

# PRIVACY AND INFORMATION SECURITY

## BREXIT AND EU DATA PROTECTION: ASSESSING THE IMPACT FOR US ORGANIZATIONS

By: Mary J. Hildebrand, CIPP/US/E

Our 24/7 news cycle has not disappointed over the past few days, with speculation on every imaginable aspect of Brexit. Amid the furor, US companies are wearily asking what it means for the Privacy Shield, the General Data Protection Regulation (GDPR), and other initiatives intended to standardize data protection across the EU. Will doing business in the EU become even more challenging?

Assuming the UK acts on Brexit (which was a nonbinding referendum), the process of negotiating an exit from the EU will take approximately two years. As an initial step, the UK must invoke Article 50 of the Treaty on European Union. Prime Minister David Cameron may leave that task to his successor, who is expected to take office in October 2016. By contrast, fearing a domino effect, EU leaders across the continent are demanding a swift departure. To further complicate matters, Scotland has strongly signaled that it may leave the UK so that the country can remain part of the EU.

### So where does this leave EU data protection in general, and US companies in particular?

**Expect the status quo to continue for the immediate future, as the UK negotiates the precise terms of its withdrawal from the EU. However, current legislative and political efforts to approve the Privacy Shield and implement GDPR in a timely and efficient manner may be disrupted.**

The UK remains a member of the EU until the negotiations for withdrawal

are completed in 2018 or later, depending on exactly when the government chooses to start the process. During the intervening period, the UK will continue to be subject to EU data protection laws just as other member countries are. According to the UK Information Commissioner's Office (ICO), "The Data Protection Act remains the law of the land irrespective of the referendum result." In addition to maintaining current practices, the ICO recommended continued preparation for GDPR implementation. *It appears inevitable, however, that the UK's clout at the negotiating table for the Privacy Shield, and the ability of its data protection authorities to influence rollout of the GDPR, will be substantially diminished.*

There are several current models the UK could follow in creating a post-withdrawal relationship with the remaining 27 members of the EU, or the UK may choose to forge its own path. Norway, Lichtenstein, and Iceland are members of the European Economic Area (EEA). EEA members have certain trading privileges with the EU, but the trade-off is that they are subject to EU laws, including data protection laws. Switzerland is not a member of the EU, and has its own data protection laws; however, it was the first country designated by the European Commission as providing "adequate security" for the personal data of EU citizens. Under either model, the UK would be compelled to comply with all or part of current and future EU data protection laws.

With respect to GDPR, remember that jurisdiction is digital, not based on geography. Any organization that processes the personal data of EU citizens is subject to GDPR irrespective of location or EU membership. UK businesses are no exception, and if they want to conduct business with the remaining countries in the EU, they will have to comply.

There may be a temptation for the UK to enact relatively less-strict data protection/transfer laws in an effort to compete with the EU for global investment, business, and trade. While there's merit in being viewed as "easy to do business with," less regulation may make it difficult to meet the "adequacy" standard established by the European Commission for processing EU personal data. The UK should be wary of any decision that may impair the free flow of data between the UK and the EU.

### Will this complicate GDPR?

Ironically, there will be substantial overlap between the two-year GDPR implementation and the UK's withdrawal negotiations. In other words, the legislation intended to streamline data protection laws across the 28-member EU bloc is losing a key player. The UK will continue to have representatives involved in WP29 and its successor, the European Data Protection Board (EDPB), but the UK's desire and ability to influence the process will be greatly reduced. Brexit should not impact the effective date for GDPR in 2018; however, US companies and others seeking

guidance on many issues associated with GDPR may have to continue waiting as resources are redirected to more exigent issues (such as filling the gap left by the UK's departure).

### What about the Privacy Shield?

For US companies hoping that the Privacy Shield will replace Safe Harbor during 2016, Brexit may translate into further delays. After WP29 heavily criticized the Privacy Shield earlier this year, the EU and the US quietly returned to the negotiating table in an effort to close the gaps. The European Commission promised the Article 31 Committee a final draft of the Privacy Shield for review during the first week in June; as of today, there has been no public announcement that the document is ready for analysis by the committee. The European Commission is not bound by the WP29 Opinion, or the Article 31 Committee opinion when issued. If the European Commission approves the Privacy Shield, commentators expect judicial challenges in the European Court of Justice. ***As the rocky road toward EU approval of the Privacy Shield***

***continues, the UK may pull out entirely and seek to make its own deal with the US.***

### What to expect...

While Brexit is causing political, economic, and financial dislocation in the UK and beyond, EU data protection law remains intact for the moment. During the withdrawal process, the UK will continue as an EU member with all the attendant obligations including compliance with EU laws. Any immediate impact will likely be reflected in the UK's diminished status within the EU, including various committees such as WP29 and the EDPB that will oversee implementation of GDPR, and at the negotiating table with the US regarding the Privacy Shield. The consequence could be further delays and uncertainty for US companies awaiting guidance with respect to GDPR and EU approval of the Privacy Shield. We will keep you updated and continue to provide helpful counsel as the situation continues to evolve.

## contact

**Please contact the attorney named below for more information on this matter.**

**Mary J. Hildebrand, CIPP/US/E**  
973 597 6308  
mhildebrand@lowenstein.com

Follow us on [Twitter](#), [LinkedIn](#), and [Facebook](#).

[www.lowenstein.com](http://www.lowenstein.com)

New York Palo Alto Roseland Washington, DC Utah

© 2016 Lowenstein Sandler LLP.

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation.