Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Brexit To Further Splinter Global Data Protection Rules

By **Allison Grande**

*Law360, New York (June 24, 2016, 10:58 PM ET)* -- The U.K.'s decision to pull out of the European Union is likely to eventually result in the creation of new data protection and transfer agreements that, while similar to the EU's current regime, will contain deviations that could leave companies to grapple with divergent standards and duplicative enforcement, attorneys say.

In a historic decision that sent shock waves across the globe, British citizens voted Thursday to end their 43-year membership in the EU and its predecessors after a late surge in support for the "leave" campaign. Nearly 52 percent of voters came out in favor of the so-called Brexit, while only 48 percent supported staying in the bloc, the U.K.'s Electoral Commission announced Friday morning.

The move will affect a wide range of long-standing policies and relationships, including the rules for how personal data is handled and transferred by companies who do business in the region.

After more than four years of negotiations, the EU last month finalized a new general data protection regulation, or GDPR, that significantly strengthens the bloc's privacy regime and is slated to take effect in May 2018, and U.S. and EU negotiators are in the final stages of hammering out a new deal, dubbed the Privacy Shield, to facilitate trans-Atlantic data flows.

The U.K. electorate's stunning decision Thursday is likely to throw the anticipated application of both of these carefully negotiated deals into disarray, attorneys say.

"I think there will be much uncertainty in the coming days and months about whether the U.K. will follow EU data protection law and implement the GDPR, whether the U.K. will provide an 'adequate level of protection' for EU data, and what data protection framework companies operating in the EU will need to comply with," London-based Hogan Lovells partner Eduardo Ustaran said.

If the U.K. elects to make a clean break from the EU rather than join the European Economic Area — membership in the EEA would require the U.K. to continue to comply with EU privacy regulations — the country will need to come up with its own data protection framework.

While attorneys predict that these rules will skew closely to the GDPR, its independence allows the U.K. to make changes that companies will need to look at when building their already-complex compliance plans.

"This is only going to add to the melting pot of all the different laws and regulations that companies are

going to need to familiarize themselves with," Field Fisher Waterhouse LLP partner Phil Lee said.

However, attorneys were quick to note that the potential upheaval won't be immediate, but instead will emerge over the period of several years.

In order to commence breaking away from the EU, the U.K. must invoke Article 50 of the Treaty of Lisbon. The article provides a two-year period to agree on exit terms, which would include replacement trade agreements with the EU, and any extension would need unanimous agreement from the remaining 27 countries.

Given that it will be at least two years before the U.K. can formally exit — and experts forecast the actual transition period will be much longer, as the clock doesn't begin ticking until the U.K. gives its formal notice, which it is not bound to do at any set time — both the GDPR and Privacy Shield should be in place well before the U.K. breaks away, meaning that the nation at least for a short while will be required to comply with the new arrangements.

"Right now, our message is that this is a case of 'don't panic,'" Cooley LLP partner Sarah Pearce said. "Our advice to companies is that if they're getting ready for the GDPR to take hold, then they should continue to do that, because nothing has changed yet."

When the U.K. does eventually make its exit, a new data protection regime there will likely take hold — but U.K.-based attorneys predict that it won't look all that different than the GDPR.

A big factor in support of the U.K. adhering closely to EU data protection standards is that it is much more difficult for countries that have been found to not have privacy standards "essentially equivalent" to the EU to trade data and do business within the bloc. For example, countries like Canada and Australia who have data protection regimes similar to the EU's have been deemed adequate by the EU, while jurisdictions like the U.S. have not.

"When we become an ex-member of the European Union, then we are no longer part of the club and there will be obligations to ensure an adequate level of protection for data being transferred outside the U.K.," said Dechert LLP special counsel Renzo Marchini, who is based in London. "So if the U.K. becomes a separate country, then in order to continue to carry on doing business with the EU, we're incentivized to keep equivalent laws in place in order to carry out trading."

The general feeling that there won't be any dramatic changes to the U.K.'s data protection regime was backed by the country's privacy regulator, the Information Commissioner's Office, in a statement Friday.

According to the ICO, while an exit from the EU means that the GDPR won't apply directly to the U.K., the country will still need to come up with standards equivalent to the sweeping overhaul in order to continue business with EU member countries.

"With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organizations and to consumers and citizens," the regulator said. "Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will be speaking to government to present our view that reform of the U.K. law remains necessary."

However, while the new law is expected to be similar, few believe that it will be identical to the GDPR.

“Because the U.K.’s Data Protection Act was adopted to be consistent with the current EU Data Protection Directive, EU-type data privacy principles will certainly continue to apply, with perhaps a greater dose of British common sense,” said Alan Charles Raul, who leads Sidley Austin LLP’s privacy, data security and information law practice.

With the U.K. having long had a reputation as being more business-friendly than some other member states, attorneys expect the main departures from EU law will be to relax standards that have been seen as constraining businesses’ ability to freely move data.

“The U.K. is likely going to be tempted to create a law that softens the EU standard in order to attract businesses to the U.K. and make itself a hub for businesses,” Lee said. “But in doing so, it will have to find a way to strike a very fine balance between soft enough to attract U.S. investment and tough enough to meet the EU standard in order to be considered adequate.”

The country is likely to take a similar approach to international data transfers. With popular data transfer mechanisms such as binding corporate rules, model contracts, and the likely Privacy Shield not being applicable to the U.K. once it leaves the EU, the country will need to look to craft deals with its traditional data transfer partners to ensure that long-established data flows aren’t interrupted.

“It’s a big unknown about what such a data transfer deal will look like, but when it’s said that the U.K. might try to soften things to attract EU investment, one of the things that they might try to soften is the data flow regime,” Lee said.

The U.K. could also elect to put in place a deal that essentially mirrors the new Privacy Shield pact — Marchini noted that “there’s nothing preventing other countries from using these documents for their own purposes” — in a move that would echo what Switzerland did in implementing its own safe harbor deal with the U.S. in the wake of the EU’s similar trans-Atlantic agreement.

“In short, the unwinding and rewinding of U.K. data transfers to and from the EU and EEA countries, and to the US, will be pretty confusing for a while before it stabilizes,” Raul said.

The result of the data transfer destabilization would, as Pearce put it, likely “require companies to drill down a bit more and think about data flows not only between the EU and the U.S. but also additional data.”

Attorneys say that, in the shorter term, they’ll be keeping their eye on how the U.K.’s exit from the bloc will impact the approval process for the new Privacy Shield, which is expected to wrap up within the next month or so.

“It will be interesting to see how Brexit will affect the dynamic among the EU and 27 member states in relation to the ongoing U.S.-EU Privacy Shield negotiations,” said Ann LaFrance, partner and co-leader of the data protection and cybersecurity practice at Squire Patton Boggs LLP. “As the U.K. was one of the strongest proponents of compromise, its new ‘exit ramp’ status may lead to a tougher stance on the part of the EU [and] 27 member states in the upcoming vote by [the member states] on the latest version of the Privacy Shield.”

The U.K.’s relationship with the bloc’s other data protection regulators will also be thrown into flux due to Brexit. Under the new data protection regulation, regulators will be encouraged to coordinate with

one another on important cross-border enforcement actions involving alleged violations of regulations and standards such as the GDPR and Privacy Shield.

But while the U.K. regulator on Friday pledged that it would continue to work closely with regulators in other countries, the country's departure from the group means that the ICO may not be privy to as much information from other agencies as it once was — and also increase the chances that the U.K. commissioner may be inclined to take more independent action against multinationals that other member states may already be probing.

"If a company has an incident in the U.K. and in other member countries as well, it can face enforcement across the EU and in the U.K., which makes it incredibly difficult for companies that want to operate in multiple countries," Lee said.

However, while the general consensus is that the surprising Brexit vote is likely to inspire a move away from the more unified regime that the GDPR was intended to usher in, some hold out hope that greater harmonization is still possible.

"Somehow the EU needs to make good on its commitment to promote Europe's own digital economy, and the loss of the U.K. may help focus the mind," Raul said. "Perhaps the silver lining will be a move towards greater international convergence on regulatory policy, and more reasonable harmonization on privacy."

--Editing by Katherine Rautenberg and Brian Baresch.

---