Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 34, ISSUE 7 / SEPTEMBER 9, 2016

EXPERT ANALYSIS

Doing Business Abroad? Brexit and Its Implications on Your Data Practices

By Michael Nesheiwat, Esq.
Gottlieb, Rackman & Reisman

The U.K.-EU membership referendum of June 23, popularly termed Brexit, has sent shock waves throughout the world since the final vote was tallied. Political commentators, economists and various pundits have speculated as to the implications of Brexit, particularly in the areas of free trade, migration and regional security. This speculation has caused, among other things, a change in leadership in the U.K. and the largest worldwide stock market drop in history.[1]

Despite the publicity surrounding Brexit, little thought has been given to the effects of this referendum on international data privacy laws. Nonetheless, the implications of Brexit on international data privacy laws — and on companies doing business within the U.K. and the EU — will be significant.

SAFE HARBOR TO PRIVACY SHIELD

The global nature of the internet has resulted in many conflicts of law among jurisdictions, most notably between the United States and European countries. Much of Europe, including the entire EU, places a strong emphasis on protecting their citizens' personal data.

These countries generally require entities operating within their jurisdictions to ensure that citizens know when their personal data is collected, how their information is being used, who their data is being transferred to, and for what purpose it is being transferred.

These countries also allow their citizens to request that the personal information that was collected from them be deleted at their request. This is commonly known as "the right to be forgotten."

While not devoid of data protection laws of its own, the United States generally does not afford safeguards as extensive as those found in European countries.

The EU's privacy laws apply to all "data controllers." A data controller is any entity that processes or stores EU citizens' personal information and has a physical presence in the EU.[2]

The physical presence requirement is broad. For example, it can mean having an office or server located in the EU. In some cases, an entity can reach this threshold simply by leaving cookies, or tracking data, on an EU user's computer when they visit a website.[3] This broad definition means many U.S. companies that do business in the EU, or otherwise interact with EU customers, must comply with EU data privacy laws.

To streamline the process for U.S.-based data controllers to meet these strict EU data privacy requirements, in 2000 the European Commission and the U.S. Department of Commerce instituted U.S.-EU Safe Harbor.

This agreement between the EU and the United States permitted transfers of personal data located in the EU into the United States as long as data controllers self-certified they complied with certain

principles related to the collection and use of the EU user's personal data. These principles involved notice, choice, onward transfer, security, data integrity, access and enforcement.

However, in October 2015 the European Court of Justice invalidated U.S.-EU Safe Harbor on the basis that it did not sufficiently protect the personal information of EU citizens.

In July the European Commission and U.S. Department of Commerce fully implemented the new EU-U.S. Privacy Shield, which allowed for additional safeguards to protect the personal data of EU citizens above and beyond the U.S.-EU Safe Harbor agreement.

Notably, the EU-U.S. Privacy Shield strengthened the principle of "onward transfer" by requiring third parties to whom the data was transferred to maintain Privacy Shield principles as well.

As with the U.S.-EU Safe Harbor, however, EU-U.S. Privacy Shield is applicable only to members of the European Union (as well as Iceland, Lichtenstein and Norway). As such, it will not apply to the U.K. once Brexit happens.

Despite the publicity surrounding Brexit, little thought has been given to the effects of this referendum on international data privacy laws.

This raises the question of what will happen to the personal data of U.K. citizens after Brexit, and how the exit will affect U.S.-based companies doing business in the U.K. and EU.

UK PRIVACY LAWS AFTER BREXIT

While the U.K. is generally more laissez-faire with respect to regulation compared with the countries of mainland Europe, it still takes its data privacy very seriously.

For example, in 1998, prior to the institution of the U.S.-EU Safe Harbor, the U.K. Parliament passed the Data Protection Act of 1998, a law on how to process data of U.K. citizens. The Data Protection Act is considered generally similar to the various individual data protection laws of the other EU member states.

Accordingly, it is unlikely that the U.K. will curb its data protection laws after leaving the European Union. In fact, the U.K.'s Information Commissioner's Office has already said that the current data protection laws in the U.K. will not change after Brexit happens.

The ICO explained that if the U.K. wants to maintain agreeable trade terms with the European Union, the U.K. privacy laws must remain on par with those found in the EU member countries.[4] As such, it is likely that the privacy laws of the U.K. will remain equally stringent post-Brexit.

WHAT WILL REPLACE PRIVACY SHIELD IN THE UK?

As the U.K. will no longer be an EU member, the EU-U.S. Privacy Shield will no longer apply to U.S.-based data controllers doing business within the U.K. To close this gap, the U.K. will have to institute a bilateral agreement akin to EU-U.S. Privacy Shield in order to avoid disrupting any cross-border business relationships with the United States.[5]

The matter of how the U.K. opts to institute such an agreement is still up for debate.

One option for the U.K. is to follow the lead of Iceland, Liechtenstein and Norway and continue to participate and be subject to the EU-U.S. Privacy Shield, as a nonmember of the European Union.

Another possible course of action for the U.K. is to adopt the practice of Switzerland, which has been operating a data privacy agreement with the United States independently from the EU.

In 2009, Switzerland, which is not a member of the EU and thus not bound by the U.S.-EU Safe Harbor, reached a similar agreement with the United States, known as the U.S.-Swiss Safe Harbor. This U.S.-Swiss Safe Harbor agreement includes all of the tenets and safeguards found in the U.S.-EU Safe Harbor, and also includes several provisions that are catered to the specific needs of Switzerland.

For example, while the U.S.-EU Safe Harbor (now Privacy Shield) only affords protections to EU citizens, the U.S.-Swiss Safe Harbor also applies to Swiss corporations and other legal entities.

It is possible the U.K., which has a robust corporate climate that is similar to that of Switzerland, will adopt a similar directive should it choose to reach a separate data privacy agreement with the United States.

Regardless of which course of action the U.K. takes, U.S.-based data controllers will have to ensure they are following U.K. law when dealing with the personal data of U.K. citizens.

DOES MY COMPANY NEED TO WORRY ABOUT PRIVACY SHIELD?

Before a U.S.-based company begins sifting through the complex regulatory framework of international data privacy compliance, they should first determine if they are subject to the EU's data privacy laws as well as those of the U.K., Switzerland and other jurisdictions that contain strict data privacy laws.

Generally, these laws will apply to your company only if it is considered to be a "data controller." As mentioned earlier, this definition is very broad. It can include activities such as having a server in the relevant territory or collecting cookies — data generated by a website and saved by your web browser on your computer — from a user accessing your company's website from one of the relevant countries abroad.

If your company avoids these activities — such as by maintaining servers in the United States and not collecting cookies or other personal data from European users — it likely does not have to worry about complying with these data privacy laws.

Assuming that your company is a data controller, there are also a limited number of options for avoiding the need to certify under the EU-U.S. Privacy Shield (and presumably any potential U.S.-U.K. agreement).

One such option is to ask the EU user to provide affirmative consent to the transfer of his data outside of the EU (for example, through an "I agree" pop-up on the data controller's web page).

This affirmative consent, which presumably would also be available in a potential U.S.-U.K. Safe Harbor type arrangement, must be obtained every single session in which data is collected from a user, and consent can be revoked by the user at any time. Accordingly, this method is practical only for companies that collect data infrequently from EU users and maintain controls to delete this data on command.

AFFECT ON U.S. COMPANIES DOING BUSINESS IN THE EU AND UK

Assuming that your company is considered a data controller in the EU and U.K., and it would not be practical to obtain affirmative consent every time you collect a user's personal data from these territories, then your company must evaluate how the EU-U.S. Privacy Shield, and any potential similar agreement between the United States and the U.K., affects your data collection, transfer and storage procedures.

For example, if the U.K. follows Switzerland's lead and reaches an independent data privacy agreement with the United States, it is possible that the U.K. would no longer be considered part of the European Economic Area with respect to data transfers. If this turns out to be the case, your company may no longer be able to process data of EU citizens within the U.K. without taking additional precautions.

A potential U.S.-U.K. data privacy agreement may also include terms above and beyond those found in the Privacy Shield. For example, it is very possible that the U.K. will mimic Switzerland and push to extend its data privacy laws to protect corporate users as well, forcing your company to account for these entities in your data management plan.

On the other hand, if the U.K. remains a party to the EU-U.S. Privacy Shield, in all likelihood the above scenarios will not play out.

While not devoid of data protection laws of its own, the United States generally does not afford safeguards as extensive as those found in European countries.

CONCLUSION

If your company is doing business in Europe, it is critical to ensure compliance with international data privacy laws. Notwithstanding the uncertainty surrounding Brexit's impact on international data privacy laws, restrictions on data management and transfer across borders are here to stay. That is why it is so important to consult with attorneys with experience in EU data privacy compliance prior to expanding your business into Europe.

NOTES

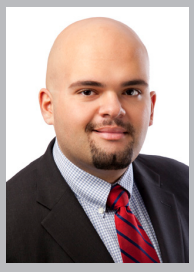
[1] Javier E. David, *Brexit-related losses widen to $3 trillion in relentless 2-day sell-off*, CNBC (June 27, 2016, 6:56 PM), http://cnb.cx/2aRvRhI.

[2] The recently enacted General Data Protection Regulation (Regulation (EU) 2016/679), which will be implemented May 25, 2018, will eliminate this "physical presence" requirement. As such, any entity that processes or stores EU citizens' personal information will be subject to EU privacy laws.

[3] *See* Article 29 – Data Prot. Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (2002), http://bit.ly/2bK0ZSV. *But see* Julia Fioretti, *Facebook wins privacy case against Belgian data protection authority*, Reuters (June 29, 2016, 4:53 PM), http://reut.rs/2cciH3b.

[4] Claire Hopping, *Data protection laws will not change following Brexit vote*, IT Pro (June 27, 2016), http://bit.ly/2b3CQ8n.

[5] It is also likely that the U.K. will have to reach a similar understanding with the EU, although such an agreement would be fraught with much less difficulty, as both parties would generally employ the same safeguards with respect to data privacy.



Michael Nesheiwat is an associate attorney at **Gottlieb, Rackman & Reisman**, an intellectual property boutique law firm in New York. In addition to advising clients on international data privacy law, his practice includes patent prosecution and trademark prosecution as well as copyright, trademark and unfair-competition litigation. He can be reached at mnesheiwat@grr.com.