Client Update
Privacy Shield Not Trumped

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Olena V. Ripnick-O'Farrell
ovripnickofarrell@debevoise.com

Andrew Adair
amadair@debevoise.com

WASHINGTON, D.C.
Jeffrey P. Cunard
jpcunard@debevoise.com

LONDON
Jane Shvets
jshvets@debevoise.com

FRANKFURT
Dr. Thomas Schürrle
tschuerrle@debevoise.com

Dr. Friedrich Popp
fpopp@debevoise.com

President Trump's January 25 Executive Order on immigration is attracting a great deal of attention, to say the least. While the order is plainly focused on the Middle East, some commentators have suggested that the order has made collateral damage of Privacy Shield—the protocol for transfers of personal data from the European Union to the United States that came online in August 2016. We respectfully submit that such commentary is off point. Privacy Shield faces challenges but is alive and well.

WHAT IS PRIVACY SHIELD?

Privacy Shield is the mechanism negotiated by US and EU authorities to allow companies to bring personal data of EU origin west across the Atlantic for storage and processing in the US. It aims to solve a basic problem: the EU generally recognizes stronger personal rights to data privacy than the US. Accordingly, the EU generally does not allow transfers of personal data to less protective jurisdictions unless the transfer occurs pursuant to an approved exception or mechanism.

Under Privacy Shield, companies certify that they will follow certain standards for the protection of EU citizens' personal data and will submit to enforcement in both the US and the EU. In exchange, companies are free to move personal data from the EU to the US—a key protection for companies doing business on a global basis. Over 1500 companies have self-certified thus far.

Privacy Shield replaced the now-defunct Safe Harbor, a predecessor data transfer system that was invalidated by the European Court of Justice in 2015 due to concerns about the level of privacy protection in the US. The ECJ stated that US government authorities had "access on a generalized basis" to personal data in the hands of private companies. EU approval of Privacy Shield was based in part on certain commitments by the US government. For example, the Federal Trade

Commission promised to pay particular attention to Privacy Shield enforcement. Congress also passed, and President Obama signed, the Judicial Redress Act of 2015. That statute allowed the US Attorney General to extend the protections of the Privacy Act of 1974 to citizens of certain other countries. Outgoing Attorney General Loretta Lynch, as one of her last acts in office, extended those protections to citizens of EU member countries, effective February 1, 2017.

The Privacy Act creates no broad right to privacy in the US. Rather, as noted in the Justice Department's helpful overview, the Privacy Act merely establishes certain information handling practices for US federal agencies. These include that agencies can only disclose citizens' personal information for certain purposes or with the individual's consent.

DOES THE NEW EXECUTIVE ORDER AFFECT PRIVACY SHIELD?

Commentators concerned about the impact of President Trump's January 25 Executive Order on Privacy Shield have pointed to Section 14 of the Order:

> Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.

On this basis, European privacy advocates—such as Jan Philipp Albrecht, a member of the European Parliament—have claimed that the EU must immediately suspend Privacy Shield and issue sanctions against the US. The US tech and business press have echoed the concerns: "Trump order strips privacy rights from non-U.S. citizens, could nix EU-US data flows," reads a typical headline.

Such commentary notwithstanding, the text of Section 14 actually has no direct effect on the Privacy Shield framework. It should first be noted that the ultimate fate of Privacy Shield strictly speaking rests not with any unilateral action of the White House, but with EU authorities—particularly the ECJ, which will hear a pending legal challenge to Privacy Shield's validity. Moreover, Section 14 does not change US companies' ability to meet their obligations under Privacy Shield, because Section 14's instructions do not apply to these companies. The text of Section 14, and the text of the Privacy Act, is directed to "agencies"—that is, US government entities—and not US companies. Nor does the Executive Order undo Attorney General Lynch's designation of the EU and its member states as covered under the Judicial Redress Act.

In short, the Privacy Shield remains intact. US companies are still free to self-certify under Privacy Shield, and meet the resulting obligations, without worry that this might run afoul of Section 14 of the Executive Order.

Concerns remain. As noted, privacy advocates in the EU have already begun to mount legal challenges to Privacy Shield in the courts there. We have conferred with our friend and former colleague Professor Joel Reidenberg, a leading global privacy scholar and director of the Center for Law and Information Policy at Fordham Law School. Professor Reidenberg says: "Both sides of the Atlantic are heavily invested in the Privacy Shield and the other legal mechanisms to bridge the differences in transborder privacy protections. While this Executive Order does not revoke the Privacy Shield, it does create uncertainty over the new administration's commitment to Privacy Shield. At the same time, the Executive Order is likely to be a factor against the future validity of the Privacy Shield in the upcoming EU court decisions and is likely to push greater scrutiny by EU data protection authorities of data transfers to the United States."

WHAT MIGHT US COMPANIES DO NEXT?

Privacy Shield remains effective. Companies that qualify for it may still wish to consider whether to self-certify. Companies may also wish to consider a belt and suspenders approach—i.e., self-certifying under Privacy Shield, while also adopting one or both of the alternative mechanisms for EU-to-US data transfers. The alternatives are the Binding Corporate Rules and Standard Contractual Clauses; these, like Privacy Shield, formally obligate US-based data recipients to provide EU-style protection for EU personal data. Standard Contractual Clauses, like Privacy Shield, are currently subject to legal challenge in the EU. The benefit of the belt and suspenders approach is that if any one of these mechanisms is ultimately invalidated by the EU courts, a company that has adopted multiple mechanisms could still rely on any that survive these legal challenges.

* * *

We would be pleased to discuss these issues with our clients and friends.