Brexit Won't Shift U.K. Privacy Law in Short-Term

By Marcus Hoy and Bryce Baschuk

Aug. 18 — The European Union and the U.K. will have joint custody of privacy policy for at least the next two years even though the U.K. has voted for separation on the way to a formal divorce, privacy analysts told Bloomberg BNA.

It is unclear whether the U.K. will abide by the EU's new General Data Protection Regulation (GDPR) following Brexit. But the U.K. will be required to align itself with the GDPR before it officially quits the 28-country trading bloc.

Regardless of the exit model chosen, U.K. companies will still have to meet the EU's "adequate level of protection" criteria in order to legally transfer personal data from the EU after Brexit.

Brexitchoices

The U.K. government confirmed July 18 that it won't trigger Article 50 of the Lisbon Treaty, the formal mechanism for leaving the EU, until 2017 at the earliest. Because the exit negotiations are expected to take place over subsequent years, the U.K. will remain an EU member when the GDPR enters into force on May 25, 2018 (21 ECLR 711, 5/11/16). This means that U.K. businesses will be required to take steps to comply with the GDPR before that date.

The U.K. might backpedal and end up back in the EU or go at it alone, Omer Tene, vice president of research and education at the International Association of Privacy Professionals told Bloomberg BNA.

But the U.K. may more likely seek to negotiate to shift its economic relationship with the EU to one of two models that include specific rules aimed at maintaining an adequate level of personal data

protection. The Swiss model of being a member of the European Free Trade Area offers greater independence from EU law. The Norwegian model of being a member of the European Economic Area offers automatic access to the single market.

“If and when Brexit occurs, Norway and Switzerland offer two potential models for the U.K., with important implications for data protection.” Tene said. “If the U.K. opts for the Swiss model, it would have to secure trade deals to gain access to the EU market for each specific business sector. Switzerland's data protection laws closely mirror those of the EU, and indeed, they have been deemed adequate by the European Commission,” he said.

“If and when Brexit occurs, Norway and Switzerland offer two potential models for the U.K., with important implications for data protection.”

It remains to be seen to what extent Switzerland—and the U.K., should it follow suit—will have to keep pace with the GDPR to retain adequacy, he said.

Norway Model May Be Unacceptable

Iceland, Liechtenstein and Norway aren't EU members but are, by treaty, members of the European Economic Area (EEA). EU laws must be separately transposed into the EEA agreement, which allows member nations full access to the single market.

If the U.K. joins the EEA, it would “need to formally implement the GDPR into its regime,” Bathilde Waquet, a data protection lawyer at the London-based Bristows LLP, told Bloomberg BNA.

Should the U.K. join the EEA, it would remain subject to EU data protection regulations, including the GDPR. However, EEA membership also mandates freedom of movement—allowing largely

free-flowing immigration among the EEA members—which likely is politically unacceptable to many of the U.K.'s Brexit supporters. That makes an EEA-based relationship similar to the one enjoyed by Norway unlikely for the U.K.

Kim Ellertsen, legal director at the Norwegian DPA, told Bloomberg BNA that membership theoretically allowed Norway to negotiate on any new EU law that shifts power from Norway to Brussels. In practice, he added, Norway's EEA treaty obligations mean that it follows all EU privacy and data protection laws.

Some of Norway's legislation is stricter than the EU demands, Ellertsen said, though none is less stringent. From a privacy standpoint, there isn't any advantage or disadvantage for data subjects—individuals or corporate entities—to be located in an EEA nation, as opposed to an EU nation, he said.

“All EEA countries have to maintain a close relationship with EU and because of that they tend to harmonize the practice of their own legal system to the EU” Ellertsen said. “There are differences of course, but not because they are EEA countries. You will find the same diversity within the EU itself.”

Philipp Mittelberger, Data Protection Commissioner of the Principality of Liechtenstein, said any differences between EEA and EU law would be minimized further when the GDPR is incorporated into the EEA agreement.

“In practice, there can be differences to EU law in matters concerning data protection,” Mittelberger said. “In my opinion, the Liechtenstein DPA does not have greater nor less independence with regard to its EU colleagues.”

In the EU and the EEA “some DPAs have wider powers than others,” Mittelberger said. “Some have the power to issue sanctions, including

fines. Others do not."

The EU Data Protection Directive (95/46/EC) allowed differences in the privacy laws adopted by countries to transpose it into national law, Mittelberger said. "This will change when the GDPR is incorporated into the EEA agreement," he said.

Swiss Model

Switzerland isn't a member of the EU or the EEA but is a member of the European Free Trade Area. This means that it maintains accesses to the EU single market via a unique bilateral agreement that is regularly updated. The nation's support for migration quotas means that it has been at odds with the EU on this issue.

Although Switzerland's data protection laws are very similar to those of EU countries, it isn't obliged to transpose the Data Protection Directive into national law. Switzerland also won't be obligated to adhere to the GDPR.

If the U.K. follows the Swiss approach, the EU would likely consider it to be a "third country" and would have to verify whether the U.K. offers an "adequate level of protection" of personal data in accordance with the GDPR.

Switzerland has adopted the EU's adequate level of protection concept into a domestic legal framework known as the Federal Act on Data Protection, which seeks to balance Swiss domestic data protection rules and unrestricted trans-border data transfer.

The Swiss law specifically states that no personal data may be transferred abroad if doing so might "seriously jeopardize the personality rights of the data subject." The law also guarantees that the transfer of any personal data to an entity that isn't covered by the European Convention must provide an "appropriate level of

protection."

Waquet said if the U.K. takes a similar route, "it may decide to retain whole or part of its existing Data Protection Act."

In order to receive the adequate level of privacy protection blessing of the EU, "the U.K. is likely to adopt the GDPR wholesale or a similar, possibly more business-friendly, version" she said. The U.K. privacy commissioner has said that in order to maintain trade with the EU, the U.K. would need to amend its privacy law, Waquet said.

Eduardo Ustaran, European head of Privacy and Cyber Security at Hogan Lovells International LLP in London, said that after a formal departure from the EU, the U.K. could theoretically repeal the Data Protection Act to purge it of any EU law. But the U.K. is unlikely to do so because it would want to satisfy the EU privacy adequacy threshold.

Broad Reach

The GDPR asserts a broad geographic reach, Tene said.

The new regulation applies to any organization, anywhere in the world, that targets EU consumers or monitors their behavior. Hence, regardless of the chosen course, many U.K. organizations will have to implement the GDPR to continue doing business in Europe, he said.

If the U.K. opts to go it alone, it may have to negotiate its own version of the EU-U.S. Privacy Shield, Tene said. The Privacy Shield is a replacement for the now defunct U.S.-EU Safe Harbor Program. It allows companies to self-certify with the U.S. Department of Commerce that they will comply with 13 privacy principles.

The Safe Harbor was invalidated by the EU's top court in part because of concerns about U.S. government access to personal data sent to the EU. Tene said that negotiating an EU-Swiss data transfer pact won't be

simple given disclosures about the extent of British intelligence access to EU data.