Legaltech news

🖶   Click to Print or Select '**Print**' in your browser menu to print this document.

Page printed from: *Legaltech News*

Privacy Shield Certifications Begin Aug. 1, but Experts Warn of Shaky Legal Ground

Many believe the agreement's privacy protection assurances and obscure redress mechanisms will soon face challenges in EU Courts.

Ricci Dipshan, Legaltech News

July 12, 2016

Coming on the heels of EU's Article 31 Committee endorsement, EU and U.S. officials officially approved the Privacy Shield today. While the agreement will take effect immediately, U.S. organizations will be able to certify with the Department of Commerce starting Aug. 1. The approval marks the end of a monthslong process that included sharp rebukes over initial language and a breakthrough in negotiations on the day the UK voted to leave the EU .

But far from instilling confidence in transatlantic data transfers, experts are warning that the agreement may be on shaky legal ground.

A part of the apprehension was from uncertainty over the final language itself, Don Aplin of Bloomberg Law explained. "The commission didn't immediately release the text of the document approved by the Article 31 Committee. So even though there was an expectation that the commission had worked to address concerns EU privacy officials raised in response to the initial agreement released in February, there wasn't any clarity until the commission released the text."

Without the text, many were left to decipher Privacy Shield changes through the broad statements released by public officials.

Linda Sharp, associate general counsel at enterprise information governance technology provider ZL Technologies, for example, questioned what "'equivalent' protections that would have been availed had the data been stored in the EU" meant in the context of the agreement.

Another area she is concerned about is "ongoing communications between employees within an organization or across organizations wherein there are cross-border transfers. There is no clear indication as to whether the Privacy Shield applies in these situations any more than when the Safe Harbor was in play."

While the updated text was made public on July 12th, the documents sent to the Article 31 Committee were leaked earlier, "strategically dropped into certain people's mailboxes, so it's not like no one [knew it], word for word, but they kept it to a very small community," said Gregory P. Bufithis, managing director of eTERA Europe.

He added that it will take a significant amount of time for this select group to get through the

agreement's complicated text. "You need to remember that the actual Privacy Shield is contained in the EU Commission's draft adequacy decision, so it's part of a very large and complex series of documents that have annexes to the annexes to the annexes —the thing runs over 200 pages. There are whole series of commitments and explanatory notes, etc.," Bufithis said.

Privacy: The Agreement's Achilles Heel?

While there is still much to understand, experts are already seeing cracks in the Privacy Shield's structure.

[In a statement released online](#) , U.S. Secretary of Commerce Penny Pritzker said that "with new privacy protections in place, we are confident the framework will withstand further scrutiny."

Bufithis disagreed, noting that the privacy protections, especially in regards to mass surveillance, did not go as far as the EU wanted, and may ultimately be short-lived.

"The EU side obviously wanted legislative changes, and the U.S. was adamantly opposed to that. So what you basically have is a bunch of assurances by the Obama administration, you have assurances by [Secretary Pritzker], you have a promise by the director of the office of national intelligence — so you have a lot and lot of promises and, as you well know, those promises can be undone in a heartbeat," with a new U.S. administration.

"Some of my privacy contacts and some of the people I work with on this through the EU parliament are thinking that this will go to court pretty fast, that it doesn't meet the European Court of Justice safeguard requirements. And even people on the commission will tell you the same thing," he added.

Bufithis, who is both a U.S. and EU national and practices law in both areas, noted that, to bring a data violation complaint in the EU, there is a clear path from a country's data protection administrators to an appeals court to, ultimately, the European Court of Justice, "pretty much what Max Schrems had to do."

However, "making a parallel case with respect onto a U.S. process—yes, there is an ombudsman now installed that allegedly is going to be a very independent individual, who is going to hear various EU complaints about people who say 'My data has been violated.' … But it's a very obscure and not transparent process."

Concerns over privacy protections was apparent in the Article 31 Committee, whose endorsement of the agreement was far from unanimous. "There were four abstentions. There was a lot of haggling and a lot of discord, and four countries basically said, 'We're not going to vote; we're just going to abstain.' The feeling was [that] this thing will take its normal course," Bufithis said.

Whether it stands in the near future is anyone's guess. "I think the Max Schrems case was simply a warmup," he said, adding that the legal teams that aided the Schrems case against Safe Harbor "will be a lot quicker on their feet and organized" in fighting the Privacy Shield.

Bufithis also cautioned that Privacy Shield litigation might not be the only impactful court action to watch on EU and U.S. data regulation.

"I think [a] more important case is the Microsoft Ireland case, with the Department of Justice fighting to say data stored in Ireland is subject to U.S. access because you are a U.S. company and we have access to wherever the data is. That case, I think, is far more paramount than Privacy Shield, because if Microsoft wins, then game over, then basically everyone will be hiding their data over there."