CENTRE FOR EUROPEAN REFORM
LONDON ★ BRUSSELS ★ BERLIN

Post-Brexit data transfers are not a done deal

by Sam Lowe and Camino Mortera-Martinez

Data transfers are essential for both trade and security co-operation. The EU and the UK should not let minor differences obscure the fact that they have more in common than divides them.

The freedom to move data between the EU and the UK is as important to some businesses as the freedom to move goods, services and people. And for European and British security services, the ability to share and access data about criminals is an essential component of keeping people safe. The European Commission's decision to propose two adequacy decisions for the transfer of personal data to the UK, under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), therefore came as a relief to both EU governments and the UK.

But this is just the beginning of a long, bumpy road. The Commission's adequacy decisions are not final: the European Data Protection Board (EDPB, an EU privacy oversight body) must issue an opinion and a committee of representatives from the 27 member-states must green-light the decisions. While the EDPB's opinion is not binding, it will indicate whether there are any grounds for concern amongst national data protection authorities. And if the adequacy decisions are adopted, the European Parliament and the Council of Ministers can ask the Commission to withdraw them at any time, if there are concerns about the way the UK is applying privacy rules. MEPs are already suspicious that Britain plans to undercut the EU on data protection in the future, and the threat of legal challenges looms large.

In 2013, Austrian lawyer Max Schrems complained to the Irish data protection authority about Facebook's transfers of European citizens' data to its Californian headquarters, under the EU-US Safe Harbour agreement. Schrems argued that the EU could not guarantee that its citizens' privacy would be respected when their data was transferred to the US, because surveillance laws there required private companies to hand data to the government. The case ended up before the European Court of Justice (ECJ), which eventually struck down the Safe Harbour agreement in 2015. In 2016 the EU replaced Safe Harbour with a data adequacy decision, known as the Privacy Shield. This too was felled by the ECJ in July 2020, after another case instigated by Schrems. Now transatlantic personal data transfers can only happen if the data subject consents or if transfers are needed for the fulfilment of a contract.

Commission officials are well aware that the UK adequacy decisions could face similar legal challenges and have set out in detail how the decisions will deal with some of the issues raised by the Schrems saga. For example, they will be reviewed every four years, to ensure compliance. But a review clause does not guarantee the UK adequacy decisions will continue; the Privacy Shield had to be re-examined every year and that did not stop it from being annulled by the ECJ.

An additional problem for the UK is that the ECJ has already said that UK data retention laws are not in line with EU standards. In 2016, the Court said that Britain's 2014 Data Retention and Investigatory Powers Act breached EU law because it allowed for general and indiscriminate retention of citizens' data by law enforcement authorities. And in a separate 2017 case, the ECJ ruled that the UK government should be more careful when gathering data, as it was failing to show why bulk data retention was needed for some investigations. The court has recently confirmed this view in cases against French and Belgian security services. While the adequacy decisions refer to all these cases, they do not explain how the ECJ's concerns may be assuaged.

Eventually the longevity of the UK data adequacy decisions may depend on perceptions, and in particular the growing EU suspicion that the UK will renege on its previous commitments in order to eke out a competitive advantage for its companies. The UK has already signalled that it intends to embrace a less defensive attitude to cross-border data liberalisation than the EU. In its trade agreement with Japan, in contrast to the EU's with Japan, the UK accepted provisions preventing unjustified data localisation measures and restrictions on the free flow of data between the two countries. The UK also intends to accede to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) – an agreement on trade and investment between 11 Pacific countries – which has liberal commitments on the flow of data.

This is not to say that the UK intends to rip up its privacy laws. The British government hopes to be able to retain adequacy decisions with the EU, while pursuing a more forward-thinking approach to data in its trade agreements. Technically speaking this should be possible. Both Japan and New Zealand benefit from EU adequacy decisions, despite being members of CPTPP, and despite some early EU concerns about onward data transfers in the case of Japan. And notwithstanding some EU suspicion of CPTPP's data provisions, GDPR is arguably covered by the agreement's exemptions, which allow for restrictions on data flows so long as they serve a legitimate public policy objective.

The main difference between the EU and others such as Japan, the US, and now the UK, is one of mind-set: whereas the EU presumes the data protection regimes of other countries are inadequate unless proven otherwise, others reverse the burden of proof.

On the EU side, the Commission has found itself in a never-ending struggle to balance its desire to set global standards on data against the inherent aversion of some member-states to any measures that could jeopardise the privacy of their citizens. But the EU will not succeed in setting the global agenda on data if it only approaches the topic defensively. The pandemic has changed the way people use and understand data, and the real-time sharing of open-source data helped scientists to develop COVID-19 vaccines speedily. And citizens' health data will be more public after the pandemic: the EU has recently published plans for a 'vaccine passport', which will allow vaccinated and COVID-19-negative people to travel across the bloc. Such sensitive data sharing would have been unimaginable a few months ago.

In practice, the EU and UK are more instinctively aligned on privacy and data flows than some law-makers think, despite slightly different conceptual frameworks. But trust between the parties is in short supply, with the UK's seemingly cavalier approach to its Withdrawal Agreement commitments, and the EU's threats to restrict vaccine exports to Britain. There is a risk that any and every UK action could be viewed by the EU as an aggressive act, and an excuse to rescind the adequacy decisions. This would be a mistake.

The real threat to the EU's attempts to establish global data protection norms and protect its citizens' privacy is not the UK, or even the US, but digital-authoritarian China. The EU should prioritise reaching a common understanding with the UK, the US and other like-minded countries – perhaps by opening up the membership of its proposed EU-US Trade and Technology Council. And if legal challenges continue to make it hard for non-EU businesses and law enforcement agencies to share data with the EU, the bloc should contemplate alternative routes instead. The EU could consider offering to sign all-encompassing data treaties with close partners that include judicial redress and co-ordinated review clauses, to avoid the problems raised by the Schrems rulings. The 2016 EU-US Umbrella Agreement on law enforcement data transfers could be a good model to follow, as it is an overarching treaty that has, for now, escaped legal challenges. Despite the present acrimony, data sharing between the EU and UK remains vital for the trade and security of both.

Sam Lowe
Senior research fellow, CER
@SamuelMarcLowe
Camino Mortera-Martinez
Senior research fellow, CER
@CaminoMortera