The Global Data Protection Implications of "Brexit"

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

Christopher Kuner
Brussels Privacy Hub

Dan Jerker B. Svantesson
Bond University

Orla Lynskey
London School of Economics

Christopher Millard
Cloud Legal Project

Follow this and additional works at: https://www.repository.law.indiana.edu/facpub
Part of the International Law Commons, and the Privacy Law Commons

Recommended Citation
Cate, Fred H.; Kuner, Christopher; Svantesson, Dan Jerker B.; Lynskey, Orla; and Millard, Christopher, "The Global Data Protection Implications of "Brexit"" (2016). Articles by Maurer Faculty. 2631.
https://www.repository.law.indiana.edu/facpub/2631

This Editorial is brought to you for free and open access by the Faculty Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Articles by Maurer Faculty by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact rvaughan@indiana.edu.
On 23 June 2016, the UK voted by referendum to leave the European Union (EU). This vote may have significant implications for data protection law both in the UK and globally. There is now particular uncertainty regarding the fate of the EU’s General Data Protection Regulation (GDPR) in the UK, while, beyond the UK, Brexit will again put the spotlight on the EU’s criterion of ‘adequacy’ for data transfers to third countries. These implications will be briefly sketched here.

The decision to leave the EU is likely to have data protection consequences within the UK. The Data Protection Act (DPA) 1998, which transposed the European Data Protection Directive (Directive 95/46 EC), was due to be replaced by the GDPR on 25 May 2018. While the UK’s Minister for Data Protection has not ruled out the possibility that the GDPR will still take effect in the UK on that date, this is not certain. The UK has yet to trigger the exit mechanism to leave the EU (Article 50 of the Treaty on the Functioning of the EU). However, if it does, it will ordinarily have two years to renegotiate its legal relationship with the EU. There will therefore be a time period between the entry into force of the GDPR in May 2018 and the conclusion of the re-negotiation agreement when the UK will find itself in a legal limbo.

The UK will then have three choices. First, it may request that the GDPR never enters into force in the UK. It could argue that it would be impracticable and inefficient for the UK to require data controllers, data processors, and the regulator to implement the changes required to comply with the GDPR if this law would not be retained post-Brexit. The 1998 DPA would thus continue in force until new data protection legislation is implemented. For such a solution to be lawful, it would require further action, for instance, an amendment to this end in the GDPR. Alternatively, the UK may stall for time while awaiting the outcome of EU–UK negotiations in the knowledge that any infringement proceedings against it for breach of its EU data protection law obligations would likely be equally protracted. Finally, it could recognize the GDPR and implement the accompanying legislative measures to be fully compliant with EU data protection law.

Proops has suggested that this latter option—full compliance with the GDPR—seems most likely for several reasons: post-Brexit governments will have more important legislative initiatives to tackle; GDPR compliance may be required by the EU as a pre-condition for participation in the single market; there may be support for the pre-existing levels of data protection embodied in the GDPR in the UK; and, perhaps most importantly, that ‘heavy tinkering with the GDPR principles may well threaten [the UK’s] ability to secure a finding of “adequacy” when it comes to cross-border transfers from the EU’.2

It is this element—the fact that Brexit will shine a light on the adequacy of the regimes governing personal data processing in the UK—that is likely to be of most interest to those beyond the UK. In October 2015, the Court of Justice of the EU (CJEU) invalidated the EU–US Safe Harbor scheme on the grounds that the USA did not meet the EU’s strict standards for ‘adequate’ data protection. A challenge is currently pending before an Irish Court on similar grounds against the use of model clauses for EU–US transfers in a case dubbed ‘Schrems II’. The UK will therefore be keen to secure...
recognition of the adequacy of its data protection framework so that data flows between the UK and the EU will not be suspended or affected as a result of Brexit.

Adequacy is assessed against a stringent standard of ‘essential equivalence’ to the EU regime. While the UK regime does not need to be identical to the EU regime to be adequate, one easy way to secure such a finding of adequacy may be to simply adopt the GDPR. Indeed, there have already been suggestions by industry experts that any variation in legislation may convince firms that it is more cost-effective and less cumbersome to host data in the EU rather than the UK. Yet, despite such fears, the UK may opt for a data protection regime that differs from the GDPR and is more closely aligned to those of its Commonwealth partners or other allies. Members of the ICO have recognized that ‘international consistency is crucial’ while highlighting that such consistency could be achieved by aligning the UK data protection framework to that of other international jurisdictions. Bourne, for instance, has emphasized that alternatives may be ‘much more attractive than GDPR internationally’ and that there are ‘many countries all over the world, in places like Australia, Indonesia, New Zealand and Canada where there is a fully functioning data privacy law’. Similarly, while acknowledging that the underlying reality on which policy is based has not changed all that much, the Minister for Data Protection, Baroness Neville-Rolfe, has left the door open to the possibility that ‘the detailed future may be different’.

It will not, however, be the level of protection offered by the legislation that ultimately replaces the 1998 DPA that will attract most scrutiny in the context of an adequacy assessment. A legal and political blind eye has been turned to the elephant in the room following the Snowden revelations, namely that GCHQ, the UK’s intelligence and security agency, was allegedly engaged in mass personal data interception and retention without putting in place the requisite safeguards for individual rights. The UK, which has hitherto benefited from a presumption of ‘adequacy’, is, in this regard, difficult to differentiate from the USA, which was deemed not to meet the ‘adequacy’ standard in Schrems. This presumption of adequacy was never challenged following the Snowden revelations, although legal proceedings against the State were initiated for an alleged breach of Article 8 of the European Convention on Human Rights.

Further doubt regarding the adequacy of the UK regime may arise as a result of the current data retention legislation in place—the Data Retention and Investigatory Powers Act (DRIPA) 2014. The High Court of England and Wales deemed this Act to be incompatible with EU law and on appeal the Court of Appeal referred a number of questions to the ECJ. In particular, the Court of Appeal wishes to ascertain whether the ECJ’s judgment in Digital Rights Ireland lays down mandatory requirements for future data retention legislation and whether the judgment in Digital Rights Ireland expands the scope of the EU Charter rights beyond Article 8 ECHR. This preliminary reference was joined to a pending Swedish preliminary reference and made subject to an expedited procedure. A judgment is therefore expected before the end of the year. The Advocate General’s Opinion, delivered in July, suggests that the safeguards set out by the Court of Justice in Digital Rights Ireland are mandatory. If the Court concurs with the Advocate General’s Opinion, then it would appear that neither current nor proposed UK data retention legislation contain all of the mandatory safeguards, thereby casting doubt on the ‘adequacy’ of the UK legal framework for data protection as a whole.

If the UK does not remain part of the EEA, it would face the same adequacy conundrum as other non-EU/EEA states. The departure of the UK from the EU may lead to further jurisprudence on the adequacy standard, thereby crystallizing the EU’s strong stance on data protection. However, it is equally plausible that as data protection is not treated as a fundamental right in the UK, Brexit may strengthen the hand of those States who wish to regulate personal data processing differently and to strike an alternative balance between fundamental rights and other societal interests in data protection law. The EU has thus far acted as a benchmark for strict data protection laws and a leader in data protection matters. However, Brexit may facilitate a new international consensus.

Of course, Brexit also raises a number of issues of political and legal importance on a global level that we cannot analyse in detail here, but that have significant implications for the future. The popular frustration
with the political system that led to the vote for Brexit is present in many other EU Member States as well, and also in other regions of the world (including the USA). The GDPR was enacted to harmonize data protection law across the EU, but the political momentum seems to be in favour of increasing fragmentation. It is questionable whether legal harmonization can lead to greater uniformity of data protection and practice at a time when the political trends are moving in the opposite direction. Only time will tell how the legal issues of Brexit are resolved, and whether it remains an isolated incident or just the first example of a broader trend.