

Data Protection Post-Brexit

November 7, 2018

Brexit will have fundamental implications for data protection, in particular, the ongoing flow of personal data from the European Union to the UK. However, as with many other issues, the precise implications will depend on the type of deal reached between the EU and the UK.

Data Protection in the UK

Data protection in the UK is currently governed by the EU General Data Protection Regulation 2016/679 (GDPR) as applied by the UK's Data Protection Act 2018 (DPA).

If the UK leaves the EU on March 29, 2019 as planned, the DPA will remain in place and the European Union (Withdrawal) Act 2018 – the legislative framework for the UK's withdrawal (Brexit) from the EU – will incorporate the GDPR into UK law.

In March 2018, the UK and the EU reached political consensus on the terms of a transitional period that will start on March 29, 2019, until December 31, 2020. Such terms are intended to be included in the EU-UK withdrawal agreement, which is still being negotiated. If a transitional period is formally agreed on the proposed terms, common EU rules (including the GDPR) will continue to apply in the UK during such period.

International Transfers

The GDPR prohibits the transfer of personal data to third countries unless: (a) the transfer is made to an "adequate jurisdiction;" (b) the data exporter has implemented a lawful data transfer mechanism, for example, EU Standard Contractual Clauses, Binding Corporate Rules or the EU/Swiss-Privacy Shield; or (c) an exemption or derogation under the GDPR otherwise applies.

On exit from the EU, the UK will be considered a third country and as such, transfers of personal data from the EU to the UK will need to satisfy one of these three conditions.

Adequacy Decision

In May 2018, the UK government published a position paper outlining its proposal for a post-Brexit data agreement. In the proposal, the UK is seeking a legally binding agreement to allow for EU-UK data flows post-Brexit that the EU cannot change unilaterally. Interestingly, there is now precedent for such a

bilateral agreement, with the EU and Japan recently having agreed on a reciprocal adequacy assessment. However, this agreement took years to negotiate, and Michel Barnier (the EU's chief Brexit negotiator) has since rejected the UK's proposal on the basis that the proposed framework goes beyond the standard adequacy approach the EU has adopted for other third countries.

Interestingly, the European Commission has indicated that it will not consider a determination of adequacy for the UK until the point at which the UK is considered a third country (i.e., on March 29, 2019).

Further, while in theory an adequacy decision should be possible to obtain, given that the UK has only very recently incorporated the GDPR into UK law and as such, should be "essentially equivalent" to the EU, the question of adequacy is broader than data protection legislation alone. In particular, if the UK is to obtain a post-Brexit adequacy decision from the European Commission, it can expect its surveillance regime (including the UK Investigatory Powers Act 2016) to come under close scrutiny. Indeed, the recent European Court of Human Rights ruling in *Big Brother Watch and Others v. The United Kingdom*, which found that UK law enforcement agencies engaged in bulk interception of private electronic communications with insufficient safeguards in violation of fundamental rights, is likely to complicate matters further.

Standard Contractual Clauses

On September 13, 2018, the UK government published a technical notice, "Data protection if there's no Brexit deal," which sets out recommended actions for UK organizations to take to enable the continued flow of personal data from the EU to the UK in the event that the UK leaves the EU with no exit agreement in place. In particular, the UK government recommends that organizations consider using standard contractual clauses (SCCs) as the mechanism to legitimize transfers of personal data from the EU to the UK (i.e., with the UK as the data importer).

Interestingly, the technical notice did not address either transfers of personal data from the UK to the U.S. (i.e., what actions will be taken in relation to the EU-U.S. Privacy Shield), nor the onward transfer from the UK of personal data received from the EU to a third country (e.g., India).

Immediate Steps?

It remains to be seen what the UK's international data transfer mechanism will look like post-Brexit. Will the UK adopt the EU's SCCs, as Israel and Switzerland have done? Will it develop its own form? With so much uncertainty surrounding post-Brexit international transfers, it is recommended that organizations review their existing data transfer solutions now and determine what steps should be taken to minimize any post-Brexit disruption of data flows.

For more information and updates, please visit our [Brexit Resource Page](#).

CONTACTS

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you

usually work, or

William RM Long, Partner

+44 20 7360 2061, wlong@sidley.com

Francesca Blythe, Partner

+44 20 7360 2058, fblythe@sidley.com

Attorney Advertising—Sidley Austin LLP is a global law firm. Our addresses and contact information can be found at www.sidley.com/en/locations/offices.

Sidley provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Readers should not act upon this information without seeking advice from professional advisers. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at www.sidley.com/disclaimer.

© Sidley Austin LLP