BREXIT: DATA PROTECTION

Date: 18 July 2016

Brexit/EU Data Protection, Privacy, and Security Alert

By: Arthur Artinian, Philip J. Morgan, Andrew R. Danson, Daniel L. Clyne, Andrew W. Gilchrist

This Brexit Bite assesses the post-Brexit landscape with respect to the UK's data protection laws. It is important to remember that the UK remains a member of the European Union until the terms of its withdrawal have been finalised and, until the UK government invokes Article 50 of the Treaty on European Union, the likely two-year countdown towards Brexit will not start.

Therefore, there will be no immediate impact on UK data protection law. However, it is important that companies already begin to consider what the legal framework may look like in the post-Brexit world. This article first gives an outline of the UK's current data protection regime, and then considers what that regime may look like once the UK has fully withdrawn from the European Union.

THE UK'S CURRENT DATA PROTECTION REGIME

- The UK's Data Protection Act 1998 (the "**Act**") implements the EU Data Protection Directive (95/46/EC) (the "**Directive**") and sets out the rules by which entities can process and transfer personal data. As a result of the Directive, European Member States have fairly harmonised rules (and can be said to provide a minimum standard of protection) in relation to the processing of personal data, which aides the cross-border transfer of personal data across the European Union.
- Further harmonisation of Europe's data protection and cyber-security standards is on the way in the next few years, which may or may not be implemented prior to Brexit. As well as the new "General Data Protection Regulation" (the **"GDPR"**) which is due to come into force in May 2018 (further details below) there will be two new European Directives on cyber-security and trade secrets, which will help encourage minimum standards in relation to cyber-security practices.
- The current Directive recognises that (in the view of the EU institutions at least) data protection standards outside Europe may fail to adequately protect the rights of individuals with regard to the processing of their personal data. Article 25 of the Directive only allows a data controller to transfer personal data to a recipient based in a third country - a country outside the European Economic Area (the **"EEA"**) - if the recipient can and will provide an "adequate" level of protection to the personal data.
- If the European Commission considers a third country's data protection regime to be adequate, it may issue an "adequacy decision", as it has done in relation to several countries, including Argentina, Canada, New Zealand and Switzerland. Personal data can be transferred to a recipient in these countries on the same terms as if the recipient was located in the EEA. Where a third country is not subject to an adequacy decision, the data controller must ensure that, once transferred, the data will be subject to an adequate level of protection. To that end, the European Commission has authorised certain standard

form contractual clauses to be used where transferring data outside the EEA. Use of the standard clauses is not mandatory but in practice their use can be the easiest way to ensure compliance with the Directive.

THE GDPR

- The GDPR will replace the Directive and will come into force in May 2018. It will have direct effect in all EU Member States, and, among other changes, will introduce more onerous rules on how personal data must be handled and protected, and higher penalties in relation to non-compliance. Importantly, the GDPR will not just apply to businesses established within the European Union but will also apply to all companies offering goods or services (even free of charge) to individuals located within the European Union.

POSITION AFTER BREXIT?

- Once the UK has withdrawn from the European Union, the Act will remain in force, so , whilst the GDPR may cease to have direct effect, the laws on processing personal data in the UK will not immediately be different from those in force today. However, the UK will (in theory, at least) have more flexibility to lower the current level of protection that the Act affords personal data, and will also have to consider its future relationship with the EU with respect to data transfers. Whilst the eventual position will mainly be driven by the nature of the UK's relationship with the EU post-Brexit, the following represent some of the possible outcomes:

1. **The UK obtains an adequacy decision from the European Commission.** As the UK's data protection laws currently implement the Directive there should not be many technical difficulties in obtaining an adequacy decision, which would result in transfers of personal data between the UK and the EU continuing as before Brexit. However, the speed at which the European Commission grants the decision would depend on political will. It is also important to note that, although the GDPR would not directly apply to the UK in its position outside the EU, the UK might well need to update its data protection laws in 2018 to comply with the GDPR in order to obtain and/or sustain any adequacy decision granted in its favour.
2. **The UK joins the EEA.** As a member of the EEA, the position is unlikely to change as the Directive applies to the non-EU EEA countries in the same way as it applies to the EU Member States. Furthermore, the GDPR, when it comes into force, will apply to the EEA states if it is incorporated into the EEA Agreement.
3. **The UK reduces personal data restrictions.** The UK may choose to reduce the burden on those dealing with personal data in the UK by reducing restrictions on processing personal data in the UK and sending personal data overseas (particularly outside of the EEA). While this might be beneficial in some respects, this might also restrict UK companies' ability to receive personal data originating from Europe (for example, because the UK will be less likely to obtain an adequacy decision from the European Commission). Without an adequacy decision, if a company in the EU wants to transfer data to a business in the UK, it may require the UK business to sign up to EU model contract clauses. It is worth noting that countries outside the EU (for example, Australia) have also been tightening up their data protection regimes, including placing similar restrictions on exporting personal data to countries offering “inadequate” protection.

4. **The UK agrees a "UK Privacy Shield" with the EU** (similar to that being negotiated currently between the EU and the US). UK companies could voluntarily agree to provide enhanced data protection in return for being able to receive personal data from companies in the EU. As with the other options, the enhanced standard would, at least from May 2018, be measured in comparison with the GDPR. This option could work in tandem with option 3, combining reduced mandatory restrictions with a voluntary enhanced protection for those seeking to receive personal data from the EU. However, as can be seen from the current negotiations of the US Privacy Shield, such a scheme might be complex and difficult to approve in practice.

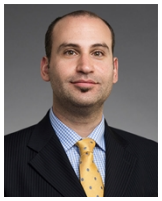
A REGULATORY-LITE FUTURE IS HIGHLY UNLIKELY

- Other countries, for example, Canada, New Zealand, Japan and Australia, have implemented very similar data protection laws to the EU, in order to facilitate cross-border exchanges of data including (in certain cases) restricting the export of personal data to countries offering "inadequate" protection. Once the UK's withdrawal from the EU has been completed, it may be unlikely that there will be any incentive to cut Brussel's "red tape" in relation to data protection if the effect would be to create barriers to global trade which may rely on the free movement of personal data between the UK and European Member States.
- Furthermore, as noted above, the GDPR will have extraterritorial effect outside of the European Union and will impact all businesses selling into Europe or monitoring the behaviour of European citizens. In practice, these businesses will need to comply with the higher standards dictated under the GDPR when doing business with Europe, even in the unlikely scenario that UK standards are lowered or relaxed.
- Consequently, as we have seen in relation to many other regulatory issues, the effect of Brexit will likely mean that many UK businesses are still subject to EU rules, but without being able to influence those rules from the inside.

WHAT CAN COMPANIES DO IN THE MEANTIME?

- Review any incoming transfers of personal data from Europe into the UK so you can understand the potential impact to your business following Brexit, and what further compliance steps might need to be taken to minimise any business interruption.

KEY CONTACTS



ARTHUR ARTINIAN
PARTNER

LONDON
+44.20.7360.8207
ARTHUR.ARTINIAN@KLGATES.COM

PHILIP J. MORGAN
PARTNER

LONDON
+44.20.7360.8123
PHILIP.MORGAN@KLGATES.COM

