Brexit's Effect On GDPR, Privacy Shield Limited, But Many Eye Data Transfer Uncertainties

Given the late stages of Privacy Shield negotiations, and the long process of a Brexit, experts see little change to data privacy and transfer laws until Britain leaves.

Ricci Dipshan, Legaltech News

June 28, 2016

Britain voted in favor of leaving the EU at a time when Europe is facing existential threats from an ongoing migrant crisis and the specter of a Grexit, to the geopolitics challenges posed by a newly aggressive Russia. But the Brexit vote also came during a time of transition for the EU's data privacy laws—the recently approved General Data Protection Regulation (GDPR) will modernize data laws across the continent by 2018, while the pending finalization of Privacy Shield will soon herald in a new paradigm for trans-Atlantic data transfers between Europe and the U.S.

But now that Britain may be on its way out, what does this means for such a transition?

Linda Sharp, associate general counsel of ZL Technologies, believes that in the near term, the Brexit vote will not disrupt any data law changes, given that the U.K.'s "exit from the EU is going to take some time to ever materialize."

"From the time that the U.K. actually invokes the Article 50 provisions, there is a term of two years to work through the process. Currently, most estimates place the actual date around 2018. Additionally, all 28 remaining EU member states will have to come to a single agreement with the U.K. regarding its exit," she said. "If we take a lesson from history, I believe that this is going to take longer than the two years anticipated when Article 50 was established."

While the U.K. is planning to soon transition out of the EU, its status as a member is not in doubt. In a joint statement, European Parliament president Martin Schulz, European Council president Donald Tusk and Dutch Prime Minister Mark Rutte said:

"We stand ready to launch negotiations swiftly with the United Kingdom regarding the terms and conditions of its withdrawal from the European Union. Until this process of negotiations is over, the United Kingdom remains a member of the European Union, with all the rights and obligations that derive from this. According to the treaties, which the United Kingdom has ratified, EU law continues to apply to the full to and in the United Kingdom until it is no longer a member."

While it continues on as an EU member for the time being, the UK's influence on shaping the Privacy Shield is limited, given the late stage of the agreement's negotiations. The Wall Street Journal

reported that the U.S. and EU finalized changes to the Privacy Shield on June 24, addressing concerns voiced by the Article 29 Working Party .

The changes will require companies to delete personal data that no longer serves its collection purpose and hold third-party processers to the same standards as the privacy shield certified companies. In a letter, the U.S. government also specifically outlined to EU officials how it would go about its bulk collection of data for security purposes and explained the safeguards it had in place that govern how data is handled. According to European Commission spokesman Christian Wigand, the finalized agreement will likely be adopted by July.

While the Privacy Shield still has to be approved by the Article 31 Committee and adopted by the College of the EU Commission, on which Britain has representatives, these bodies do not need complete consensus to make decisions.

Despite a finalized agreement, however, it is likely that negotiations over Privacy Shield data updates or changes will continue as new issues and challenges arise, and as the GDPR takes effect in 2018. Ryan Costello, operations manager, eTERA Europe, noted that Britain's absence from these negotiations may shift the stance of the EU as a whole to the U.S.'s disadvantage. He said that "without the U.K., the U.S. loses the most enthusiastic security partner and intelligence ally that it has in the Privacy Shield negotiations."

Sharp added that traditionally, "the U.K. has been more surveillance-friendly than the rest of the EU, and their decision for data protection moving forward will probably reflect that."

Britain's Next Data Steps

What data regulations looks like in the U.K. if and when it leaves the EU is anyone's guess. But Deema Freij, global privacy officer at Intralinks, believes that the "U.K. would try to adhere as closely as possible to the GDPR. The rationale being, if there is a full separation in due course, it will be regarded as an 'adequate' country from a data privacy perspective by the European Union and would be able to have transfers of personal data to and from Europe without problems."

Whether this happens or not, Freij notes, depends on whether the U.K. takes "the European Economic Area (EEA) route (like Norway, Lichtenstein and Iceland) which wouldn't be likely to cause much disruption. However, if the U.K. were completely separate from the EEA, data transfers from the U.K. to the EU and vice versa would need to be reviewed by the EU to ensure the U.K. provides 'an adequate level of protection.' Switzerland had to go through this review, for example."

"Realistically, more privacy-aware countries, such as Germany, France and Spain would be likely to put up a fight to challenge the U.K.'s more relaxed approach to data protection legislation. Should the U.K. not be regarded as having 'an adequate level of protection' then, legally, any transfers to the U.K. would have to be via EU model clauses—a very administrative-heavy task," he adds.

Similarly, Costello believes that given the U.K.'s role in and preparation for the GDPR, the country "will be freely adaptable to the regulatory requirements of the GDPR. We've already seen a trend in the U.K. for companies to increase control of their data and improve their governance, risk and compliance capabilities, in large part in anticipation of stricter rules of the GDPR."

But he does not think it will be a straight adoption, given the chance for the U.K. to mold the laws to its own specific needs and culture. "I think we can expect a uniqueness in the U.K.'s own data protection laws, striking, perhaps, a middle-road between the strict requirements of Europe, and the more industry-friendly approach of the U.S.," he said.

Costello added that given the close relationship between the U.S. and U.K. over intelligence and

security matters, "Upon leaving the EU, a separate privacy agreement [with the U.S.] is possible, and would likely not see the roadblocks that the current Privacy Shield arrangement has."

Freij agreed, yet cautioned that, "No one can be sure what the result [of a new agreement] would look like, but it may be more pragmatic than the Privacy Shield."

'Nothing Can Be Ruled Out'

A new trans-Atlantic EU U.S. data transfer agreement, however, is only one of the many uncertainties facing organization on both side of the Atlantic. For multinational organizations that govern data intra-company transfers through binding corporate rules (BCR), for example, the Brexit votes spurs apprehension over whether such mechanisms will still be possible or valid in the years to come.

"The legal community will need to know whether transitional rules will be put in place so the U.K. data protection authority can continue reviewing BCR applications in the interim. Even if these rules were put in place, there are questions over how long this would take," Freij said.

Freij also noted, "With the U.K. data protection authority in the midst of managing these applications for many global conglomerates, any hold-up in the process could prevent these companies from finding an alternate legal means of transferring personally identifiable information intra-group around the world."

"Having voted to leave the EU, any practical guidance around data transfers would be unlikely to arrive immediately, and that it will be some time before global and U.K. companies will know what to do on the issue. During this time, companies will be largely unaware that they might be operating against the law, increasing the risk of technical data breaches," she added.

The Brexit vote also looms large for organizations who established a European headquarters in the U.K. to meet EU data regulations. "Many multinational companies have looked to the U.K. as their place of preference for hosting EU data whether on premise or in a cloud-based environment," said Sharp. "Although in the short term, I don't see much will change; however, as the exit process materializes, this may create a huge wrinkle in the way that we handle EU data in the future.

It will take some time for these issues to be fully ironed out, but one thing is certain—anything is possible. "At the moment, nothing can be ruled out," cautioned Freij.
