Privacy, Data Security & Information Use

August 15, 2016

The EU's Data Transfer "Privacy Shield"—Full Body Armor or a Candle in the Wind?

By Rafi Azim-Khan, Mercedes Tunstall, Steven P. Farmer and Andrew Caplan

With the August 1st start of the Privacy Shield, the European Commission's new and long-awaited transatlantic data transfer agreement with the U.S., businesses that had previously relied on the invalidated Safe Harbor scheme now have a similar option available again. U.S. companies subject to Federal Trade Commission or Department of Transportation jurisdiction can begin to self-certify with the U.S. Department of Commerce that they comply with the Privacy Shield's data privacy and security requirements, thus enabling them to transfer EU citizen data to the United States lawfully. However, looming legal challenges and an annual review of the Privacy Shield may well undermine the value of the program as a long term compliance solution.

Although self-certifying for the Privacy Shield will ensure transatlantic transfers are lawful in the short term, U.S. companies are therefore advised to continue considering and implementing other compliance solutions (such as Binding Corporate Rules or Model Contract Clauses) to legitimize transatlantic data transfers for the time being.

By doing so, should the Privacy Shield be challenged as is expected, or ultimately invalidated, U.S. importers and European exporters of data will be well-positioned to continue lawfully processing EU citizen data.

Background

As we discussed in a previous client alert, the Privacy Shield replaces the EU-U.S. Safe Harbor Framework, which the European Court of Justice (CJEU) invalidated last October after Facebook practices were legally challenged by Max Schrems, on the basis that the Safe Harbor Framework did not provide an "adequate" level of protection to EU citizens' personal data. This decision was heavily informed by the Edward Snowden revelations regarding the United States government's bulk data collection practices. In

addition to the CJEU's focus on U.S. government handling of EU citizen data, and EU citizens' corresponding lack of redress, it also coincided with growing EU regulator frustration at a perceived lack of compliance with EU data law generally and particularly by U.S. companies, which in turn has led to increased enforcement activity and the recent approval of new law and much more serious sanctions (which will be the subject of future alerts).

The Privacy Shield and U.S. Government Data Collection

The Privacy Shield departs most significantly from its predecessor with respect to the U.S. government's own activities involving EU citizen data. A central pillar supporting the EU's acceptance of the Privacy Shield is the U.S. intelligence community's assurance that new measures have been put in place to restrict indiscriminate, bulk collection of EU citizen data, while offering EU citizens greater abilities to obtain redress for alleged improprieties.

Indeed, the majority of the 104-pages comprising the Privacy Shield consist of commitments from United States Federal agencies. Notably:

- The Office of the Director of National Intelligence cites to recent legislation and measures under the Obama Administration, requiring, among other things, that the collection of signals intelligence must be tailored, and that bulk data collection may only be used for specific, enumerated purposes.
- The Department of Justice reiterates that U.S. law enforcement practices are nondiscriminatory in that they apply without regard to the nationality of the data subject.
- To support the implementation of the Privacy Shield, the U.S. Department of State will create a new ombudsperson's office (separate and walled off from the U.S. intelligence agencies) that will field complaints regarding data collection efforts by the U.S. government.

With respect to U.S. government collection of EU citizen data, it has been commented in some circles that the Privacy Shield has been a big improvement, providing U.S. federal agencies with more effective enforcement authority and directives to protect EU citizens' data.

The Privacy Shield and U.S. Companies Collecting EU Citizen Data

Nevertheless, when it comes to U.S. companies collecting EU citizen data, the Privacy Shield has been criticized as not a significant enough departure from the previous Safe Harbor.

The structure of the certification process under the Privacy Shield arguably looks like a Frankenstein-esque resurrection of the Safe Harbor. The seven core principles of Safe Harbor—notice, choice, onward transfer, access, security, data integrity and enforcement—are carried over in Privacy Shield. Of course, these categories are the key elements for allowing for careful control of data and the privacy restrictions related thereto.

In terms of divergence, however, Privacy Shield introduces the requirement that certifying companies must ensure that if EU citizen data is being shared with a third-party service provider, then that service provider is following the same requirements as the certified company.

There is also a new dispute mechanism regime, pursuant to which certifying companies must provide no-cost arbitration to EU citizens who wish to challenge the effective processing of their data by the company.

Should the arbitration not resolve adequately, the dispute mechanism provides for a "last ditch" arbitration panel, administered by the EU DPAs themselves.

For companies looking to certify under the Privacy Shield, the most work will likely involve creating a Privacy Shield-compliant privacy policy and establishing arbitration protocols. Significant time will also likely be spent reviewing which third parties are touching EU citizen data and determining whether it is better to revise the data processing flows or the contracts with such third parties. Companies that certify for Privacy Shield within the first 60 days (i.e., before October 1, 2016) will be granted a nine-month period to conform third-party relationships, thus providing a marked incentive for early adoption.

Is Privacy Shield the Right Move?

Privacy Shield arguably provides a step forward from the Safe Harbor Framework. U.S. companies that relied upon the previous Safe Harbor to legitimize transatlantic data transfers will be well-positioned to undertake the Privacy Shield certification, and, with new enforcement threats out there, U.S. companies that have never looked carefully at their processing of EU citizen data may realize that they need to certify under the Privacy Shield, even if they never thought about certifying under the Safe Harbor.

However, if a business does wish to certify it will almost certainly need to undertake a review of its policies, internal processes and procedures (and update the same) to avoid exposing itself to risk given the obligations and likely sharper enforcement regime under Shield.

It should also be noted that Privacy Shield will almost certainly be subjected to challenges.

Although U.S. Commerce Secretary Penny Pritzker and EU Commissioner for Justice, Consumers and General Equality Vera Jourová have argued that the Privacy Shield will be able to withstand EU legal scrutiny, some EU privacy advocates disagree.

In particular, Privacy Shield critics espouse that the dispute mechanisms, which are not even available to U.S. citizens, are unduly complex, reducing the likelihood that EU citizens will use them.

Moreover, the commitments made by the Obama Administration could easily be watered down by the next presidential administration, thus delivering a blow to many of the central assumptions underlying the EU Commission's approval. Such "watering down" could occur regardless of who is the next U.S. President, in light of the threat of global terrorism.

With the Privacy Shield's built-in annual review mechanism, it is possible that theoretical commitments made in 2016 could be deemed inadequate in practice in the coming years, particularly once the new EU General Data Protection Regulation ("GDPR") is implemented in 2018 and it becomes clear how this affects international data relationships.

With these factors in mind, whilst Privacy Shield certification has some advantages, companies importing data in the U.S. and European exporters might be well advised not to put all their faith in it.

In particular, other transfer solutions such as Binding Corporate Rules or Model Contract Clauses arguably provide much more comfort and certainty for the time being, and these recent developments would appear not to diminish their value in any way.

What should businesses do?

Simply signing up to Privacy Shield without proper consideration would be an unwise move. For numerous reasons, it is not business as usual and it carries increased potential exposure (particularly as enforcement commitments were made as part of the effort to revive a Safe Harbor style scheme).

Even if Privacy Shield may be a good fit in theory, it is important to understand that a good deal of internal assessment and improvements to policies, documents and processes may well be required before looking to certify.

It is equally important to note the other compliance mechanisms that may offer a better fit and greater stability.

Seeking experienced counsel input to assess the pros/cons of each solution and the best fit for a business would be strongly advised and a prudent first step.

If you have any questions about the content of this Alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Rafi Azim-Khan (bio)
London
+44.20.7847.9519
rafi@pillsburylaw.com

Mercedes K. Tunstall (bio)
Washington, DC
+1.202.663.8118
mercedes.tunstall@pillsburylaw.com

Steven P. Farmer (bio)
London
+44.207.847.9526
steven.farmer@pillsburylaw.com

Andrew L. Caplan (bio)
Washington, DC
+1.202.663.8110
andrew.caplan@pillsburylaw.com

Pillsbury Winthrop Shaw Pittman LLP is a leading international law firm with offices around the world and a particular focus on the energy & natural resources, financial services, real estate & construction, and technology sectors. Recognized by *Financial Times* as one of the most innovative law firms, Pillsbury and its lawyers are highly regarded for their forward-thinking approach, their enthusiasm for collaborating across disciplines and their unsurpassed commercial awareness.