Milbank

24 JUNE, 2016

CONTACT

Joel Harrison
Partner
+44-20-7615-3051
jharrison@milbank.com

Data Privacy Group Client Alert: The UK Votes for Brexit – Data Protection Implications

The outcome of yesterday's referendum raises a number of important data protection issues for UK organisations, as well as for organisations in other EU member states that share data with them. Many of these issues focus on whether and how the forthcoming EU General Data Protection Regulation (GDPR), which is set to apply from May 2018, will apply to UK companies, and whether EU companies will still be able to transfer personal data to affiliates, suppliers and partners in the UK.

It's currently too early to say exactly what the UK's post-Brexit relationship with the EU will look like, and how and when this will change the data protection landscape in the UK. For now, here are some of the key points based on what we know on the morning after the referendum:

1. DATA PROTECTION LAW HASN'T CHANGED OVERNIGHT.

The referendum itself has no legal effect, so the UK remains a member of the EU for the time being. This means that companies in other EU member states can continue to transfer personal data to the UK, and vice versa. There's no need to halt or restructure any data processing activities or any data transfers to or from the UK right away.

So, when will the UK actually cease to be a member of the EU? The EU Treaties set out a formal process for a member state to withdraw from the EU: once the member state has indicated its intention to leave, it will negotiate an agreement with the EU setting out the terms of its withdrawal. The member state then ceases to be a member once the withdrawal agreement becomes effective or, if that hasn't happened by two years after the start of the process, after the end of the two-year period. (This period can be extended, but only with the unanimous agreement of the European Council.) It currently isn't clear whether the UK will invoke the formal withdrawal process or use the Brexit vote as a means to enter into a wholesale renegotiation of the UK's relationship with the EU, but the Prime Minister has previously made clear that he expected the formal withdrawal process to be followed if the UK voted to leave the EU.

2. THE UK WILL PROBABLY BE A 'SAFE' DESTINATION FOR PERSONAL DATA…EVENTUALLY.

EU data protection law prohibits the transfer of personal data to countries outside the European Economic Area (EEA) unless certain conditions are met. Many transfers outside the EEA currently make use of mechanisms to implement adequate safeguards, such as model contracts or, less commonly, binding corporate rules (BCRs). However, these mechanisms are unlikely to be acceptable for the UK, particularly in the long term, given the level of trade between the UK and the EU (not to mention the sheer number of existing data flows). Some other arrangement is likely.

There are three main possibilities:

- *EEA model:* The UK might seek to remain a member of the EEA despite no longer being a member of the EU, which would allow personal data to be transferred between EU member states and the UK. (The other non-EU members of the EEA are Norway, Iceland and Liechtenstein.) In this case, companies in the UK would still be subject to EU data protection law (including, eventually, the new requirements of GDPR).

- *Adequacy finding:* The UK could alternatively apply for the European Commission to recognise the UK's data protection regime as providing an adequate level of protection for personal data. Again, this would allow personal data to be transferred between EU member states and the UK.

  Whilst the UK has already implemented the current Data Protection Directive and has ratified other international instruments on data protection (such as the Council of Europe Convention), an adequacy finding is not guaranteed. There have been persistent concerns over the UK's implementation of the Directive, while the Snowden revelations have placed the activities of the UK's intelligence agencies under unprecedented scrutiny; the Investigatory Powers Bill has done little to help the UK's position in this respect.

  The judgment of the CJEU in the *Schrems* case that invalidated the Safe Harbor also made clear that, in order for the UK's data protection regime to be treated as adequate, it would have to provide a level of protection for personal data that is 'essentially equivalent' to that of the EU. In the long term this would be assessed against the new requirements of GDPR, meaning that if the UK wanted to be treated as an adequate third country, it would have to adopt many of the provisions of GDPR into its national laws.

- *Privacy Shield-style arrangement:* The third possibility is that the UK could press for a bespoke arrangement with the EU along similar lines to the Privacy Shield currently being negotiated with the US. This seems very unlikely. The

aftermath of the *Schrems* judgment and the continuing difficulties in negotiating the Privacy Shield have left the European Commission with very little enthusiasm for using this as a model for arrangements with other countries.

3. HAVE A BACK-UP PLAN FOR CRITICAL DATA TRANSFERS.

Whilst it seems highly likely that the UK will, through one approach or another, be treated as a 'safe' country for data transfers, the process may not be straightforward and it may take some time before the new arrangements are put in place. This means that there may be an interim period, following the UK leaving the EU, in which personal data cannot be transferred from the EU to the UK without additional mechanisms such as model contracts or BCRs. The aftermath of the *Schrems* judgment has shown that a number of the EU data protection authorities are willing to take action against EU companies that continue to transfer data to third countries without an adequate legal basis.

In light of this uncertainty, we would advise organisations to start to identify at least their most critical data transfers from the EU to the UK (whether organisations are transferring or receiving the data, or both). Whilst it will, on any view, be some time before mechanisms such as model contracts need to be put in place, recent experience from the demise of the Safe Harbor demonstrates just how time-consuming the identification of these transfers can be.

4. THINK BEFORE YOU PUT YOUR GDPR COMPLIANCE PROJECTS ON HOLD.

A number of organisations have already started their projects to assess the impact of GDPR on their businesses and determine the changes that they will need to make. Whilst May 2018 may seem a long way off, most organisations have a great deal to do in order to be compliant with GDPR's new requirements.

We would advise organisations to think very carefully before discontinuing these projects in light of the Brexit vote. This is for two reasons in particular:

- For the reasons given above, the UK is likely to want its data protection regime to be recognised as adequate by the European Commission. The UK will have to adopt many of the provisions of GDPR in order for this to happen.
- Even if the UK doesn't implement GDPR, many UK companies will still have to comply with it. This is because GDPR applies to non-EU companies if they process personal data in relation to offering goods or services to individuals in the EU or monitor the behaviour of individuals in the EU. A great many UK companies will fall into one or both of these categories.

5. EU-WIDE GROUPS WILL NEED TO RE-ASSESS THEIR GDPR ARRANGEMENTS

One outcome that is highly likely, absent a special deal between the EU and the UK, is that the ICO will not be able to act as lead supervisory authority for a data controller or processor that is established both in the UK and in one or more EU member states.

One of the most talked-about provisions in the European Commission's original proposal for GDPR was the 'one-stop shop', under which a data controller or processor established in multiple EU member states would need to deal only with the data protection authority for the state in which it had its main establishment. (This contrasts with the scheme under the current Directive, in which a data controller established in multiple EU member states has to deal with the data protection authority in each of them.) Whilst the one-stop shop has been significantly watered down since the Commission's proposal, the final version of GDPR does provide that a controller or processor will have to deal only with the authority for its main establishment in many cases.

Under GDPR, the main establishment of a controller or processor has to be in the EU, meaning that, once the UK has left the EU, an establishment in the UK cannot be its 'main establishment' for these purposes. Accordingly, businesses with EU-wide operations that were planning to adopt the UK as their lead establishments (particularly in light of the ICO's reputation as one of the more 'business-friendly' authorities) will most likely need to re-assess those plans in light of the Brexit vote.

DATA PRIVACY GROUP

Please feel free to discuss any aspects of this Client Alert with your regular Milbank contacts.

If you would like copies of our other Client Alerts, please visit our website at www.milbank.com and choose “Client Alerts” under “News.”

LONDON
10 Gresham Street, London EC2V 7JD England

Joel Harrison	jharrison@milbank.com	+44-20-7615-3051