Armstrong Teasdale

February 2, 2016 • Advisory • www.atllp.com

EU-U.S. REACH DEAL ON SAFE HARBOR 2.0 - PACT CREATES NEW DATA TRANSFER FRAMEWORK

After months of uncertainty triggered by the now infamous *Schrems* decision by the European Court of Justice (ECJ), the EU Commission and the U.S. Department of Commerce have reached an agreement with respect to the transfer of consumers' and employees' personal data from Europe to the United States. What will be known as the "Privacy Shield" comes just in the nick of time, as EU data protection authorities ("DPAs") had threatened the aggressive enforcement activity if the January 31 self-imposed deadline to reach agreement was not met.

Last year the ECJ invalidated the transatlantic EU-U.S. Safe Harbor Framework that permitted U.S. companies to transfer consumers' and employees' personal data from Europe to the United States under a presumed level of "adequate" privacy protection if they certified compliance with a set of privacy principles similar to those contained in the EU Data Protection Directive ("DPD").

The decision was the culmination of a 2013 lawsuit brought by privacy activist Max Schrems against the Irish DPA. In his suit, Schrems alleged that Facebook had violated his privacy rights by permitting his personal data to become subject to one of the mass surveillance programs of the U.S. National Security Agency. Although the Irish DPA initially rejected the case, Schrems appealed the matter to the Irish High Court, which in turn referred to the ECJ the specific question of whether the respective European DPAs had the authority to investigate and suspend transfers of personal data under the Safe Harbor Framework without limitation by the EU Commission. On October 6, 2015, the ECJ answered that question in the affirmative and then went a step further by declaring the 2000 implementation of the Safe Harbor Framework invalid, thereby nullifying its legal basis.

Since that time, U.S. companies have been scrambling to understand and implement other EU-approved alternative transfer mechanisms, such as Binding Corporate Rules ("BCRs"), standard contract clauses ("Model Contracts"), and statutory derogations, in order to stay compliant with the DPD. This scrambling has come at great cost and disruption for U.S. companies hoping to avoid interruptions in their transatlantic business and data flows.

While the exact terms of the deal have not yet been drafted, the negotiations

PEOPLE

Jeffrey Schultz, CIPP/US

Lucas Amodio, C|EH

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

in recent weeks have focused on four major sticking points:

- The creation of an independent ombudsman designed to oversee and investigate complaints from EU citizens about the use of their personal data by U.S. companies;
- Limitations to the degree and scope of access by U.S. law enforcement authorities to the personal data of EU citizens transferred to the United States;
- The creation of a redress mechanism of "last-resort," should EU citizens be unable to resolve complaints against U.S. companies through the traditional means of an alternative dispute resolution mechanism; and
- Commitments from U.S. at the "highest political level" and the publication of these commitments in the Federal Register so that the agreements are perceived as formal and legally binding, rather than voluntary.

Despite reaching an agreement in principle, much uncertainty remains across the data privacy landscape. For starters, the devil is in the details, and the negotiators still need to draft the agreement in the ensuing weeks. Next, the Article 29 Working Party, which is comprised of representatives from the DPAs of the 28 EU Member States, meets today and tomorrow to discuss how to regulate transatlantic data flows in the post-Schrems world. It has indicated that it will be specifically addressing the validity of BCRs and Model Contracts in light of the *Schrems* decision. Third, fears clearly remain that the new "Privacy Shield" framework will suffer the same fate as the Safe Harbor and be invalidated by the EU courts. Finally, and perhaps most importantly, all of these developments are taking place against the backdrop of the newly-minted European General Data Protection Regulation ("GDPR"), which is set to take effect in 2018 and carries with it significant compliance hurdles that U.S. companies will be forced to face, not to mention draconian penalties for non-compliance, including fines amounting to 20 million Euros or 4 percent of a company's total worldwide annual turnover.