THE
NATIONAL LAW REVIEW

What Does Brexit Mean for Data Protection?

Monday, March 11, 2019

With less than a month to go until the UK is due to leave the EU (at 11pm GMT/12pm CET on 29 March 2019), there is still much uncertainty as to whether, and if so how, the UK will exit the EU (commonly dubbed "Brexit"). In light of this uncertainty we outline what will happen, and what should be considered, depending on how things play out especially given the important votes due to take place within the UK Parliament this week.

Article By Proskauer Rose LLP
Kelly McMullonPrivacy Law Blog

Communications, Media & Internet
Global
European Union
United Kingdom

What happens if there is a deal?

Currently, as the UK is part of the EU and so has implemented the General Data Protection Regulation (the "GDPR"), there are unrestricted personal data flows between the UK and the rest of the EU.

If the UK and EU are able to agree a deal as to how Brexit will be implemented (officially the "Agreement on the Withdrawal of the United Kingdom from the European Union", or "withdrawal agreement"), that will mean that the EU and UK will enter into a transition period (to 31 December 2020, or possibly later) during which time the EU and UK will seek to agree to a new long term trade deal.

During this transition period the UK must abide by all EU rules. With respect to data protection considerations that means that personal data can continue to flow freely during this transition period. The EU will use this time to assess whether the UK's data protection practices are essentially equivalent to the EU's and "endeavour to adopt" an adequacy decision to seek to ensure the continued free flow of personal data after the transition period.

The EU has recognized a limited number of countries as providing "adequate" protection for individuals' personal data, such that personal data can be transferred freely from the EU to these non-EU jurisdictions. The list currently includes Israel, transfers made under the Privacy Shield framework in the USA, Switzerland, and most recently Japan.

The UK will have to be assessed like any other country that wishes to receive an "adequacy decision". The UK has a head start given that it has implemented the GDPR, but the result of the adequacy assessment is not a foregone conclusion. The EU will look at all aspects of UK data privacy protection including the rule of law and the access public authorities have to personal data. On the latter, for instance, the European Court of Justice has been concerned about the access the UK's security services can have to personal data. The UK Government has sought to resolve this concern.

Meanwhile, the UK will incorporate the GDPR into UK law with references to EU bodies/legislation instead referring to the appropriate UK bodies and incorporated legislation.

What happens if there is no deal?

In a "no deal" Brexit, there will be no transitional arrangements in place. Though the UK will still incorporate the GDPR into UK law, the UK will be seen as a third country by the EU. Businesses should therefore consider the following areas that could require action:

Privacy Documentation: Consider, and if necessary update, privacy related documentation and agreements including references to the EU, UK, and the European Economic Area ("EEA"), references to relevant privacy

legislation and associated terminology. The EEA is the EU Member States plus Iceland, Liechtenstein and Norway.

International Transfers: Consider and map any personal data flows between the UK and EU/EEA. The UK Government has already made clear that with respect to transfers from the UK to the EU/EEA, the UK will view the EU/EEA as adequate. The UK will also view as adequate the laws of any other country that has already received an adequacy decision, though exporters from the countries considered adequate will need to comply with any local law.

With respect to personal data transfers from the EU/EEA to the UK, the EU/EEA will consider the UK as a third country. The EU/EEA will not consider the UK "adequate", and so those transfers will need to occur on another lawful basis, such as binding corporate rules ("BCRs") or standard contractual clauses. The EU/EEA will, in time, assess the UK's adequacy, though there would be no agreed timeframe and the process can take a number of years.

Therefore, in this situation, there will be a need for businesses to ensure that there are appropriate safeguards in place (or that there is an exception that can be relied upon) to lawfully transfer personal data from the EU/EEA to the UK.

If that safeguard is binding corporate rules, consider where the current lead authority is. If the current lead authority is the UK, then that will need to change to an EU lead authority. BCRs will also need to be updated to ensure that the UK is considered a third country.

The UK and the EU would both need to approve any future BCRs.

One-Stop Shop: If the UK was previously the lead authority, then the business will need to consider if any of its other operations in the EU could be the lead authority instead.

EU Representative: If a business is based in the UK and does not otherwise have operations in the EU but targets data subjects in the EU or monitors the behaviour of data subjects in the EU, the business should consider whether it needs to appoint an EU representative. The UK will also replicate this provision such that if a business is based outside of the UK, but targets data subjects in the UK or monitors the behaviour of data subjects in the UK, then an UK representative should be appointed.

Breach Reporting: If a breach occurs in both the UK and in the EU, then the business will need to report the breach to both the ICO and the relevant data protection authority/ies in the EU. This could lead to fines being imposed by both the ICO and the EU data protection authority/ies.

I've heard that Brexit could be delayed or even halted, what happens then?

At the time of writing, it is not clear if Brexit will be delayed or halted, but what is clear is unless and until the UK exits the EU, then the status quo will continue. Whilst the UK is a member of the EU and EEA, personal data can continue to flow freely.