in the country to which the personal data is imported. Therefore, the party exporting the personal data to a country in which government authorities have access to personal data must implement additional safeguards to ensure data protection with respect to government authorities. Therefore, the decision implies that exporting parties should require importing parties to implement non-contractual measures to protect personal data, such as encrypting personal data and demonstrating that government authorities do not have a need to access the transferred personal data.

C. A Two Pronged Attack: the Decision Creates Contractual and Regulatory Risk

The CJEU requires exporting parties, and European regulators, to suspend or terminate personal data transfers if the transfer lacks adequate safeguards, including if a transfer is made pursuant to the SCCs. U.S. vendors transferring personal data from the EEA to the U.S. therefore face some risk that such customers might exercise rights to suspend or terminate the transfer of personal data through the vendor.

Moreover, the CJEU ruling takes immediate effect and does not establish an express regulatory grace period under which the Privacy Shield program and SCCs remain valid, and regulatory response will likely be inconsistent across the EEA given that enforcement will be done by the EEA's thirty Data Protection Authorities ("DPAs"). For example, the UK's ICO provided that companies currently relying on Privacy Shield should continue to do so until the agency releases additional guidance. The Berlin DPA, conversely, directed all controllers to suspend personal data transfers to the U.S. Norway's Datatilsynet has recently issued guidance almost as strong as that of Berlin. Certain European regulators could therefore bring enforcement actions for violating the GDPR's data transfer rules against companies that currently have no valid data transfer mechanism in place.

D. The Few Arrows Left in the Quiver: A Summary of Current Options for Transferring Personal Data Out of the EEA

- *The Standard Contractual Clauses.* The SCCs are an agreement between an entity exporting personal data out of the EEA and the party importing personal data into the non-European jurisdiction. The SCCs contain substantial obligations on the exporting and importing parties, including, among other obligations, that the parties agree to (i) allow the individuals whose personal data is transferred to have directly enforceable rights against the parties, (ii) allow disputes arising under the clauses in European forums, and (iii) cooperate with European regulators.
- *Binding Corporate Rules.* Certain large organizations, in particular, effectuate EEA-U.S. intracompany data transfers by establishing a set of internal policies known as binding corporate rules ("BCRs"). Approved BCRs are a time-consuming process for an organization to achieve since establishing BCRs require the approval of each European Union ("EU") Member State supervisory authority where the controller or processor operates in the EU, thus requiring the interaction with

and approval of many European privacy regulators. Plus, the BCRs permit only intracompany transfers and do not address data transfers to third party organizations.

- *Derogations in the Absence of Appropriate Safeguards.* The GDPR establishes several "derogations" pursuant to which parties may transfer personal data out of the EEA in the absence of appropriate safeguards. For example, a transfer may take place if the data subject has explicitly consented to the proposed transfer or if the transfer is necessary to perform a contract between a data subject and a controller. The derogations, however, are currently only to be used in limited circumstances, and should not now be relied upon for regular data transfers.

E. Belt and Suspenders Approach to Data Transfer

Many large technology vendors that transfer personal data from the EU to the U.S. on behalf of enterprise clients have effectuated transatlantic data transfers by relying on both the SCCs and Privacy Shield certification. Such vendors may assure customers that data transfer will continue under the SCCs agreed upon between the parties. However, EU supervisory authorities may find that such vendors are regularly subject to the very type of U.S. governmental requests of greatest concern in Schrems II (and, by the way, are major competitors of European concerns) and that the customer-controllers cannot adequately protect personal information from government surveillance, effectively eliminating the customer-controllers' reliance on SCCs to effectuate data transfer with such large vendors.

F. Running the Data Transfer Gauntlet

Going forward, we recommend that organizations transferring personal data from the EEA to the U.S.:

- Quickly (and this may be the only immediate step to take), sign SCCs for agreements (whether with customers or vendors) that rely solely on the importing party's Privacy Shield certification to effectuate the transfer of personal data.
- As the specific implementations of Schrems II become more clear, document, in internal policies and in agreements, (i) measures (such as encryption or hashing) that are designed to protect personal data and (ii) that government authorities should not need to access personal data processed by the organization.
- Evaluate whether the company may rely on the derogations to effectuate personal data transfers, with or without new encouragement from Europe to use those derogations more broadly.
- Monitor the response of European regulators to the CJEU decision in jurisdictions that the organization currently operates or intends to operate.
- Determine how the UK and Switzerland will respond to the CJEU's ruling and whether those countries will follow Schrems II by invalidating Privacy Shield as a valid data transfer mechanism from the UK and Switzerland, respectively.
- If the company has been under Privacy Shield, continue to apply Privacy Shield protections to any data transferred pursuant to Privacy Shield, and assess the merits of withdrawal or remaining under that shattered shield.