DATA PROTECTION AND EU - UK DATA TRANSFERS

(Paper 2 of a series of 3)

By Tom Hayes, BEERG Executive Director

Introduction

***BREXIT REALITIES:** The announcement that the UK will not be extending the Brexit transition arrangement beyond December 31, 2020 means that, as and from January 1 next, the UK will be outside the EU's single market and customs union, the framework of EU law and the jurisdiction of the European Court of Justice.*

This paper on data protection and data transfers between EU and UK is the second of three BEERG papers examining what this means for. Data protection and data transfers between the EU and the UK. Paper #1 looks at European Works Councils and Paper #2 looks at Freedom of movement between the EU and the UK

An individual can send her or his personal data to anywhere in the world anytime they want, and they freely do so every day. That is their choice.

But there are significant political and legal problems for businesses when transferring personal data between countries. Call them "data borders".

Governments put data borders in place to protect the privacy of their citizens. Nowhere is this truer than in Europe where personal privacy and data protection are values core to the European Union. This is not surprising, given the Continent's searing experiences with Nazism and Communism.

GDPR

The transfer of personal data across borders is central to businesses in the age of the internet and social media. To facilitate such transfers within the Single Market the European Union has crafted the General Data Protection Regulation (GDPR). The GDPR treats the EU as a single entity within which personal data can be transferred freely by businesses from country to country.

The GDPR also has provisions which allow for the transfer of data outside the EU, subject to stringent conditions.

Key to the working of the GDPR is the role of the Court of Justice of the European Union (CJEU). It ensures that Europe's data laws are correctly interpreted and enforced. It is not swayed by economic considerations in doing so, as shown, for instance, in its striking down of the EU/US Safe Harbour arrangement (here). European citizens know that there is a robust judicial mechanism in place to guarantee their data privacy rights.

Even though it left the EU on January 31 last, the UK remains within the Single Market during the transition period which runs until December 31, 2020, and so also remains within the protective framework of the GDPR.

Brexit Problem

The central Brexit problem is this. Once the UK quits the Single Market on January 1, 2021, it puts itself outside the framework and the GDPR and the jurisdiction of the CJEU. In doing so it puts a new data border in place where none previously existed.

Of course, in leaving the EU's Single Market and Customs Union the UK is recreating trade and travel borders that previously existed before it joined the EU back in 1973. We know that recreating such borders will put in place barriers to trade and travel involving customs controls, regulatory paperwork, and costs, where none now exist. But we have been here before, even if a long time ago, and we know what border controls on goods and people look like.

But the EU's "common data space" has grown while the UK has been a member of the EU as information and communications technology (ICT) created new industries and radically changed the way many others work. The enabling legal framework has grown in parallel.

There is no prior example of a country leaving a "common data space" and disavowing the enabling legal framework that make such a space possible. What will happen when you put data borders in place for the first time between a country and its biggest export market for goods and services?

We cannot know as there are no precedents to guide us. But it is not going to be easy and may be a lot more difficult than many people believe. In an area as politically sensitive as data privacy, politics are going to trump business considerations. If the UK wants its Brexit omelette, many eggs are going to get broken. After Jan 1, 2021 things are going to be different, very different. If they are not going to be different, why leave the EU in the first place?

No one can say that they were not warned

Speaking at the 28th Congress of the International Federation for European Law (FIDE) in Lisbon in May, 2018, the EU's chief Brexit negotiator Michel Barnier devoted a considerable section of his speech to the impact of Brexit on data transfers between the EU and UK after the UK finally leaves . He made it clear that "the UK must understand that the only possibility for the EU to protect personal data is through an adequacy decision".

In his speech Barnier was blunt about the EU's position on data transfers and that position has not moved since then. Indeed, in view of developments after Barnier's speech it may well have hardened. Optimistic views that the UK will get, is almost entitled to, a data adequacy decision are wide of the mark in our view.

Certainly, from the point of view of the transnational business community a data adequacy decision is highly desirable and to be devoutly wished, but it would be a major mistake to take such a decision as a given. There are significant political groups and privacy campaigners who are opposed to such a decision and they are not without influence. If such a decision is given in favour of the UK there will be legal challenges to it in a heartbeat. A long period of uncertainty looms, no matter what happens.

It is our view that it would be prudent for businesses to plan on the basis that as and from January 1, 2021, the UK will be outside the EU's data protection framework without an adequacy decision and that there will be significant legal difficulties in transferring personal data from the EU to the UK.

In the absence of an adequacy decision there are no easy alternatives because all the possible alternatives such as **Binding Corporate Rules and Model Contractual Clauses** are also under legal threat. (For a very full discussion around these issues see this report from UCL).

"But surely,", it will be argued, "given the importance to business on both sides of the Channel of data transfers from the EU to the UK and vice versa, the EU Commission is not going to let politics stand in the way of an adequacy decision."

To which the answer might be: "The UK is responsible for the uncertainty that will be created by deciding that Brexit meant it had to leave the EU's single market and legal framework. If the UK wanted to put economic and businesses interests before politics, it would not have left the EU in the first place. The UK cannot argue that Brexit is all about sovereignty and then complain when the EU exercises its own sovereignty and that of its member states. It was the UK that prioritised politics over economics."

For many citizens of the EU, "data sovereignty" is a core value and they will not easily agree to it being compromised simply to facilitate business with a "Brexit Britain" which left the EU to regain its own allegedly lost political sovereignty.

Fish count for more than "chips"

The following figures come from the British government's submission to the EU (here) on why it should be given a data adequacy decision:

> *The continued free flow of personal data is vital for the future relationship between the UK and the EU. Imports and exports of both goods and services heavily depend on the free flow of personal data between the UK and the EU. EU personal data-enabled services exports to the UK were worth approximately £42bn (€47bn) in 2018, and exports from the UK to the EU were worth £85bn (€96bn).*

Here are some contrasting figures from a report Fisheries and Brexit, published by the academic think-tank, The UK in a Changing Europe:

> *From a purely economic perspective, the fishing industry is not a significant economic activity in the UK. Only around 0.1% of gross value added (GVA) in the UK economy comes from the catching sector. This is less than the fish-processing sector, which is a larger economic sector by both GVA (£794 million versus £505 million) and employment (19,191 full-time employees versus 11,961 fishers).*

TechUK, a representative body for the IT industry, says on its website:

> *Around 850 companies are members of TechUK. Collectively they employ approximately 700,000 people, about half of all tech sector jobs in the UK.*

Which means that there are around 1.5m people working in "tech" in the UK, as opposed to 30,000 in the fishing industry. (The numbers depending on "tech" and EU/UK data transfers are probably considerably more, e.g., all those in the travel industry.)

When you "compare and contrast" the tech and fisheries industries financial and employment numbers you are left wondering why "control over the UK's coastal waters" is such a redline issue for the British negotiators in the Brexit process. Fisheries contribution to the UK economy is miniscule compared to that of the tech industry. "Unbalanced priorities" comes to mind.

Adequacy decision

Barnier said in 2018, and the EU has repeated consistently since then, that the best the UK can hope for is a "adequacy" decision. Adequacy decisions are made unilaterally by the European Commission. They are not negotiated or agreed with the third countries. The process involves:

- *a proposal from the European Commission*

- *an opinion of the of the European Data Protection Board*
- *an approval from representatives of EU countries by a majority vote*
- *the adoption of the decision by the European Commissioners*

At any time, the European Parliament and the Council may request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation. The effect of an adequacy decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary.

The validity of an adequacy decision can also be challenged before the CJEU.

Will the UK get an adequacy decision?

Earlier this year the UK made a comprehensive submission to the EU in support of its ask for an adequacy decision: here. The key UK arguments is that, having incorporated the GDPR into national legislation, UK data protection law meets EU standards.

Which is true, but as we have pointed out before, there is a major snag. The Investigatory Powers Act, which came into force at the end of 2016, allows the U.K. government to monitor large batches of data, collect people's browsing records and hack citizens' phones and computers for security purposes.

EU law provides for exemptions from general data protection principles in matters of:

- *national security and defence;*
- *the prevention, investigation, detection and prosecution of criminal offences;*
- *the protection of data subjects and the rights and freedom of others.*

But these exemptions only apply to EU and EEA member states. They do not apply to "third countries. There are many people in the EU governance system who regard the powers given to the UK security services, and other agencies, as far more intrusive than even the US services have.

The UK's position is not made any easier by reports such as this which suggests that the UK "has been illegally copying classified personal information from a database reserved for members of the passport-free Schengen travel zone."

Have a look at this recent letter from the European Data Protection Board to Sophie in't Veld MEP, and others, about an October, 2019, agreement signed between the UK and the US on Access to Electronic Data for the Purpose of Countering Serious Crime. The letter notes:

> *Finally, when it comes to a possible adequacy decision for the UK, the EDPB considers that the agreement concluded between the UK and the US will have to be taken into account by the European Commission in its overall assessment of the level of protection of personal data in the UK, in particular as regards the requirement to ensure continuity of protection in case of "onward transfers" from the UK to another third country.*

In mid-June, the European Parliament adopted a comprehensive statement on the future EU/UK relationship. It had this to say on data:

79. Stresses the importance of data protection both as a fundamental right, as well as a key enabler for the digital economy; notes that, according to the case-law of the CJEU, in order for the Commission to declare the adequacy of the UK data protection framework, it must demonstrate that the UK provides a

level of protection "essentially equivalent" to that offered by EU legal framework, including on onward transfers to third countries;

80. Recalls that the UK Data Protection Act provides for a general and broad exemption from the data protection principles and data subjects' rights for the processing of personal data for immigration purposes; is concerned that, when non-UK citizens' data are processed under this exemption, they are not protected in the same way as that of UK citizens and would be in conflict with Regulation (EU) 2016/679 of the European Parliament and of the Council; is of the view that the UK legal framework on the retention of electronic telecommunications data does not fulfil the conditions of the relevant EU acquis as interpreted by the CJEU, and does not, therefore, currently meet the conditions for adequacy;

81. Underlines and supports the future partnership being underpinned by commitments to respect fundamental rights, including adequate protection of personal data which is a necessary condition for the envisaged cooperation and by automatic suspension of the law enforcement agreement if the UK were to abrogate domestic law giving effect to the ECHR; calls on the Commission to pay particular attention to the UK legal framework when assessing its adequacy under EU law; advocates taking into consideration CJEU case-law in this field, such as the Schrems case, as well as ECHR case-law;

82. Takes the position that, if the UK does not explicitly commit to enforce the ECHR and will not accept the role of the CJEU, no agreement on judicial and police cooperation in criminal matters would be possible; regrets that the UK has so far refused to provide firm guarantees on fundamental rights and individual freedoms and insisted on lowering current standards and deviating from agreed mechanisms of data protection, including by the use of mass surveillance;

83. Calls on the Commission to take the above-mentioned elements into consideration when assessing the adequacy of the UK legal framework as regards the level of protection of personal data, and to ensure that the UK has resolved the problems identified in this resolution prior to possibly declaring UK data protection law adequate in line with EU law as interpreted by the CJEU; calls on the Commission also to seek the advice of the European Data Protection Board and the European Data Protection Supervisor;

While the EU Parliament has no direct role in the granting of an adequacy decision it does have a veto on any EU/UK future agreement. If the Parliament were to veto any agreement it is unlikely that the Commission would push ahead with an adequacy decision. Brexit Britain has no champions within the EU system.

So, to put it at its most blunt, there is no guarantee that the UK would get an adequacy decision from the EU post-Brexit. If it did get an adequacy decision that decision would be very quickly challenged in the CJEU.

Further, as EurActiv reports, Prime Minister Boris Johnson told the House of Commons in a written statement the United Kingdom will "develop separate and independent policies" in a range of fields, including data protection, adding that the government would seek to maintain high standards in so doing.

Which means that the UK may diverge from the GDPR over time which would put any data adequacy decision at risk.

So, where does that leave things?

Simply put, there can be no certainty on EU/UK data transfers anytime soon. The UK's insistence that it will not, in any circumstances, be subject to the jurisdiction of the CJEU rules out any type of "common data space" deal. Any other type of data transfer arrangement is legally fraught.

Bluntly, as of today, there is no good place a company can go to ensure continuity of data flows between the EU and the UK after January 1, 2021. All a company can do is what it can do.

After January 1, 2021, the UK will have its own, stand-alone data protection regime. For the moment, it will exactly mirror the EU's GDPR. The UK government has said that there will be no bar on the transfer of personal data from the UK to the EU and, unless the government says differently, companies should work on that basis.

However, it will no longer be possible to locate "EU data controllers" in the UK and companies which currently do so will need to look to move their data controllers to a jurisdiction within the EU. In deciding on a jurisdiction companies should keep in mind that GDPR fines can run to 4% of global turnover or €20m, whichever is the greater.

Given this risk, best to be in a jurisdiction where court proceeding are held in English. While Ireland obviously meets this criteria, other jurisdiction are offering English-language legal options. We strongly advise BEERG members to take detailed advice on the matter because this is not a decision to be rushed or taken lightly. Once taken, it may also be difficult to subsequently change.

If you have not already done so, look at the options of Binding Corporate Rules and Model Contractual Clauses. Yes, they may be struck down by the CJEU but until that happens, they offer some protection.

If all of this reads like EU/UK data transfers are heading towards a "black hole" well, regrettably, that is the way things are.

The EU is where it is. It is the UK that is walking away.

June 2020