Client Update
Brexit: What Now for UK Data Protection?

LONDON
Jane Shvets
jshvets@debevoise.com

Christopher Garrett
cgarrett@debevoise.com

FRANKFURT
Dr. Thomas Schürrle
tschuerrle@debevoise.com

Dr. Friedrich Popp
fpopp@debevoise.com

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

WASHINGTON, D.C.
Jeffrey P. Cunard
jpcunard@debevoise.com

As with many other areas of UK law, uncertainty surrounds the future of UK data protection law following the recent referendum vote in favour of the leaving the European Union (the "EU"). The main concern relates to the ease with which personal data will be able to be transferred from the EU to the UK. Once the UK withdraws from the EU and unless it joins the European Economic Area (the "EEA"), the UK will be treated, from a data protection perspective, in the same way as all other non-EEA countries ("Third Countries"). The manner and extent to which EU companies will be able to continue to transfer personal data to the UK (or to the US via the UK) will depend upon the view taken by the European Commission (the "Commission") as to whether, post-Brexit, UK law offers protection to personal data that is essentially equivalent to protection in the EU. Whilst the greatest impact may be felt by companies whose businesses intrinsically involve personal information, such as social media companies and payment processors, it is likely that all multinational companies with a presence in the UK will experience some change.

Despite this uncertainty, UK-based companies doing business in the EU should continue to prepare for compliance with the EU's General Data Protection Regulation ("GDPR") coming into force in May 2018. If a UK company after Brexit does business in the EU by offering goods or services, the GDPR will apply to it directly and fully, without the necessity of an EU establishment which is currently required for EU law to apply, even if the data of EU-located data subjects are processed only on a UK-based server.

BACKGROUND

Data protection in the UK is currently governed by the Data Protection Act 1998 (the "DPA"), implementing into UK law the requirements of the EU's Data Protection Directive (the "Directive"). The GDPR, which will come into force in May 2018, will repeal the Directive.

Although the timing of Brexit is uncertain, once the UK gives notice of its intention to leave the EU under Article 50 of the Treaty on European Union, there is a two-year period during which the EU and the UK would negotiate the terms of the UK's withdrawal.[1] As this notice has not yet been given, and may not be for several months, it is not unlikely that the UK will still be a member state of the EU when the GDPR comes into force. As a regulation, the GDPR will have direct effect in each of the EU's member states, meaning not only that domestic legislation is not required to implement it (although the GDPR does allow for certain matters to be further regulated by domestic legislation, and some members states may have supplementary data protection laws) but also that it overrides the DPA. Under ordinary circumstances, the DPA would be repealed by the UK parliament at the same time as the GPDR comes into force. Once the UK leaves the EU, the GDPR will cease to apply directly in the UK, except to those who must continue to comply due to the scope of the GDPR (see below).

Assuming that the DPA is repealed, the UK Parliament will therefore need to pass new data protection legislation following Brexit. One option would be to pass legislation essentially mirroring the GDPR. For the reasons set out below, this would be the option least likely to disrupt existing flows of data between the UK and the remaining EU member states, and to the US via the UK. A second option would be to preserve or, if it is repealed in anticipation of the GDPR coming into force, to reinstate the DPA. For businesses operating solely within the UK, this would preserve the position as it currently stands, although by that point businesses are likely to have had to comply with the GDPR already. It is in our view unlikely, however, that the Commission would consider that simply retaining the DPA would meet the standards required for an adequacy decision and thus permit the free transfer of personal data. If this is the route that the UK takes, it will make the transfer of personal data to the UK from the EU more difficult. A third, and least likely, option would be for the UK to turn its back on EU-style data protection regulation and implement a less restrictive law allowing freer movement of personal data across borders than is currently permitted under the Directive and the GDPR, when it comes into force, whilst preserving individuals' rights to respect for their private lives, as required by the UK Human Rights Act 1998.

TRANSFERS OF PERSONAL DATA FROM THE EU TO UK

The Directive and the legislation implemented by Member States of the EU and the other members of the EEA allow transfers of personal data from EU/EEA

[1] This period can be extended by agreement between the European Council and the UK.

countries to countries outside the EEA only under limited circumstances. Either the destination country must provide an "adequate level of protection" to personal data, or one of a specific set of other conditions must apply to the transfer. To date, these issues have not been relevant to transfers to the UK from other EU or EEA member states. This will change once the UK leaves the EU.

Under the Directive and, from May 2018, under the GDPR, the Commission has the power to make determinations that a Third Country ensures an adequate level of protection, allowing transfers to that country subject only to the same restrictions on transfers within the EEA. This has been a high-profile issue in recent months, particularly in relation to transfers of personal data to the US, following the ruling by the European Court of Justice that the approval previously granted by the Commission to the EU-US Safe Harbor protocol was not valid,[2] and criticism of its replacement, the "Privacy Shield". Much of the controversy surrounding transfers of personal data to the US has arisen due to concerns around the surveillance and investigative powers of US government agencies, following the revelations made by Edward Snowden. The practices of the UK were also put under the spotlight by the Snowden revelations.

Will the Commission decide that the UK offers adequate protection to personal data? If the UK implements legislation of essential equivalence to the GDPR, this will surely ease the path to a finding of adequacy from the Commission, although it is possible that the UK's government surveillance powers will complicate the process. Even assuming that an adequacy decision will be made by the Commission, whether that is in place at the time of Brexit is a matter of speculation. If it is not, then there will be an interim period where transfers of personal data to the UK from EU member states can only take place through compliance with one of the other applicable conditions, such as the use of standard contractual clauses approved by the Commission or local data protection authorities. European national data protection regulators are unlikely to turn a blind eye to this issue.

SCOPE OF THE GDPR

One of the significant differences to be brought about by the GPDR is the expansion of the scope of EU data protection law. Unlike existing laws within the EU, which require an entity to have an establishment in the EU (albeit this is has a very broad meaning in this context) before coming within their scope, the GDPR will also apply whenever: (i) the personal data of an individual located in

[2] See: http://www.debevoise.com/insights/publications/2015/10/transfers-of-personal-data-to-the-united-states.

the EU is processed in relation to goods/services offered to him/her or (ii) the behaviour of individuals within the EU is "monitored". Therefore, irrespective of the future developments of UK legislation, UK businesses which offer goods or services to EU residents will need to comply with the GDPR.

WHAT SHOULD COMPANIES DO NOW?

There is no immediate need for action, as the UK is likely to remain a member of the EU for at least the next two years and personal data can still be transferred from the other EU or EEA member states in the same way as before during this period. There is, therefore, no need for companies to commence steps immediately to move the processing of personal data to outside the UK. If, however, a company is currently considering where to establish an EU data centre or to otherwise centralise the processing of EU data, the UK may be a less attractive option given the present state of uncertainty. We are closely monitoring the intended direction of UK data protection law post-Brexit and will update our clients when the situation becomes clearer.

In the meantime, UK-based companies that process personal data of individuals in the EU to whom they offer goods or services should continue to make preparations for the new requirements of the GDPR.

* * *

Please do not hesitate to contact us with any questions.