GT GreenbergTraurig Maher

Cybersecurity, Privacy and Crisis Management/Global - Europe Practice | Alert

July 2016

Brexit: Impact on Data Privacy and Cybersecurity

This note addresses the potential impact of Brexit on data privacy and cybersecurity legislation in the UK. It is one of a series of GTM Alerts designed to assist businesses in identifying the legal issues to consider and address in response to the UK's referendum vote of 23 June 2016 to withdraw from the European Union.

Timing of Brexit

The UK has not left the EU. It will remain a member of the EU, and EU law will continue to apply in its territory, for some time.

Before exiting, the UK needs to go through the exit procedure set out in Article 50 of the Treaty on European Union, starting with notification to the European Council of its decision to leave the EU. The new UK Prime Minister, Theresa May, appointed on 13 July 2016, has clearly stated that while "Brexit means Brexit," there should be no rush to serve the Article 50 notification. She and David Davis, the Secretary of State for the new government department in charge of managing Brexit, have supported the view that notification should not take place before the end of the year. While the situation remains fluid – with the EU institutions and the remaining 27 EU Member States increasing pressure for formal negotiations to commence swiftly – notification may be delayed for some time to allow consideration of the UK's preferred exit terms and model for its future relationship with the EU. When the notification is made, it will trigger a two-year, extendible period of negotiation with the EU on the UK's terms of exit only. To read more about the timeline for the Brexit, please see our previous *GTM Alert*, "Brexit: The Timeline."

At this time, it is not clear if negotiation of new arrangements with the EU will be conducted in parallel, or at a later stage. It is clear, however, that the UK intends to start negotiating trade terms with non-EU countries as soon as possible.

Potential Impact on Data Privacy Legislation

Given the importance and sensitive nature of personal data in an increasingly online world, it is not surprising that data privacy is one of the more harmonised areas of EU law. As a result, the UK's current data privacy laws are derived from EU law.

However, contrary to many other areas of law affected by Brexit that rely on directly applicable EU legislation or secondary legislation passed under the European Communities Act 1972, the main piece of UK data privacy legislation is a stand-alone Act of Parliament: the Data Protection Act 1998. As a result, withdrawal of the UK from the EU will not have any immediate impact on the legislative landscape.

In the longer term, the shape and content of UK data privacy law are still likely to reflect the rules and standards that apply across the remaining 27 EU Member States, including those set down by the EU General Data Protection Regulation (**GDPR**), which is scheduled to come into force in May 2018. This is because of the importance to UK businesses (especially in the digital sector) of being able to share data freely between establishments based in the EU and the UK.

There are two approaches that the UK could adopt to ensure this:

- The "Norwegian model," under which the UK would re-join the European Free Trade Association (**EFTA**). The UK could then decide to become part of the European Economic Area (the **EEA**), which comprises the EU Member States and the EFTA Member States (except Switzerland, which is a member of EFTA only). As a result, the UK would remain a member of the EU's Single Market via the EEA, preserving the status quo on data flows between the UK and the other EEA Member States. To do so, the UK would have to implement data privacy laws that are harmonised with EU law (in other words, the GDPR).

- The "Swiss model," under which the UK would seek confirmation from the European Commission that its data privacy laws are "adequate" to protect personal data. If the UK were to obtain adequacy status, it would join the EU's "white list" of adequate countries such as Argentina, Canada, and Switzerland. The EU treats data flows from EEA-based establishments to adequate countries and to EEA Member States in the same way. Data flows from the UK to EEA Member States would be subject to UK law but the UK would presumably wish to permit such transfers, in particular given that this model would require the UK to implement legislation that provides similar protections and obligations to the GDPR.

There is a third option, under which the UK would decide to "go it alone" and develop its own data protection legislation without regard to EU law. It is less likely that the UK will take this option, but not inconceivable. In the past, the UK has consistently applied a more liberal approach to EU data protection law than the other EU Member States. If the UK does take this option, then EU law is likely to treat it as a "non-adequate" country for data protection purposes. In that event, UK businesses would have to implement somewhat cumbersome mechanisms such as Binding Corporate Rules or EU-approved Model Clauses, or an equivalent of the EU-U.S. Privacy Shield, to permit the lawful transfer of data from the sites and servers of their customers or affiliated entities located in the EEA to those servers of the UK business that are located in the UK. Data flows in the opposite direction would need to comply with UK data protection legislation.

Regardless of Brexit's eventual impact, multi-national businesses that process the personal data of EU citizens or supply goods and services to the EU from the UK will still have to comply with the GDPR. If the UK moves away from harmonising its data privacy law with the GDPR, the compliance challenge for such businesses is likely to increase, as they will be operating under two regulatory regimes instead of one. For its part, the UK Information Commissioner's Office has recommended that UK businesses continue to plan to implement the GDPR.

Potential Impact on Cybersecurity Legislation

In the area of cybersecurity, the EU has adopted the EU Network and Cybersecurity Directive (the **NIS Directive**), which is likely to enter into effect in May 2018. The goal of the NIS Directive is to implement a harmonised EU-wide regime for co-

operation and capability in dealing with the rise of cyber threats. The NIS Directive will apply to companies in certain "critical sectors" and digital service providers. To read more about the NIS Directive, please see our previous *GT Alert*, "EU Network and Information Security Directive Expected to Enter into Force August 2016: Will Your EU Operations be Affected?"

At present, it appears likely but not certain that the UK will implement the NIS Directive (or something similar to it), notwithstanding its exit from the EU. This is due to the advantages of having a common approach with the EU to the cross-border challenges that cybersecurity threats pose.

Conclusion

The full implications of the UK's withdrawal from the EU are still being worked through and they will to a great extent depend on the model chosen by the UK for its future relationship with the EU and the EU exit arrangements. Those choices will be heavily influenced by the new UK Prime Minister, but also heavily negotiated by the EU. Until there is greater clarity and certainty, businesses should continue to monitor developments, identify those areas where their businesses are likely to be affected by new or amended legislation and regulation – and, importantly, those areas that are unlikely to be affected – and determine how to mitigate risks in affected areas.

Further information on issues related to Brexit can be found here.

This *GTM Alert* was prepared by **Luke Dixon** and **Simon Harms** in Greenberg Traurig Maher's London office. Questions about this information can be directed to:

- Luke Dixon |+44 (0) 203 349 8756 | dixonl@gtmlaw.com
- Simon Harms | +44 (0) 203 349 8767 | harmss@gtmlaw.com
- The GTM Brexit team:
  - Gillian Sproul | +44 (0) 203 349 8861 | sproulg@gtmlaw.com
  - Lisa Navarro | +44 (0) 203 349 8757 | navarrol@gtmlaw.com
- Or your Greenberg Traurig Maher attorney

For more information:
Greenberg Traurig Maher LLP
The Shard, Level 8
32 London Bridge Street
London SE1 9SG

T +44 (0) 203 349 8700
F +44 (0) 207 900 3632
www.gtmlaw.com

Albany
+1 518.689.1400

Amsterdam
+ 31 20 301 7300

Atlanta
+1 678.553.2100

Austin
+1 512.320.7200

Berlin¬
+49 (0) 30 700 171 100

Berlin-GT Restructuring¯
+49 (0) 30 700 171 100

Boca Raton
+1 561.955.7600

Boston
+1 617.310.6000

Chicago
+1 312.456.8400

Dallas
+1 214.665.3600

Delaware
+1 302.661.7000

Denver
+1 303.572.6500

Fort Lauderdale
+1 954.765.0500

Houston
+1 713.374.3500

Las Vegas
+1 702.792.3773

London*
+44 (0)203 349 8700

Los Angeles
+1 310.586.7700

Mexico City+
+52 55 5029.0000

Miami
+1 305.579.0500

New Jersey
+1 973.360.7900

New York
+1 212.801.9200

Northern Virginia
+1 703.749.1300

Orange County
+1 949.732.6500

Orlando
+1 407.420.1000

Philadelphia
+1 215.988.7800

Phoenix
+1 602.445.8000

Sacramento
+1 916.442.1111

San Francisco
+1 415.655.1300

Seoul∞
+82 (0) 2.369.1000

Shanghai
+86 (0) 21.6391.6633

Silicon Valley
+1 650.328.8500

Tallahassee
+1 850.222.6891

Tampa
+1 813.318.5700

Tel Aviv^
+03.636.6000

Tokyo¤
+81 (0)3 3216 7211

Warsaw~
+48 22 690 6100

Washington, D.C.
+1 202.331.3100

Westchester County
+1 914.286.2900

West Palm Beach
+1 561.650.7900