Cybersecurity, Privacy & Data Protection Alert

October 30, 2015

United States and European Union Reach Agreement in Principle for Continued Transatlantic Data Transfers Following Safe Harbor Invalidation

In the wake of the European Court of Justice's ("CJEU") landmark decision of *Schrems v. Data Protection Authority* earlier this month, the EU Justice Commissioner Vera Jourova announced this week that the EU has "agreed in principle" with the U.S. on a new trans-Atlantic data transfer agreement. The *Schrems* ruling sent shockwaves across the Atlantic when it invalidated the 15-year old U.S.-EU Safe Harbor Framework (the "Framework"). Since the year 2000, thousands of U.S.-based multinational companies had relied on the Framework to transfer consumer and employee data of EU citizens across the Atlantic in compliance with the European Commission's Directive on Data Protection ("Directive"). Following the *Schrems* ruling, more than 4,000 U.S. companies that had been certified under the Framework and were transferring data pursuant to their certification found themselves scrambling to interpret the full import of the CJEU pronouncement and evaluate viable alternatives for transatlantic data transfers containing the personally identifiable information of EU citizens.

The Framework was established by the U.S. Department of Commerce and the European Commission in 2000 after the EU declared that the United States did not guarantee "adequate" levels of protection for personally identifiable information under the Directive. Pursuant to the Framework, companies could self-certify compliance with EU data protection standards in order to transfer European data to the United States. The Framework had been the subject of criticism for many years, resulting in protracted negotiations between the United States and the European Commission over the last two years regarding an updated Framework ("Safe Harbor 2.0"). *Schrems* was fueled by the Edward Snowden revelations about global NSA surveillance, and the CJEU ultimately found that personal data protections under the Framework were not "adequate" due to U.S. law enforcement surveillance and national security practices. Following *Schrems*, many privacy advocates questioned the continued possibility of reaching agreement on any Safe Harbor 2.0, which, prior to the CJEU ruling, was nearly complete, but for an agreement on national security access to data transferred to the United States.

Following the *Schrems* decision, which took effect immediately after its issuance, many previously certified companies—especially those that may not have had other compliance mechanisms, such as Binding Corporate Rules or Model Contracts in place—began operating under a cloud of operational uncertainty. Many U.S. lawmakers expressed disappointment in the decision and ruminated about the suffocating ramifications on the global digital economy. Many companies became especially concerned with the potential for disparate enforcement of EU privacy regulation among the 28 different EU Data Protection Authorities (DPAs), given the widely differing approaches to privacy protection and enforcement in some of those member countries. Indeed, in the wake of the *Schrems* decision, regulators

in Germany and the United Kingdom issued statements and guidance adopting seemingly divergent tones regarding future enforcement and the viability of alternative data transfer vehicles, such as Model Contracts.

The Article 29 Working Party ("Working Party")—the collective body of all EU DPAs—published a statement shortly following the *Schrems* decision, calling on EU and U.S. regulators to enter discussions aimed toward reaching solutions to enable data transfer while still respecting fundamental human rights. The Working Party reiterated that "the question of massive and indiscriminate surveillance" is a "key element" of the *Schrems* decision and noted that such surveillance is "incompatible with the EU legal framework." The Working Party stated that any solutions reached "should always be assisted by clear and binding mechanisms, and include at least obligations on the necessary oversight of access by public authorities, on transparency, on proportionality, on redress mechanisms and on data protection rights." Ultimately, the Working Party added to the sense of urgency felt by already-anxious U.S. companies by setting a deadline of January 2016 to reach an appropriate solution with U.S. authorities. The Working Party stated that if, by the end of January, no solution is found, and depending on the DPAs' assessment of alternative data transfer tools, the national DPAs "are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions."

Meanwhile, on October 20, 2015, the U.S. House of Representatives passed the Judicial Redress Act, which would give citizens of countries closely allied with the United States the same legal rights enjoyed by U.S. citizens under the Privacy Act of 1974, including a private right of action against certain U.S. agencies for mishandling their personal information. The bill will now move to the U.S. Senate for consideration and approval. However, some commentators have cautioned that the bill does not sufficiently address the concerns over law enforcement and intelligence conduct highlighted by the CJEU in *Schrems*.

Federal Trade Commission (FTC) Commissioner Julie Brill gave a keynote address at the Amsterdam Privacy Conference last week, shedding light on her views regarding the path forward after *Schrems*. In short, she said that the *Schrems* decision has highlighted "the need to have an honest conversation about the strengths and weaknesses of privacy protections on both sides of the Atlantic." She noted that the aim should be to create "a new data transfer mechanism that strengthens the privacy protections that were in the Safe Harbor principles," and she expressed her belief that "both sides understand the need to ensure that these substantive protections are more robust, and that both sides have been working to that end."

Indeed, following closed-door discussions, just this Monday, the EU announced that it had "agreed in principle" with the United States on a new trans-Atlantic data transfer agreement. Working groups are now discussing the final technical points to ensure that the new framework complies with the *Schrems* ruling, including the extent of protection of EU citizens' personal information from U.S. law enforcement and intelligence agencies. However, it is unclear how much legal certainty this new transfer pact will guarantee if, as the CJEU in *Schrems* declared, individual EU DPAs must be able to investigate and

potentially suspend personal data transfers with "complete independence." EU Justice Commissioner Vera Jourova stated that the new transfer regime would include stronger oversight by the U.S. Department of Commerce and FTC, as well as greater cooperation between EU DPAs and U.S. authorities. "This will transform the system from a purely self-regulating one to an oversight system that is more responsive as well as proactive and back[ed] up by significant enforcement, including sanctions," she said. She noted that the "biggest challenge in the judgment" is placing clear limits on law enforcement access to personal data and ensuring adequate safeguards and oversight. Ms. Jourova did not give a certain date by which the agreement will be complete, but noted that she expected significant progress on the remaining issues in time for her visit to Washington, D.C., in mid-November.

At this week's currently ongoing 37th International Data Protection and Privacy Commissioners' Conference, data protection and privacy commissioners from around the world gathered in Amsterdam to continue discussions over EU-U.S. data transfer solutions. Discussions involved a joint report by EU and U.S. academics titled *Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solutions* (the "Bridges Report"), which advocates for a data protection approach involving continued reliance on existing laws coupled with industry self-regulation. The Bridges Report had been drafted prior to the *Schrems* decision; its publication just two weeks after *Schrems* was coincidental. The Bridges Report is not without critics, and a group of EU and U.S. digital rights organizations and consumer NGOs issued a statement voicing their concerns over report as "out of touch with the current legal reality."

Given the uncertain and dynamic nature of the post-*Schrems* international data privacy landscape and the impending release of a new EU-U.S. data transfer agreement, U.S. companies transferring data from the EU to the United States should remain vigilant in monitoring new developments and evaluating their compliance efforts. Akin Gump Strauss Hauer & Feld LLP lawyers can provide valuable assistance to organizations in navigating these murky waters and ensuring compliance with existing and emerging EU data protection regulations.

Contact Information

If you have any questions regarding this alert, please contact:

Davina Garrod
davina.garrod@akingump.com
+44 20.7661.5480
London

Natasha G. Kohne
nkohne@akingump.com
+971 2.406.8520
Abu Dhabi

Michelle A. Reed
mreed@akingump.com
214.969.2713
Dallas

David S. Turetsky
dturetsky@akingump.com
202.887.4074
Washington, D.C.

Hal S. Shapiro
hshapiro@akingump.com
202.887.4053
Washington, D.C.

Francine E. Friedman
ffriedman@akingump.com
202.887.4143
Washington, D.C.

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
202.887.4220
Washington, D.C.

Kelli A. Kiernan
kkiernan@akingump.com
415.765.9569
San Francisco