The Debrief

What a No-Deal Brexit Would Mean For Transfers of Personal Data

December 21, 2018

As the probability of a "no-deal Brexit" increases, companies should consider how that outcome would affect their ability to transfer personal data between the UK and the European Economic Area[1] (the "EEA"), and what steps they should take to prepare.

Debevoise & Plimpton

WHAT IS THE ISSUE?

Transfers of personal data to jurisdictions outside the EEA are subject to additional requirements under the EU General Data Protection Regulation ("GDPR"), unless the recipient is in a jurisdiction that benefits from an adequacy decision of the European Commission (the "Commission"). The Commission has stated that the adoption of an adequacy decision for the UK "is not part of the Commission's contingency planning" for Brexit. As a result, if there is a "no-deal Brexit", transfers of personal data to the UK will be subject to the same rules as transfers to any other non-EEA jurisdiction without an adequacy decision. That is so despite the fact that UK companies would still have to comply with GDPR-style requirements, imposed on them by the UK Data Protection Act 2018 and, in many cases, by the extraterritorial application of the GDPR.

In contrast, under current proposals, transfers of personal data from the UK to the EEA (and other countries that benefit from a Commission adequacy decision) would not be affected—even in the case of a "no-deal Brexit". The Department for Digital, Culture, Media & Sport has confirmed that the UK intends to recognise on a transitional basis all EEA states, EU and EEA institutions and Gibraltar as providing an adequate level of protection for personal data, as well as preserving, also on a transitional basis, the effect of existing Commission adequacy decisions, allowing data to continue to flow to these destinations.

---

[1] The EEA is comprised of the member states of the EU (Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and, currently, the UK) in addition to Liechtenstein, Norway and Iceland.

WHAT SHOULD COMPANIES DO?

- Companies within the EEA should ensure that they have a valid GDPR basis for transferring personal data to the UK after Brexit.

- For companies that transfer personal data between affiliated EEA and UK operations, the easiest option to maintain those data flows is likely to be to enter into intra-company agreements based on the EU Standard Contractual Clauses. Alternatively, they could implement group-wide Binding Corporate Rules or rely on various exemptions for specific data transfers. Binding Corporate Rules require the approval of the relevant data protection supervisory authority, so it is unlikely such a solution could be implemented prior to Brexit unless preparations are already underway.

- Companies with more complex data flows should review their onward transfers to third parties, whether those third parties are inside or outside of the UK. For example, any third-party transfer of data that was transferred to the UK using Standard Contractual Clauses may necessitate a new set of Standard Contractual Clauses to be entered into with the third-party data recipient.

- Companies that may have used their UK affiliates as a hub for the transfer of personal data from the EEA to third parties elsewhere in the world may want to reconsider those data flows to allow for data transfers directly from the EEA to third countries, reducing the complexity and the number of agreements using the Standard Contractual Clauses that would need to be in place. That may require amendments to existing data transfer agreements.

- If companies rely on the consent of individuals to transfer their personal data outside of the EEA, those consents should be reviewed to ensure that they adequately cover transfers to the UK.

- Likewise, companies should review their GDPR transparency notices (usually implemented as privacy policies or notices) to make sure that they transparently disclose personal data transfers to the UK.

OTHER ISSUES

A "no-deal Brexit" will present a number of other data protection related challenges for companies operating in the UK and the EEA. In particular, companies should consider the following:

- Companies with EU and UK operations that have "nominated" the UK's Information Commissioner's Office ("ICO") as their lead data protection authority should identify which of the EU data protection authorities would serve in that role. The ICO would no longer have a role in the GDPR regulatory regime, including the lead supervisory authority mechanism, after Brexit.

- UK companies that are not established in the EU but that are subject to the extraterritorial jurisdiction of the GDPR would need to consider the GDPR's requirement to appoint an EU representative. Similarly, the UK government intends to require controllers based outside of the UK to appoint a representative in the UK.

Debevoise advises EU and non-EU businesses on all areas of GDPR compliance. We look forward to discussing these issues with you.

Jane Shvets
Partner, London
+44 20 7786 9163
jshvets@debevoise.com

John Young
International Counsel, London
+44 20 7786 5459
jyoung@debevoise.com

Simon Witney
Special Counsel, London
+44 20 7786 5511
switney@debevoise.com

Clare Swirski
International Consultant, London
+44 20 7786 3017
cswirski@debevoise.com

Christopher Garrett
Associate, London
+44 20 7786 9072
cgarrett@debevoise.com