Brexit May Undercut Privacy Compliance: U.K. Official

By Stephen Gardner

Oct. 20 — Brexit may cause U.K. companies to limit compliance investment for the new European Union privacy regime, U.K. Deputy Information Commissioner Steve Wood told Bloomberg BNA.

Wood told Bloomberg BNA Oct. 20 that uncertainty isn't "good because it can delay investment in compliance systems." The U.K. data protection agency, the Information Commissioner's Office (ICO), had been "relaying to government" that companies "want certainty and clarity" over data protection in the context of the U.K.'s exit from the EU, Wood said.

The U.K. voted to leave the EU in June. The U.K. government has said it will trigger in early 2017 a two-year negotiation with the remaining 27 EU countries on the terms of the U.K.'s departure.

Consequently, the U.K. is likely to leave the EU in 2019, after the EU General Data Protection Regulation (GDPR) comes into effect in May 2018. The U.K. must implement the GDPR while it remains an EU country.

The ICO was working "steadily towards" GDPR implementation ahead of the May 2018 deadline and is "working with European colleagues in the Article 29 Working Party" on GDPR guidance, Woods said.

Divergent Regimes?

After the U.K. leaves officially the EU, its data protection regime might start to diverge from the GDPR.

The U.K. government has previously said that it will attempt to harmonize it's data protection laws with EU laws before the nation leaves the bloc.

Wood said that post-Brexit "obviously it's a decision for the government to make, and parliament as well, in terms of what legislation we should have in the U.K. for data protection."

However, "the challenges which were there before the referendum are still there now: the challenges of the digital economy, digital public services, challenges of better transparency online so citizens have more control, challenges of children's personal data online," Wood said.

"Those difficult issues won't go away so we still need a strong, progressive data

protection law. We'll always make the case for strong enforcement powers and an independent agency enforcing the data protection laws in the U.K," he said.

The ICO would continue to stress that strong data protection is needed because it's a fundamental right and "good for the digital economy because the more trust you have in a digital economy, the more it is likely people will be able to share high quality personal data that can drive new businesses," Wood said.

Post-Brexit Jurisprudence

After the U.K. formally leaves the EU, it will no longer be able to rely on the European Court of Justice (ECJ) for data privacy case law.

is unclear if binding decisions, such as decisions of the European Data Protection Board (EDPB) that will be set up under the GDPR, will apply in the U.K. post-Brexit.

However, even if post-Brexit EU rulings and decisions don't apply in the U.K., the nation and the EU may remain close in terms of privacy regimes, Wood said.

"If the position is we're outside the EU and we become a third country in the concept of European law, then we wouldn't be subject to binding decisions," he said. But, "U.K. companies selling into the EU, or with other establishments in the EU, would still be affected by the case law" from the ECJ, he said.

He added that "it's possible that the case law will still be influential at a slightly removed point." The EU Court of Justice's Google Spain judgment about the right to be forgotten "had an effect outside the EU anyway, with other jurisdictions looking and thinking about the direction of case law, so data protection case law and developments in the EU will still be important in the UK, but there will be a redefined relationship."

"The future strategy for the ICO will be how we have to interact with that," Wood said. The U.K. Information Commissioner, Elizabeth Denham, "will start to develop over time what the ICO's relationship with the EDPB might need to be after we leave," but "we can't really say at this stage how that will work."

Adequate to Receive Data?

As part of the post-Brexit fallout, the U.K. may have to apply for its data protection regime to be found adequate by the European Commission, the EU's executive arm.

A decision to apply for adequacy "is ultimately a political one for the government to make," Woods said.

To trade with the EU "adequacy is normally seen as a key component, as evidenced by

the work done by the U.S. to get the Privacy Shield in place," Wood said. The EU-U.S. Privacy Shield is the data transfer framework that replaced the canceled U.S.-EU Safe Harbor arrangement.

For the ICO, "the heart of our considerations are not the trade issues, which are connected with adequacy, but the protection of personal data of U.K. citizens that is transferred out to different countries under any new law we have in place after we exit," Wood said.

This would likely necessitate a U.K.-U.S. deal on data transfers. For this, the "Privacy Shield is one model that could still be considered, given the effort and time that has gone into making it work and the input we gave as the ICO," Wood said.

"I suspect companies will want regulatory certainty and to be able to continue to use a model like that," Wood said.

By Stephen Gardner

To contact the reporter on this story: Stephen Gardner in Marrakesh, Morocco at correspondents@bna.com

To contact the editor responsible for this story: Donald G. Aplin at daplin@bna.com