WALKERS

Global Legal and Professional Services

# Brexit – Data protection implications

26 July 2016

The outcome of the UK's recent EU membership referendum has raised a host of questions on what will happen next following the UK's decision to exit from the EU. One major concern for businesses sending personal data to and/or from the UK will be the effect of Brexit on the data protection landscape over the coming years.

## Timing

The timing of the UK's likely exit from the EU is significant as a major overhaul of existing EU data protection law is scheduled to come into effect in May 2018 with the commencement of the General Data Protection Regulation ("GDPR"). Given that the UK must serve a two year notice period under Article 50 of the Lisbon Treaty, the GDPR will most likely be in effect in the UK for a number of months (if not longer) before it exits the EU.

## Territorial scope of GDPR

Regardless of Brexit, a UK business trading in the EU post-May 2018 will need to comply with GDPR as the obligations in GDPR apply to businesses located anywhere in the world which process EU citizen's data in connection with the provision of goods/services or the monitoring of customer behaviour.

## Post-Brexit options

The eventual data protection landscape in the UK will likely reflect the nature of the UK's post-Brexit relationship with the EU, with the folowing representing some of the possible outcomes:

- UK obtains an adequacy decision from the European Commission

  The UK's data protection laws currently implement EU data protection law which means that in theory it should not be difficult for the UK to obtain an adequacy decision, which would result in transfers of personal data between the UK and the EU continuing as before Brexit. However, the UK would probably have to update its data protection laws in 2018 to comply with GDPR in order to obtain and/or sustain any adequacy decision granted in its favour. Switzerland as a non-EEA member currently benefits from an adequacy decision and has indicated that it intends to sustain its adequacy status post-GDPR.

- UK joins the EEA

  As a condition of the joining the EEA and being able to access the EU single market, it likely that the UK would have to comply with the GDPR. Norway, Iceland and Liechtenstein (the non-EU members of the EEA) all currently comply with existing EU data protection laws.

- UK decides to reduce personal data restrictions to become a more business-friendly destination

  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. While this might be beneficial in some respects, this might also restrict UK companies' ability to receive personal data originating from the EU.

- UK agrees a "UK Privacy Shield" with the EU

  UK companies could voluntarily agree to provide enhanced data protection in return for being able to receive personal data from companies in the EU. The enhanced standard would, at least from May 2018, be measured in comparison with the GDPR.

## Contacts

If you have any queries on the above or would like to discuss in more detail please do not hesitate to contact us or your regular Walkers contact.

Eoin O'Connor
Partner - Head of Risk and Compliance, Ireland
T: +353 1 470 6664
E: eoin.oconnor@walkersglobal.com

Shane Martin
Regulatory Compliance Director
T: +353 1 470 6673
E: shane.martin@walkersglobal.com

This advisory is part of a series of client advisories on the potential impact of Brexit prepared for clients of Walkers' office in Ireland. The full series may be found in the Brexit section of our website.