

Brexit and EU Data Privacy

There has been much speculation as to what kinds of long-term impact Brexit could have on Europe and the world. One area that has caused particular concern is data privacy and how Brexit could impact the transition from Safe Harbor to the EU Privacy Shield. Michael Whitener, partner with VLP Law Group, weighs in on Britain's exit from the European Union and what this means for data privacy.

At first glance, the Privacy Shield principles look very similar to Safe Harbor principles, as does the self-certification process required to join the Privacy Shield. Like the Safe Harbor Framework, the Privacy Shield has seven primary principles. However, the Privacy Shield also has 16 "supplemental principles," addressing such issues as consent to process sensitive data, verification procedures and an individual's right to access his or her data. Additional distinctions of the Privacy Shield from Safe Harbor include (1) stricter rules governing so-called "onward transfers" (data transfers from a Privacy Shield-certified company to third parties), (2) limits on U.S. government access to the personal data of EU citizens, and appointment of a State Department Ombudsman to deal with complaints concerning U.S. intelligence practices, and (3) multiple dispute resolution options if an individual believes that Privacy Shield requirements have been violated.

Once the UK exits the EU, it will no longer be subject to the Privacy Shield, so data transfers from the UK to the US will simply be subject to UK law – specifically, UK's Data Protection Act of 1998. However, the UK could nevertheless approve Privacy Shield certification as an adequate means of transferring UK personal data to the US, or come up with its own approval process. In any event, the UK's withdrawal from the EU will take two years or more, so for the time being data transfers from the UK will be covered by the Privacy Shield.

For the remainder of the EU, Brexit won't directly impact the Privacy Shield. But indirectly, Brexit may give a boost to the Privacy Shield. That's because it's almost certain the Privacy Shield will be subject to legal challenges – and the willingness of the European Court of Justice to further rock the EU boat may be dampened by Brexit. In other words, with the EU still reeling from the impact of Brexit, the EU may be reluctant to cause further turbulence with its primary trading partner, the U.S., by being receptive to challenges to the Privacy Shield framework that took years to hammer out and has finally been put in place. Given the trade disruptions caused by Brexit, further trade disruptions caused by hampering data

flows from the EU to the U.S. is the last thing Europe needs right now.

Michael Whitener is a partner at VLP Law Group. His legal practice focuses on two areas: (1) technology transactions, including software licensing and alliances, cloud computing, web hosting and outsourcing agreements; and (2) corporate compliance, particularly regarding data privacy and anti-corruption laws.