Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

EU Privacy Shield Gets Good Marks, For Now

By **Allison Grande**

Law360, New York (October 19, 2017, 8:47 PM EDT) -- The European Commission gave mostly glowing reviews in its first-year report on the U.S.-EU Privacy Shield data transfer system, but legal experts say there's a chance that lingering national security worries in Europe could give detractors of the pact the chance to strike it down.

The European Commission on Wednesday revealed the conclusion drawn from a joint review of the pact last month, saying that while Privacy Shield adequately protects data that flows between the continents, there remain nagging worries about the U.S. government's access to Europeans' personal data and the way that the pact is being overseen.

Privacy experts characterized the review as good news for Facebook, Google, Microsoft and the roughly 2,500 other companies that took the plunge to sign up for the Privacy Shield, which replaced the former safe harbor program after it was judged inadequate by the European Court of Justice in 2015.

"This will provide some welcome relief to U.S. companies that have joined the Privacy Shield as well as to EU-based companies relying on it," London-based Hogan Lovells partner Eduardo Ustaran said about the Privacy Shield review.

The Privacy Shield isn't out of danger, however, attorneys noted. The group of national data protection regulators known as the Article 29 Working Party, which has expressed skepticism about the deal in the past, is expected to offer its own take on the agreement, and court challenges mounted by EU citizens such as Max Schrems, the Austrian lawyer and activist who launched the case that killed safe harbor, are not yet off the table.

"The [European Commission's] recommendations will do little or nothing to assuage the concerns of privacy advocates that the [Shield's] privacy safeguards are inadequate," said Thomas G. Jackson, a litigation partner and chair of the technology practice group at Phillips Nizer LLP.

Companies that elected to certify to Privacy Shield last year knew about these well-documented criticisms of the deal, and were anxiously awaiting the commission's assessment as an important indicator of whether the deal had staying power.

The Shield largely passed this first test, with the commission concluding that the pact "continues to ensure an adequate level of protection for the personal data transferred from the EU to participating

companies in the U.S." The commission particularly praised U.S. authorities for implementing the new redress options for EU citizens required by the deal and for keeping in place "relevant safeguards" for limiting access to this data by U.S. authorities for national security purposes.

"The EU Commission's favorable review of the Privacy Shield should be taken as an encouraging step in ameliorating transatlantic data transfer anxiety," Sidley Austin LLP partner Alan Charles Raul said.

The commission's decision to make no changes to the underlying principles of the deal is likely to provide a boost not only for the companies that have already self-certified their compliance to the deal and can easily continue to forge ahead, but could also help Privacy Shield reach the membership level of its safe harbor predecessor, which was relied on by more than 7,000 multinationals at the time of its downfall.

"If I were a company that was already signed up for this, I would have more comfort and the review would be encouraging, and if I were on the fence about participating, this might tip me forward," said Timothy Toohey, the head of Greenberg Glusker Fields Claman & Machtinger LLP's cybersecurity practice.

The commission's backing of Privacy Shield is especially vital in light of the uncertainty surrounding another popular transatlantic data transfer mechanism known as standard contractual clauses. Schrems, the privacy advocate who successfully challenged safe harbor, lodged a complaint with the Irish data protection authority concerning Facebook's use of these clauses, and earlier this month, the Irish high court referred that dispute to the EU Court of Justice for a ruling on the mechanism's validity.

According to a recent privacy governance survey conducted by the International Association of Privacy Professionals and Ernst & Young, 88 percent of companies that transfer personal data from the EU to the U.S. and other non-"adequate" countries rely on standard contractual clauses as a valid method for doing so. With the fate of this mechanism now on shaky ground, more companies may start looking to Privacy Shield, experts say.

"The bottom line is that while there is optimism with respect to the Privacy Shield and there's been a good result for the first review, there's still a cloud of uncertainty hanging over the continuation of transatlantic data flows under the current framework," said Omer Tene, vice president of research and education at the IAPP.

That uncertainty extends to the Privacy Shield as well, despite the commission's willingness to continue to support the Shield, attorneys say.

"The European data privacy regime is very protective of individuals and their privacy rights," said Morgan Lewis & Bockius LLP partner Pulina Whitaker, who is based in London. "The European objective is that these rights should not be watered-down on the transfer of their data to the U.S."

This approach was apparent in the 10 recommendations in both the commercial and national security areas that the commission made for improving how the Privacy Shield functioned, according to attorneys.

These suggestions included pushing the U.S. government to enshrine a presidential policy directive signed in 2014 to curb foreign intelligence abuses into Section 702 of the Foreign Intelligence Surveillance Act, which expires at the end of the year, and that the Trump administration take steps to

staff the Privacy and Civil Liberties Oversight Board and appoint an ombudsperson at the U.S. Department of State to handle national security complaints.

"The European Commission has thrown out a lifeline for the U.S. administration to pick up," said Monika Kuschewsky, a partner in Squire Patton Boggs' global data privacy and cybersecurity practice, who is based in Brussels.

Raul noted that the commission's continued focus on national security and surveillance issues could be in part a result of who participated in the review last month. While the U.S. delegation included representatives of the intelligence community, "there was no reciprocal involvement of European intelligence officials in the EU delegation," he said.

"This imbalance of privacy interlocutors is one explanation why the EU persists in addressing U.S. surveillance without any comparative consideration of the surveillance practices and safeguards, or relative lack thereof, on the EU side," Raul added.

Aside from national security concerns, the commission also laid out several recommendations related to how those companies that implement the Privacy Shield should be monitored.

Specifically, the commission suggested that businesses should not be allowed to publicly announce that they are Privacy Shield-certified until the U.S. Department of Commerce has finalized their certification, and that the Commerce Department conduct compliance checks on a "regular basis" and work more closely with EU data protection authorities to both develop compliance guidance for companies and raise awareness among individuals about how to exercise their right to redress.

"In reviewing the commission's announcement with a particular focus on looking for what it means for companies that are certified to the framework, the most significant points are that the review is a good indication that the framework will continue to be available and that there's going to be a request that the Department of Commerce focus on companies that may claim to be Privacy Shield-certified but might not be," said Kendall Burman, a Mayer Brown LLPcounsel and former deputy general counsel for the Commerce Department under the Obama administration.

Kuschewsky agreed that, in terms of business impact, self-certified companies will perhaps be most eager to see how, in particular, the recommendation on proactive and regular monitoring of compliance by the Department of Commerce will play out.

"The European Commission's recommendations in this respect includes requiring self-certified companies to respond to compliance review questionnaires or file annual compliance reports with the Department of Commerce, which would place an additional burden on these companies to demonstrate compliance," she said. "Companies should also be careful not to publicize their Privacy Shield certification before the certification is finalized, given the recommendation of regular 'searches' to be carried out on companies not yet certified."

The Federal Trade Commission, which along with the Department of Commerce has responsibility for overseeing the pact, has to date focused primarily on technical violations stemming from allegations that companies are falsely claiming to be in compliance with the Privacy Shield as well as its predecessor, safe harbor.

Acting FTC Chairman Maureen Ohlhausen in a statement Wednesday called enforcing international

privacy frameworks such as Privacy Shield "an integral part" of the regulator's privacy and data security program, and reinforced the commission's commitment to continuing to work with its European counterparts to ensure that the Privacy Shield remains "a robust mechanism for protecting privacy and enabling transatlantic data flows."

"So far, the vast majority of the FTC's actions in this space have been focused on technical violations of the safe harbor and Privacy Shield, including failing to recertify or falsely stating certification, as opposed to actual substantive violations," Tene said. "There's no reason to think they'll abandon enforcement actions now, but the big question will be whether they will actually increase scrutiny."

Debbie Reynolds, director of eDiscovery at Eimer Stahl and adjunct professor at the Georgetown University School of Continuing Studies, said the next 12 months would be key to watch.

She flagged events such as if and how the U.S. government will implement the EU Commission's recommendations, a potential decision in the standard contractual clauses challenge at the EU high court, an opinion on the Privacy Shield by the Article 29 Working Party, and the implementation in May of the EU's general data protection regulation, which will require multinationals that do business in the bloc to adhere to stricter rules for handling and transferring EU citizens' data.

"It will be interesting to see how GDPR plays into everything, since unlike Privacy Shield it's not voluntary and it sets a higher privacy bar to meet," Reynolds said. "For companies that are pursuing the types of privacy protections that are in Privacy Shield and GDPR, they should be fine, but for those who are not thinking along those lines, it will probably be a rocky year."

--Editing by Philip Shea and Catherine Sum.