ANOTHER CHALLENGE TO THE TRANSFER OF FOREIGN DATA TO THE U.S.

Hodgson Russ Cybersecurity & Privacy Alert
September 15, 2020

As previously reported, the E.U.-U.S. Privacy Shield—one of the methods for properly transferring personal data into the U.S.—was upended by the Court of Justice of the European Union's (CJEU) conclusion that the Privacy Shield did not provide an adequate level of data protection. Specifically, in the so-called *Schrems II* decision, the CJEU found that under U.S. surveillance laws, the U.S. government has access to personal data that does not provide Europeans with privacy protections equivalent to those in the E.U. Several months later, we continue to see the ripple effects of *Schrems II*.

On September 8, 2020, the Swiss Data Protection Authority (the Federal Data Protection and Information Commissioner, or "FDPIC"), issued a seven-page policy paper on the transfer of personal data from Switzerland to the U.S. *See Policy Paper*. The policy paper arises out of an annual review of the Privacy Shield conducted by the Swiss delegation and the U.S. government authorities. Even though Switzerland is not a member of the E.U. and not bound by *Schrems II*, the *Schrems II* decision weighed heavily in that assessment. There is currently no legal decision in Switzerland comparable to the CJEU ruling. Nonetheless, the FDPIC noted that the GDPR and any CJEU rulings based upon it, will be imposed on Swiss companies that process and export personal data of EU data subjects. For this reason, the FDPIC felt compelled to reassess the status of the U.S. as an importer of personal data from Switzerland.

The FDPIC maintains several country lists. The first list of countries includes those that provide an adequate level of protection through legislation, practical application of that legislation, publications, official statements and decisions. However, the U.S. has never been included on the first list. The second list, entitled "Adequate protection under certain circumstances," is a list of countries (including the U.S.) to which data transfers are permitted in limited circumstances. With respect to the U.S., until recently, those transfers were permitted if the transfer took place directly with a U.S. business that agreed to a specific certification procedure under Privacy Shield principles established by and between the U.S. and Switzerland. This is what is referred to as the Swiss-U.S. Privacy Shield, which is in all material respects identical to the U.S.-E.U. Privacy Shield.

Attorneys

Jane Bello Burke
William Ciszewski III
Alfonzo Cutaia
Reetuparna Dutta
Patrick Fitzsimmons
Michael Flanagan
Michelle Merola
R. Kent Roberts
Gary Schober
Amy Walters

Practices & Industries

Cybersecurity & Privacy

According to the FDPIC, the special protections guaranteed by the Swiss-U.S. Privacy Shield are insufficient. In particular, it determined that the "lack of transparency and the resulting absence of guarantees concerning the interference of US authorities with privacy and informational self-determination of persons concerned in Switzerland" to be irreconcilable with Swiss law. *See Policy Paper* at 5. It is important to note that the FDPIC does not have the authority to invalidate the Swiss-U.S. Privacy Shield and its position is subject to any rulings to the contrary by Swiss courts. However, the practical implications of the FDPIC's policy position is real: companies may no longer rely, in good faith, on the Privacy Shield as a valid data transfer mechanism.

In addition, consistent with *Schrems II*, the FDPIC concluded that the use of alternative data transfer mechanisms, such as Standard Contractual Clauses ("SCCs") or Binding Corporate Rules ("BCRs), requires companies to conduct a risk assessment and possibly implement additional safeguards to assure that personal data is adequately protected. It cautioned, however, that the SCCs and BCRs cannot prevent foreign authorities from accessing personal data if the public law of the importing country, like U.S. law, takes precedence and allows official access to the transferred data without sufficient transparency and legal protection of the individuals concerned. The FDPIC also goes on to state that "it is to be assumed that in many cases the SCCs and comparable provisions do not meet the requirements for contractual safeguards pursuant to Swiss law." *See Policy Paper* at 6. Where it is not possible to implement additional safeguards, the FDPIC recommends suspending transfers of Swiss personal data to the U.S.

As a practical matter, U.S. companies that are to receive Swiss or EU data, are now faced with difficult legal and operational decisions. In conjunction with the EU or Swiss data exporter, companies need to:

- Examine the data protection risks that are implicated by the transfer, including the volume and sensitivity of the data at issue.
- Evaluate technical measures that could effectively prevent U.S. authorities from accessing the transferred personal data.
- If data is stored solely in the cloud by service providers, consider encryption along with the principles of "bring your own key" to make the data unavailable.
- If services that go beyond mere storage, however, consider if technical measures are possible and, if not, assess the consequences of an enforcement action.

As the FDPIC policy paper demonstrates, the ripple effects of *Schrems II* are likely to have a broad and lasting impact on how companies do business. If you have questions about how to transfer data to the U.S. or other GDPR concerns, contact Gary Schober (716.848.1289), Michelle Merola (518.736.2917), or Patrick Fitzsimmons (716.848.1710).