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

Privacy Shield Shelf Life In Question Despite EU Approval

By **Allison Grande**

Law360, New York (July 8, 2016, 10:51 PM ET) -- European Union member states on Friday set the stage for the new trans-Atlantic Privacy Shield data transfer pact to take effect in the coming days, providing a strong but potentially fleeting measure of comfort for multinationals such as Google and Facebook that have been in limbo since the popular mechanism that they had long relied on was struck down last year.

The vote to support the carefully negotiated Privacy Shield deal by the collective of member state representatives known as the Article 31 committee catapulted the agreement over its most difficult hurdle. While EU data protection authorities and lawmakers have voiced concerns about the Privacy Shield, only the member states had the power to block its implementation, making their backing vital.

Barring any last-minute surprises, the EU's College of Commissioners is expected to issue a decision Monday finding the Privacy Shield to provide an adequate level of privacy protection, which would open the door for representatives from the European Commission and U.S. Department of Commerce to meet Tuesday to formally sign the agreement. That final step would clear the way for the thousands of multinationals that depended on the safe harbor mechanism that was invalidated by the European Court of Justice in October to begin using the pact to support their cross-border data transfers, an opportunity that attorneys expect many businesses to seize.

"The Privacy Shield is certainly going to be a viable option for many companies," Herbert Smith Freehills LLP partner Joe Falcone said. "While there are other transfer options such as model contracts and binding corporate rules, for companies that took comfort in safe harbor, they are likely to find that comfort again in Privacy Shield."

But while the Privacy Shield is likely to be an enticing and cost-effective way for many companies to support their exchanges of data across the Atlantic, the decision to jump full force into the new regime doesn't come without a major caveat: the very real risk that the Court of Justice may deem the new arrangement invalid as well.

Max Schrems, the Austrian law graduate and activist who led the successful charge against the old safe harbor, has already vowed to mount a similar challenge to any finalized replacement deal, and the chance of the Privacy Shield ending up back before the high court is widely seen as inevitable.

"One of the most interesting aspects of the deal will be its shelf life," McCarter & English LLP partner and privacy group co-head Rich Green said. "The big question for companies will be whether they want to wait and see what happens with the Schrems challenge, or if they decide that they want to go ahead

and do Privacy Shield."

The answer to that quandary is likely to be different for each company, based on factors such as how well-positioned they are to comply with their enhanced commitments and obligations under the Privacy Shield and how much legwork they've done in recent months to find another way to legally transfer data between the U.S. and EU.

If a company has not taken steps to put into place model contracts and binding corporate rules — which attorneys noted are not a good fit for every company, since they can be costly and don't cover every kind of data transfer — then they are likely to be left with little choice but to embrace the Privacy Shield, especially in light of the substantial legal risk that is likely to stem from transferring data without any mechanism in place.

"Given the lengthy period of uncertainty while the shield was being negotiated, companies needed to put a mechanism in place to transfer data or risk immediate noncompliance," said Lisa Sotto, head of Hunton & Williams LLP's privacy and data security practice.

Regulators in the EU and U.S. have repeatedly signaled that doing nothing to counter the safe harbor's invalidation will not be viewed favorably, and the Hamburg data protection commissioner has already driven home this point by fining three companies in June for ignoring the safe harbor's demise and continuing to transfer data as before.

"Companies really have no choice, especially given the recent push to enforce and to impose penalties for violations of data transfer restrictions that we saw in Germany, but to have a valid mechanism in place," said Behnam Dayanim, co-chair of Paul Hastings LLP's privacy and cybersecurity practice. "So for companies that don't think they can rely on model contracts, they really do have to adopt Privacy Shield."

On the other hand, companies that have turned to model contracts in the wake of the safe harbor's downfall may choose to "sit on the sideline" until the dust settles on the legal challenge since "they have no immediate need to adopt Privacy Shield," Dayanim noted, although he did point out that the validity of model contracts is also currently being reviewed by the EU high court in the wake of a follow-up action by Schrems.

The thousands of businesses that turned to the safe harbor at some point during its 15-year lifespan are also likely to be more willing and more prepared to sign up for the Privacy Shield, attorneys noted.

While the new agreement will impose stronger obligations on U.S. companies to protect the personal data of Europeans, the requirements are not that far afield from both what the safe harbor required and what many of the more stringent privacy regimes in the U.S. — namely those that cover data held by health care providers and financial services companies — already require.

"If you're a company that had self-certified under safe harbor, it's going to be fairly easy to meet the requirements under Privacy Shield because you've already done all the homework," Green said. "I'm not seeing a ton of new burden for businesses."

While the European Commission and Department of Commerce did release the 128-page draft of their original Privacy Shield proposal a month after they unveiled the deal in February, the sides have since revamped the deal to address concerns raised by EU regulators and others, and that new text has yet to

be publicly released.

But according to details gleaned from the original text and statements from the negotiators, the final Privacy Shield pact is likely to impose stronger notice, purpose limitation, data retention and security requirements on businesses that agree to adhere to the deal. Enforcement will also be ramped up, with the Department of Commerce and European data protection authorities given an enhanced role to police the program along with the Federal Trade Commission, which was primarily responsible for enforcing the old safe harbor deal.

"Enforcement is likely to be stepped up for many reasons, one of which will be that the regulators want to show that the Privacy Shield is a real improvement over safe harbor, and they'll be very conscious of ensuring that they do that," Dayanim said.

But despite the increased scrutiny, attorneys say that companies for the most part should face little backlash as long as they review their policies and take steps to not only implement but also execute the high standards required by the new deal.

"The core principles of Privacy Shield are really about doing a legitimate and serious job of protecting personal information," Barnes & Thornburg LLP partner Brian McGinnis said. "As long as companies are generally geared toward understanding the ground rules and are enacting policies and practices that meet the principles, companies and regulators should be on the same page."

A pair of potential areas of concern for companies center on the enhanced restrictions for onward transfers of data and the new channels for Europeans to raise their complaints about data misuse, both of which are unique to the Privacy Shield.

The onward transfer provision will require companies to put into place contracts with vendors that may receive data after it has been transferred from the EU to the U.S., while the new avenues for redress — including one that allows EU consumers to file a direct complaint that the company must answer within 45 days — will force businesses to set up procedures to be able to field these inquiries.

"For some companies, the new redress is going to be something that they will have to focus extra attention and potentially resources on," Mayer Brown LLP cybersecurity and data privacy counsel Kendall Burman said. "During the past year, everyone has become more attentive to these issues, and I wouldn't expect that to change."

It's no mistake that the redress and onward transfer provisions, as well as commitments from the U.S. about the robust safeguards and limitations that will be in place to prevent unfettered access to transferred data by U.S. law enforcement and intelligence officials, feature prominently in the Privacy Shield. The negotiators have long said that they were building the Privacy Shield with an eye toward an inevitable court challenge, and the additions of these elements are intended to help insulate the pact from the criticisms over U.S. government surveillance that felled the safe harbor mechanism.

"The length and depth of the negotiations leading to the final version of the Privacy Shield reflects careful consideration of the EU's concerns about personal data transferred from the EU to the U.S. via the shield," Sotto said. "The final product shows the significant efforts on the part of the negotiators to address all outstanding concerns so as to leave little room for questions as to the adequacy of the protections provided by the shield to EU residents' personal data."

But even if the new pact is eventually struck down as inadequate, attorneys still predict that buy-in from companies hungry for a replacement to safe harbor will ultimately be high.

"When safe harbor was first adopted in 2000, a lot of companies weren't sure about it and some were uncomfortable about certifying because they were worried about sticking their head above the parapet and having it chopped off," Dayanim said. "The world is in a different place today, with companies being much more savvy and realizing that having nothing in place is not viable. I don't think we'll see that kind of hesitation with Privacy Shield."

--Editing by Mark Lebetkin and Aaron Pelc.
