Armstrong Teasdale

July 26, 2016 • Advisory • www.atllp.com

DECISION CLEARS PATH FOR COMPANIES TO PARTICIPATE IN THE PRIVACY SHIELD

A critical decision today by European Union privacy officials ends the era of uncertainty for the 4,000 plus U.S.-based companies and the thousands of EU-based companies that formerly relied on the U.S.-EU Safe Harbor Framework to legally transfer personal data to the United States.

In formally adopting the EU-U.S. Privacy Shield on July 12, 2016, the EU Commission cleared the final legal hurdle for the substitute data transfer mechanism to go into effect. To that end, companies that wish to participate in the Privacy Shield may begin the self-certification process with the Department of Commerce starting August 1, 2016.

But perhaps more significant to the future of transatlantic business and data flows was today's decision by the Article 29 Working Party ("WP 29"), comprised of representatives from the data protection authorities ("DPAs") of the 28 EU Member States, to withhold judgment on the adequacy of the replacement framework until at least the summer of 2017. Though having no legal effect, the WP 29's public pronouncement is crucial, as it removes the final clouds of uncertainty hovering over the data transfer mechanism (at least for a time) and clears the path to participation for companies that had been on the fence since the infamous Schrems decision.

Now companies that were concerned that participation would be short-lived because the new framework would suffer the same fate as the Safe Harbor and be invalidated by the EU courts, can devote resources to compliance with the Privacy Shield without the fear that the DPAs in the various EU

PEOPLE

F. Scott Galt, CIPP/E

Jeffrey Schultz, CIPP/US

SERVICES AND INDUSTRIES

International

Data Innovation, Security and Privacy

Armstrong Teasdale

Member States are going to attack their participation in the new regime. Companies that participate are deemed to provide "adequate" privacy protection for the transfer of personal data outside of the EU under the EU's Data Protection Directive.

Instead of poking holes in the framework from the sidelines and fanning the flames of those who feel the new regime does not go far enough, the WP 29 is going to let the process unfold as intended by the U.S. and EU authorities, who will be required to sit down on an annual basis to evaluate the successes and failures of the data transfer pact. The WP 29 has indicated that it will wait until the European Commission has completed its first annual review of the data transfer pact before it revisits the issue of whether the presumed level of privacy protection afforded to EU citizens under the Privacy Shield is "adequate." Companies that wish to participate should now turn their sights on making sure they are in a position to self-certify as soon as possible, but in any event, no later than September 30, 2016. This is because companies that sign up by that date will be given a nine month reprieve by which to bring their contracts with third parties vendors into compliance with Privacy Shield principles.

But before companies are even in a position to self-certify, the first step is to make sure your company is eligible to participate and/or not subject to an exemption. Generally speaking, most companies will be subject to the Federal Trade Commission's enforcement jurisdiction and not subject to a B2B exemption. Next, participating companies will need to identify and select an independent recourse mechanism. Several third party recourse mechanisms exist, including the Council of Better Business Bureaus and the American Arbitration Association, but if your self-certification also covers employee personal data, that information must be made subject to a unique EU-based DPA panel. Third, companies must make sure that their privacy policy appropriately contemplates the Privacy Shield's seven primary and sixteen supplemental privacy principles. While the seven primary principles

are universally known and echo the same principles found in the now-defunct Safe Harbor, the supplemental principles impose significant new obligations on companies familiar with the old regime. Additionally, prior to self-certification, companies must evaluate whether they have the appropriate procedures in place to verify their compliance with the Privacy Shield. This assessment can take place through a self-auditing regime or through an outside third party performing a verification compliance review.