Schrems II: Privacy Shield Invalid and Severe Challenges for Standard Contractual Clauses

July 17, 2020

Yesterday the Court of Justice of the European Union ("CJEU"), the EU's highest court, invalidated the EU-U.S. Privacy Shield for cross-border transfers of personal data. The CJEU's decision also cast significant doubts over whether companies can continue to use the European Commission-approved Standard Contractual Clauses ("SCCs") to transfer EU personal data to the United States, or to other jurisdictions with similarly broad surveillance regimes. The CJEU's lengthy decision is here and its short-form press release is here.

What does this mean for organizations that rely on Privacy Shield or SCCs? History suggests that privacy enforcement authorities in the EU may hold their fire while efforts are made to come up with a replacement system for data transfers. EU authorities hopefully will clarify their enforcement intentions soon. In any event, organizations that have relied on Privacy Shield will have to turn immediately to considering what practical alternatives they might adopt. U.S. government authorities will also have to turn to the knotty question of what data transfer mechanisms might ever satisfy the CJEU, given persistent EU concerns about U.S. government surveillance of personal data.

What Is This About? For anybody entering in "the middle of the movie": The EU's General Data Protection Regulation ("GDPR") creates a stringent EU-wide uniform law of data privacy, going well beyond what U.S. privacy law requires. GDPR provides among other things that, when it comes to personal data, what happens in the EU generally stays in the EU.

That is—GDPR effectively builds a data protection "wall" around the perimeter of the EU. Personal data can only be brought across the wall to a non-EU country if the data goes via an approved "door," *i.e.*, one of several data transfer mechanisms that are authorized by GDPR. These mechanisms, broadly speaking, all are meant to ensure that once EU personal data arrives at its non-EU destination, it will continue to be protected by privacy standards that approximate those of GDPR.

One of the key doors, or transfer mechanisms, is Privacy Shield, a European Commission-approved framework for transatlantic data transfers enacted in 2016 between the United States and the EU. U.S.-based organizations that sign up for Privacy Shield voluntarily certify to compliance with a GDPR-like set of data privacy terms. Privacy Shield replaced Safe Harbour, a predecessor mechanism that the CJEU struck down as being inadequately protective of EU personal data. The CJEU acted against Safe Harbour after Edward Snowden's revelations about how broadly U.S. intelligence and law enforcement agencies were reviewing telephone records and other personal data.

Approximately 5,000 organizations have self-certified under Privacy Shield, including major companies like Facebook, Google and Microsoft. One feature of Privacy Shield is the designation of an "ombudsperson." That is an official within the U.S. Department of State who can take inquiries from EU data subjects who are concerned about what happens to their personal data once in the United States.

Another widely used transfer mechanism are the SCCs. These are a set of European Commission pre-approved terms that private parties can incorporate into their own agreements. SCCs can be entered into by unrelated commercial counterparties—say, as part of the terms of a business transaction. They can also be entered into by affiliated entities, such as between parents and subsidiaries or between "sibling" organizations. Like Privacy Shield, the SCCs boil down to a commitment by private parties to follow GDPR-like standards in the handling of personal data.

What Just Happened? The case is the latest chapter in the long-running battle played out in the Irish courts and the CJEU among Facebook, Austrian privacy advocate Maximillian Schrems, and the Irish Data Protection Commission. Schrems' complaint posed the question: Do the Privacy Shield and SCCs provide sufficient safeguards to EU personal data once it leaves the EU? For Privacy Shield, the Court answered with—in our words—a firm "no," and for SCCs, "it depends, but sometimes not."

The Court found Privacy Shield invalid on two principal grounds.

First, that U.S. law enforcement agencies' access to personal data transferred under Privacy Shield is "not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law," due to a lack of proportionality—meaning that they are not "limited to what is strictly necessary." Long story short: Just as Safe Harbour failed at the CJEU several years ago because of perceived excessive access to personal data by the NSA and similar agencies, Privacy Shield has failed for basically the same reason.

Second, that the Privacy Shield ombudsperson mechanism did not give EU data subjects effective administrative and judicial redress for violations of their rights.

This means that Privacy Shield immediately ceases to be a valid basis on which to transfer personal data from the EU to the United States.

On the SCCs, the Court found that while they are valid, as such, whether they can constitute a lawful basis for the transfer of personal data to a jurisdiction without an adequacy decision depends on whether the recipient is in a jurisdiction which affords "a level of protection essentially equivalent to that guaranteed within the EU." Crucially, this necessitates an assessment of any potential "access by the public authorities of that third country" by the data exporter and the data importer.

Given the Court's findings on U.S. surveillance laws in the context of Privacy Shield, the risk seems high that—on further scrutiny, in some future case—the same concerns would render transfers to the United States based on the SCCs invalid as well. The same risk would apply to transfers to other jurisdictions with broad surveillance regimes that do not provide (in the eyes of the CJEU, at least) the same safeguards as GDPR.

For this reason, the impact of today's decision is likely to be far greater than when Safe Harbour was ruled invalid. At that time, organizations could comfortably fall back on the SCCs. Now that option might not be open to them.

What Happens Next?

- It appears that organizations that today rely on Privacy Shield alone for data transfers out of the EU must, in due course, either simply stop the transfers or adopt a different GDPR-approved mechanism for making them. The SCCs remain an option today, subject to the risk noted above. For transfers within a corporate family, another GDPR-approved option are the Binding Corporate Rules ("BCRs"). The BCRs are a set of terms, pre-approved by the EU authorities, which multinational organizations can adopt as their own internal rules. Following the rationale of the decision transfers made on this basis may also be at risk.

- Companies may also want to revisit the terms on which they have contracted with third parties regarding data transfers, and assess whether representations that they will send or receive data based on the Privacy Shield are no longer accurate. The U.S. Federal Trade Commission has taken the position that a statement of Privacy Shield certification or compliance—for example, in a company's online privacy policy—must be true, or the statement violates U.S. consumer protection law. All such statements must now be reconsidered.

- Companies may want to start identifying for which jurisdictions they rely on the Standard Contractual Clauses for cross-border transfers and, of those, whether any have local laws that could ultimately render reliance on SCCs invalid.

- Given that the challenge to Privacy Shield and the SCCs has been pending for some time, some organizations have already adopted a "belt and suspenders" approach—that is, certifying under Privacy Shield but also enacting SCCs and BCRs where feasible. Organizations in this position, especially those relying on BCRs, may be less directly affected by today's decision.

- Perhaps the most immediate challenge is this: As a practical matter, some companies today rely only on Privacy Shield for data transfers that are mission-critical to daily business operations. Such companies may feel they have no choice but to continue making the transfers while all this gets sorted out. That tees up the question of whether such companies face legal risk for future transfers. The EU's data protection authorities ("DPAs"), a/k/a the privacy enforcement agency of each EU member state, will hopefully issue guidance on this soon. When Safe Harbour fell, the DPAs stood down in terms of enforcement action to allow for the creation of Privacy Shield as a replacement mechanism.

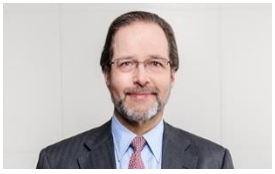
- It is worth keeping in mind that the culture surrounding private litigation risk in the EU is considerably heightened since Safe Harbour fell—meaning that even if DPAs are not willing to take action, private litigants might be. The need to take a proactive approach to addressing these issues might therefore be more pressing than it was last time around.

- Today's decision may intensify discussion in U.S. political circles about whether to (finally) adopt a national privacy law on par with GDPR. Such a law has been long discussed in the U.S. Congress, but has never gotten seriously close to passage. A national U.S. privacy law that passed muster with EU authorities—meaning that the law includes meaningful limits on U.S. intelligence and law enforcement access to personal data—could be the solution that cuts the Gordian knot.

Watch this space. We will continue to assess the impact of the decision and report any relevant guidance from the United States or the EU on the blog.

* * *

Please do not hesitate to contact us with any questions.


Jeffrey P. Cunard
jpcunard@debevoise.com


Luke Dembosky
ldembosky@debevoise.com


Jeremy Feigelson
jfeigelson@debevoise.com


Avi Gesser
agesser@debevoise.com


Jim Pastore
jjpastore@debevoise.com


Dr. Thomas Schürrle
tschuerrle@debevoise.com


Alexandre Bisch
abisch@debevoise.com


Christopher Garrett
cgarrett@debevoise.com


Fanny Gauthier
fgauthier@debevoise.com


Anna R. Gressel
argressel@debevoise.com


Robert Maddox
rmaddox@debevoise.com


Dr. Friedrich Popp
fpopp@debevoise.com