Global Perspectives

Brexit

The referendum backing the withdrawal of the U.K. from the EU has caused much speculation about how such a move may affect international data transfers, but the author writes that for most organizations, the prudent course is to continue with preparations for the new EU data protection regulation ''as if Brexit had never happened.''

Brexit's Impact on International Data Transfers

BY ROHAN MASSEY

On June 23, 2016 the people of the U.K., by a slim margin of 52 percent to 48 percent, voted to leave the European Union, a move better known as ''Brexit'' (15 PVLR 1316, 6/27/16). This somewhat surprising result has created turmoil in the financial markets, resignations from the government and the opposition party, and great uncertainty as we look for the answer to the question ''what happens now''?

The U.K.'s exit from the EU will not be immediate; we need to give notice to leave formally, commencing the Article 50 exit process. Even initiating this process seems some time off and, once notice is served, there is a minimum two year period under Article 50 before a Member State can leave the EU. For this reason, any final exit by the U.K. is unlikely to occur before late 2018 or early 2019.

So in a year that has seen the U.S.-EU Safe Harbor Framework invalidated by the Court of Justice of the European Union (CJEU); the new EU General Data Protection Regulation (GDPR) adopted and scheduled to take direct effect from May 25, 2018; the draft EU-U.S. Privacy Shield published and criticised by the Article 29 Working Party, the European Parliament and the European Data Protection Supervisor; and the U.K. actually voting to leave the EU, where does this leave the U.K. with regard to international data flows, going forward?

Rohan Massey is a partner at Ropes & Gray LLP in London and leads the firm's privacy and data security practice in Europe.

For Now—Keep Calm and Carry On

The U.K. Information Commissioner's Office (ICO) made clear in its press release of June 24, 2016, that the Data Protection Act 1998 (DPA) remains the law of the land and all processing of personal data must be undertaken in accordance with the DPA. An updated statement on July 1, 2016 confirmed that reform of U.K. data protection law remains necessary (although the precise form this reform will take is, as yet, unclear).

The U.K. Information Commissioner's Office made clear that the Data Protection Act 1998 remains the law of the land and all processing of personal data must be undertaken in accordance with the DPA.

The DPA allows for personal data to be transferred freely to the European Economic Area (EEA) member states and those countries covered by European Commission findings of adequacy. The DPA also provides that consent, model clauses, binding corporate rules (BCRs) and self-assessed adequacy may be used to legitimise international transfers of personal data to countries outside the EEA, which are not covered by an adequacy decision. In addition to this, although the Safe Harbor framework is no longer a valid means for legitimising data transfers to the U.S., as recently as February 2016, the ICO's position remains that it ''. . . will not be seeking to expedite complaints about Safe Harbor

while the process to finalise its replacement remains ongoing and businesses await the outcome.''

What Are the Future Options?

Any decision on the future of data protection law in the U.K. will be influenced by the agreements that the U.K. reaches with the EU once it leaves. Possible options are set out below.

1. Implement the GDPR (or an Equivalent)

Following exit from the EU, as it has already agreed the text of the GDPR as a member state of the EU, the U.K. may decide to implement the GDPR and repeal the DPA, by way of national legislation. This option should assist in the facilitation of trade links with the EU going forward and remove at least one barrier. If the U.K. remains outside the EEA, but implements the GDPR (or something very similar) then it is likely that a finding of adequacy by the European Commission would follow.

Were the U.K. to retain the Data Protection Act instead of the equivalent to the General Data Protection Regulation, it's possible that no finding of adequacy would be made on the grounds that the GDPR is more robust than the Directive.

---

2. The Norwegian Model

If the U.K.'s relationship with the EU was agreed along the same lines as Norway's current membership of the EEA, then the U.K. would need to adhere to the GDPR and take steps to implement it with effect from the end of the Article 50 process. Under this option, data transfers from the U.K. across the EEA would be permitted freely and the U.K. would also benefit from the European Commission's findings of adequacy in respect of international jurisdictions that are deemed to provide an adequate level of protection for personal data. The U.K., together with all other EEA Member States, would also be able to avail itself of the protections offered by the proposed EU-U.S. Privacy Shield, once adopted, regarding personal data transfers to the U.S.

3. The Adequacy Route

If the U.K. were to leave the EU and not become a member of the EEA, it would be treated as a third country by the EU for the purposes of international personal data transfers. As noted above, if the U.K. chose to implement a new regime based on the GDPR principles it is highly likely that the Commission would find the protection afforded to personal data by the U.K. to be adequate and add the U.K. to its ''white-list,'' as it has done for countries including Argentina, Israel and Switzerland under Data Protection Directive (95/46/EU).

However, were the U.K. to retain the DPA and not implement an equivalent to the GDPR, then it is possible that no finding of adequacy would be made on the grounds that the GDPR is more robust in its protection and requirements than the Directive (and therefore the DPA). Furthermore, some may view the U.K.'s historical interpretation, implementation and pragmatic approach in respect of the Directive as offering a lower standard of protection than that which will be required under the GDPR. In this scenario, all personal data transfers to the U.K. from the EEA would need to be legitimised by model clauses, BCRs, consent or any of the other safeguards or derogations available under the GDPR, with the U.K. controller or processor being the data importer in each case. This may require many organisations to review commercial contracts and data sharing arrangements that are currently in place to ensure ongoing compliance.

4. An EU-U.K. Privacy Shield?

If the U.K. decided to remain outside the EEA and not implement the GDPR, intending to rely on the DPA going forward, as noted above any such regime is unlikely to be sufficient for a Commission adequacy finding under the GDPR. In addition, the Investigatory Powers Bill (IPB), which is currently before the U.K. Parliament, may make a finding of adequacy even less likely. This is because, as currently proposed, the IPB would allow bulk personal datasets to be collected for purposes of national security without regard to data protection compliance

In the absence of an adequacy finding by the Commission, one possibility would be to implement a ''Privacy Shield'' type arrangement between the U.K. and the EU similar to the proposed EU-U.S. Privacy Shield. However, the proposed terms of the IPB may mean that the U.K. will find itself in a similar position to the one that the U.S. is in at present. There would need to be careful negotiations as to the form of arrangement allowing for international data flows to the U.K..

5. A Dual System?

There is a final option in which the DPA remains in force and is applied to all international data flows from the U.K. outside the EEA when a controller is established in the U.K., where the processing of personal data takes place exclusively in the U.K. and the processing is limited to U.K. citizens. For all other international transfers the GDPR would apply. Among other things, this could allow the U.K. to assist small businesses. Although there may be some merit in this proposal, the complexity of administration makes this a very impractical solution.

So there we have it, a number of options, but no clear leader as yet. As the clock ticks ever closer to May 2018, a decision and clarity on these points would be welcome sooner rather than later. For most organisations, the prudent course of action based on the information available would be to continue with preparations for GDPR as if Brexit had never happened.

  PVLR ISSN 1538-3423