CENTRE FOR EUROPEAN REFORM
LONDON ★ BRUSSELS ★ BERLIN

Insight

The three deaths of EU-UK data adequacy

by Zach Meyers and Camino Mortera-Martinez,15 November 2021

European and British businesses can still freely transfer personal data between the EU and UK. This situation has spared both sides disruption – but is unlikely to last.

In December 2020, as the deadline for Britain's departure from the EU's single market approached, British and European businesses became increasingly nervous. Boris Johnson's choice to prioritise regulatory freedom over close economic ties with the EU spelled trouble for businesses on both sides of the Channel. In part, this was because the EU could have made it significantly harder for companies to store and process the personal data of EU citizens on UK servers.

Most businesses gather personal data for one reason or another – whether it is because they make money out of transferring data or they simply operate a single customer database for their clients in Britain and elsewhere. In the absence of an adequacy decision, these businesses would have only had a few options, all of them costly. The most straightforward option is to rely on 'standard contractual clauses' (SCCs) – provisions added into business contracts to allow for data transfers. But even SCCs are not easy to implement: they cannot be adopted mechanistically, and the business must assess on a case-by-case basis whether additional data protections are required. The UK government estimates that adopting SCCs would impose a financial impact of £1.4bn on UK businesses trading with the EU over five years, much of which would be borne by small businesses.

Eventually, the UK and the EU managed to avoid this disruption. The British government retained the EU's General Data Protection Regulation (GDPR) in domestic law, and said it would continue to allow free data transfers to the EU. And the European Commission decided that the UK would continue to provide an adequate level of protection of personal data, thereby allowing data flows to continue without any new safeguards.

That adequacy decision is separate from the UK-EU trade and co-operation agreement (TCA), which is on life support due to the parties' dispute about the Northern Irish protocol. But, regardless of the fate of the TCA, seamless data transfers from Europe to Britain are very unlikely to last. There are three scenarios, any one of which could kill the EU's adequacy decision: the European Court of Justice (ECJ) ruling that the

UK's intelligence gathering should have prevented the Commission granting adequacy; the Commission choosing to withdraw adequacy because the UK diverges too far from the GDPR in the future; or the UK unilaterally deciding to allow seamless transfers between the UK and third countries, which would probably compel the Commission to revoke the adequacy decision. Navigating these risks is likely to become increasingly politically costly for the UK government. The question is not if smooth data transfers will end, but rather when, and how.

One: Death by privacy activist

The EU did not issue an adequacy decision merely because the UK continued to apply the GDPR; nor did it do so as a favour to Britain. The European Commission knows that the EU's interests are not served by suddenly disrupting EU-to-UK personal data flows – doing so would interrupt services provided to many EU consumers and businesses.

But if an activist like Max Schrems, the Austrian privacy campaigner, challenges the UK adequacy decision at the European Court of Justice, the court will not prioritise the economic relationship. The ECJ has twice overturned the Commission's adequacy decisions for the US – despite them being in the economic interest of EU and US businesses.

The ECJ will also not uphold the UK adequacy decision merely because that the UK's data protection laws are (for now) mostly unchanged from when the UK was an EU member-state. When the ECJ annulled the US adequacy decision, it was concerned that private companies which held European citizens' personal information could be required to hand it over to the US authorities for national security reasons. Similar concerns apply to the UK. The ECJ has repeatedly found data collection by British national security agencies to contravene EU law. This issue is particularly sensitive because it highlights a double standard: as an EU member, the ECJ's concerns about the UK's national security practices could not put the free flow of personal data at risk. But as a non-EU member, the very same practices could spell the end of free data flows.

In its adequacy decision, the Commission skirts around this double standard, and has tried, unconvincingly, to explain why – despite many contrary court judgments – UK national security laws comply with EU standards. The European Data Protection Board (EDPB) and the European Parliament have both also raised concerns about the Commission's assessment of UK national security laws. If someone decided to take up the case, which is not unfeasible, the ECJ is more likely than not to side with the Parliament and the EDPB, ending unfettered data flows unless the UK agreed to new safeguards and limits on its intelligence gathering. This is not something the current British government seems inclined to do.

Two: Death by divergence

Any serious UK departure from GDPR standards could be even riskier for data flows. Like any other EU adequacy decision, the EU institutions are allowed to monitor British laws to ensure divergence does not fundamentally change the legal framework which was deemed 'adequate'. Both the European Parliament and the Council of Ministers can ask the Commission to amend, or withdraw, an adequacy decision at any time if they feel Britain has lowered its privacy standards. Because of Brexit tensions, the EU added a specific clause to Britain's adequacy decision: it will stop to apply after four years unless the EU institutions decide otherwise.

The UK government knows that this is part of the deal. Yet it has recently published a consultation paper floating a range of possible changes to UK data protection law, which it claims are necessary to

promote "innovation and economic growth" and pose "no grounds whatsoever" for the EU's adequacy decision to be revoked. The government has also hired John Edwards, currently New Zealand's privacy commissioner, to lead the UK's data protection authority. New Zealand secured an EU adequacy decision in 2012, despite its data protection laws being less stringent than the GDPR in various respects. This suggests the UK wants Edwards to achieve maximum divergence: maintaining EU adequacy but stretching adequacy to its limits.

The UK's claim that rewriting privacy laws is necessary for economic growth is questionable, at least for now: the UK already has a world-class digital sector, all while (still) complying with GDPR. Only the US and China have more tech companies valued over $1bn. However, regardless of whether the reforms are necessary, the UK may be able to adopt some of them without losing adequacy. Many of the proposed changes are mere tweaks to the GDPR; others will probably be adopted by the EU itself in future. Take the internet's relentless cookie banners. Some of these cookies are used to collect data about the user's internet browsing habits in order to deliver personalised advertising. Other cookies are more benign: for example, they might be used only to anonymously measure how visitors interact with a website. The British government thinks these more benign cookies should not require user consent. The government also thinks consumers should be able to indicate their general acceptance or rejection of tracking cookies, rather than being repeatedly bombarded with individual cookie requests. Some EU member-states have already taken a similar approach to cookies: for example, the French data protection authority allows benign cookies to be used without consent in some cases. The EU institutions are also negotiating a revised ePrivacy Directive, which will probably encourage similar mechanisms to what the UK proposes. Most web browsers have blocked, or plan to block, tracking cookies in the long term anyway. So, one way or another, UK and EU practices in relation to cookies will probably remain similar even if the UK adopts these planned reforms – either invasive cookies will disappear altogether or the EU will adopt a more pragmatic approach, in line with the UK's intentions, to address the current bombardment of cookie requests.

The UK should not underestimate the importance of the Commission's broader political and economic calculations. If the EU sees continued UK adequacy as in the EU's interests, the Commission may be willing to overlook minor UK divergences. The Commission is not legally obliged to follow the European Parliament, which is likely to take a harder line, although it is unlikely to ignore Parliament's views entirely. Conversely, if the Commission no longer sees UK adequacy as in the EU's interests, it could take a stricter approach to the UK: the Commission may claim that the nature of the UK's economy, its proximity, and its desire for increased digital trade, mean that the EU should be less willing to tolerate divergences by the UK than the EU is with New Zealand, for example. The broader EU-UK relationship will be crucial to how UK divergences are perceived: EU diplomats have reportedly suggested using the threat of withdrawing adequacy as leverage to pressure the UK to abide by the Northern Ireland protocol. And if the UK nevertheless triggers the protocol's safeguard clause, Article 16, withdrawing adequacy may be part of the EU's response.

Other suggested reforms are so problematic that they would spell the end of free data flows regardless of the broader EU-UK relationship. For example, the UK proposes that citizens subjected to automated decision-making – such as being denied a mortgage based solely on an algorithm – should no longer have the automatic right to human intervention or oversight. This change is probably inconsistent with the UK's other international obligations and sharply diverges from the EU's plans for more safeguards on artificial intelligence. But the idea emerged from a report by several influential Conservative members of parliament, and may be politically difficult for the government to abandon. Similarly, some UK

government proposals would undermine the institutional independence of the UK's data protection regulator – for example, by allowing a government minister to approve or reject the regulator's guidance, and to directly appoint the chief executive of the regulator. The regulator itself has sounded alarm at how such changes would be perceived internationally. If such incendiary proposals are adopted, the Commission would feel compelled to rescind Britain's adequacy decision, politics aside.

Three: Death by circumvention

Finally, Britain's new global ambitions may end up killing the adequacy decision, too. The UK wants to enable free cross-border data transfers with new jurisdictions, including the United States, Australia, Singapore, Dubai and Colombia, none of which currently has an EU adequacy decision – although the US has an agreement allowing for the transfer of data for law enforcement purposes.

The UK government does not fully appreciate the risks that its 'Global Britain' strategy poses to data transfers to and from the EU. EU adequacy decisions assume that EU nationals' data will remain adequately protected even if the data are transferred onwards to a third country. The countries the EU recognises as adequate therefore generally create a 'closed ecosystem' – they only recognise each other as adequate. There are some minor exceptions – for example, Switzerland recognises Monaco as adequate, even though Monaco is not recognised as adequate by the EU; a similar concern applies to the UK's recognition of Gibraltar; and New Zealand has fewer safeguards for onward transfers generally. But the Commission considers such 'leakages' to be tolerably risky in practice. The Commission will be less accommodating if the UK allows EU nationals' personal data to be sent without restrictions to a big country which the EU does not recognise as adequate.

The UK's options in its attempt to secure a digital trading advantage over the EU, without compromising the EU adequacy decision, are therefore all unattractive. For example:

★ The UK could limit its own adequacy decisions with third countries, so that they only apply to UK citizens' personal data, and not to those of EU citizens. The UK government could then trumpet the success of Brexit in lowering trade barriers for the UK. But this would require UK businesses to distinguish between EU nationals' personal data and that of UK nationals – red tape that would offset the benefits of more data transfers.

★ The UK could conduct a two-way negotiation: one with the country it wants to recognise as adequate, and another with the Commission to seek assurances that its own adequacy decision would not be rescinded if it recognised the third country as adequate. However, even if the Commission entertained this proposal, it is unclear why a third country would agree to new data protections in negotiations with the UK, but would not do the same with the EU, which has a larger economy. At most, this approach might give the UK the advantage of being able to prioritise negotiations with its own preferred countries, rather than relying on the EU's priorities.

What choices does the UK have?

The UK's adequacy decision will almost certainly not endure. Britain can probably tweak its own data protection standards without putting the adequacy decision further at risk – but only to a limited extent, unless the UK-EU relationship improves. However, the political costs of maintaining adequacy will be high – the government may be pressured into limiting its intelligence gathering; it will need to forgo changes to its data protection laws championed by some influential Conservative politicians; and the UK will probably have to abandon its attempts to establish seamless transfers with third-countries.

Abandoning adequacy carries its own costs. In 2015-16, 75 per cent of the UK's data transfers were with other European countries, and the costs of losing EU adequacy could therefore be sizeable. The UK government itself estimates £1 billion in reduced trading revenue for businesses (some of which would cease trading) and £420m in compliance costs over five years. That implies an annual loss of about 0.1 per cent of the gross added value provided by the UK's digitally-intensive sectors. The UK will also need to pay higher prices for goods and services from EU businesses (because those businesses would pass on their own compliance costs to UK customers). And – despite those costs – many UK businesses will probably keep complying with GDPR, in order to keep doing as much business as possible with the EU.

As time goes on, the political compromises required to maintain adequacy will become harder for the UK to swallow, and the UK government will probably consider more seriously forcing UK business to bear the financial cost of losing adequacy. Increasing barriers to digital trade between the UK and the EU may be a strange choice, given the UK government's desire to see data-driven economic growth. But while the UK government continues to prioritise sovereignty over close economic ties, the outlook for data flows looks dim.

Zach Meyers is a research fellow and Camino Mortera-Martinez is a senior research fellow a the Centre for European Reform.