www.worldcommercereview.com

Post-Brexit transfers of personal data: the clock is ticking

EU-UK talks on a future data-sharing relationship have yet to start. J Scott Marcus says this bodes poorly for the UKs future status under GDPR

The UK government would like to keep EU-UK data transfers largely the same following the country's separation from the EU. But talks have yet to even commence on a future data-sharing relationship, and a landmark European Court of Human Rights ruling in September bodes poorly for the UK's future status under the EU's General Data Protection Regulation.

The UK economy is closely integrated with that of the rest of the EU. One need only consider the number of UK firms with branches in the EU27, and the number of EU27 firms with branches in the UK, to realise that data interchange is of vital economic importance.

Assuming that the UK indeed leaves the EU as a result of the Brexit referendum of June 23rd 2016, transfers of personal data from the EU27 to the UK may become problematic. This problem has long been recognised, but the associated risks have increased markedly in the past few weeks. Aside from the obvious risks associated with the UK 'crashing out' with no agreement at all in place, newly visible developments include:

- An acknowledgement by the UK's digital minister Margot James (on October 24th) that substantive talks on data sharing between the EU27 and the UK had not yet even commenced; and

- A landmark ruling by the European Court of Human Rights (ECHR) (on September 13th) to the effect that GCHQ, the UK government's intelligence and security organisation, has breached human rights in its mass surveillance programme.

In its 'Chequers' White Paper, the UK Government called not only for an Adequacy Decision to permit personal data to be transferred in both directions largely as it is today, but also for a close integration of the UK into the ongoing

evolution of EU27 privacy policy. The developments noted above call into question whether this is a realistic hope in the limited time remaining.

The disruption of the UK 'crashing out' with no agreement in place would likely be severe.

If the UK is to avoid economically harmful limitations to its ability to transfer personal data to the EU27, UK security services should be working now to consider undertakings that the UK would be willing to offer in order to address the concerns that the ECHR has already raised

The linkage between data transfers and surveillance for purposes of national security

The UK has already implemented the EU's General Data Protection Regulation (GDPR) in UK national law. Prime Minister Theresa May has rightly claimed that the UK has *"exceptionally high standards of data protection"*. This is all well and good, but it is not sufficient to ensure continued transfer of personal data to the UK post-Brexit.

For the UK to no longer be an EU or EEA member state would raise issues that previously emerged in a case brought by Austrian privacy activist Maximilian Schrems. A European Court of Justice (ECJ) ruling on October 6th 2015[1] invalidated data transfers from the EU to the US under a Safe Harbour agreement that had existed since July 2000. The finding was that the personal data of EU users is not adequately protected when it is transferred to the US from the EU because US firms make the data available to the US National Security Agency (NSA), for which the Safe Harbour protections are either unavailable or irrelevant[2].

As long as the UK is an EU member state, transfers of personally identifiable data to the UK are governed by Article 23 of the GDPR, which permits member states to take liberties with data protection and data transfers when doing so *"respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard … national security"*.

If the UK were no longer an EU (or EEA) member state, the UK would become a third country relative to the GDPR, and transfers of personal data would instead be governed by Articles 45 through 49 of the GDPR. Article 45 of the GDPR is consistent with the Schrems Decision, but it establishes a much higher threshold for transfers of personal data.

In order to establish an adequacy decision (the GDPR equivalent of Safe Harbour), the European Commission would be obliged to take account of *"the rule of law, respect for human rights and fundamental freedoms, relevant legislation,*

both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data". In light of GCHQ activities, the UK would be unlikely to get a free ride.

Even if there were strong economic and political grounds to do so, these privacy issues cannot simply be waved away. In the EU, privacy is treated as a human right under the European Convention on Human Rights. It is not easy to grant administrative latitude to the enforcement of a human right.

What sequence of events is likely?

Prior to the developments of the past few weeks, one might have expected the following sequence of events:

- Brexit takes place in some form other than EEA membership (unfortunately):
- The Commission grants an Adequacy Decision permitting EU27 personal data to be shared with parties in the EU).
- An appeal similar to the Schrems case is filed and works its way up to the ECJ.
- The ECJ rules as they did in Schrems, thus invalidating the Adequacy Decision, but probably allowing the UK and the EU27 time to put other arrangements in place.
- There would then be the risk that data transfers would be blocked until and unless an agreement analogous to Privacy Shield[3] were negotiated between the UK and the EU27. The agreement would ideally be better structured than Privacy Shield, which has not yet been shown to be effective.

In light of the September 13th finding of the ECHR, one has to wonder whether it will still be possible for the Commission to issue the Adequacy Decision that appears in the second bullet. Recall that the ECHR found the UK guilty of abuse of human rights in September due to its overbearing surveillance. Under these circumstances, the Commission may not be able to grant the Adequacy Decision; having granted it, there is no assurance that it would be sustained.

As previously mentioned, in granting an Adequacy Decision the Commission is obliged under Article 45 of GDPR to take into account *"the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country"*.

Given that ECHR has already ruled that the UK's surveillance services are in violation of Articles 8 and 10 of the European Convention on Human Rights, can the Commission grant the Adequacy Decision in the absence of concrete commitments from the UK security establishment?

The Adequacy Decision entails a complex procedure consisting of (1) a proposal from the European Commission, (2) an opinion of the of the European Data Protection Board, (3) an approval from representatives of EU countries, and (4) the adoption of the decision by the European commissioners. This presumably cannot take place overnight.

Even after the Adequacy Decision is in place, it might or might not be sustainable. The European Parliament and the Council could at any time request that the European Commission amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation. In the absence of concrete

commitments from the UK security establishment, the Parliament would likely have concerns over an Adequacy Decision.

Aside from that, a case similar to the Schrems case should be expected. In the absence of changes on the part of the UK security establishment, a similar ECJ outcome should be expected.

Implications

This seems to be headed for a rather bad place. In the unlikely event that the UK were to become an EEA member (or were it not to exit at all), all of this could be avoided. In all other scenarios, and especially in the 'crashing out' scenario, problems with data transfers appear highly likely.

This is in nobody's interest. It would harm both the UK and the EU27 economies.

These problems are not amenable to a quick fix through legislative or administrative measures. Most probably needed are some actual accommodations in the manner in which the UK conducts surveillance for purposes of national security.

The ECHR did not argue that surveillance is prohibited per se; what they argued, rather, is that it must be subject to a range of procedures and protections, as established in the case law. Notably, the ECHR *"was satisfied that the intelligence services of the United Kingdom take their Convention obligations seriously and are not abusing their powers, [but] it found that there was inadequate independent oversight of the selection and search processes involved in the operation, in particular when it came to selecting the internet bearers for interception and choosing the selectors and search criteria used to filter and select intercepted communications for examination.*

Furthermore, there were no real safeguards applicable to the selection of related communications data for examination, even though this data could reveal a great deal about a person's habits and contacts."

If the UK is to avoid economically harmful limitations to its ability to transfer personal data to the EU27, UK security services should be working now to consider undertakings that the UK would be willing to offer in order to address the concerns that the ECHR has already raised[4]. ■

J Scott Marcus is a Senior Fellow at Bruegel

Endnotes

1. As the ECJ's press release notes, "United States public authorities are not themselves subject to [the safe harbour agreement]. Furthermore, national security, public interest and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements. …" An additional concern was that "the persons concerned had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and … rectified or erased." See http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf. The decision itself appears at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362.

2. See also J Scott Marcus and Georgios Petropoulos (2016) 'Data transfers under the threat of terrorist attacks', Bruegel.

3. See J Scott Marcus and Georgios Petropoulos (2016) 'Data transfers under the threat of terrorist attacks', Bruegel.

4. There may be implications for EU27 security services as well under the UK equivalent of the GDPR, but these seem less immediate at the moment.

This article was originally published on Bruegel