20 SEPTEMBER 2018
#BREXIT
#DATAFLOWS
#NODEAL

JACQUES DELORS INSTITUTE
BERLIN
Centre for European Affairs at the Hertie School of Governance

TO BE OR NOT TO BE ADEQUATE

A GUIDE TO BREXIT AND DATA FLOWS

■ **PAUL-JASPER DITTRICH**
Research Fellow,
Jacques Delors Institute
Berlin

Executive summary

Personal data and data transfers were probably not uppermost in the minds of many Brits as they cast their votes on June 23rd 2016. However, while issues such the Irish border or the fate of British nationals living in the EU now dominate the headlines, future relations regarding data transfers and data protection are probably going to exercise one of the biggest economic impacts on the UK and the EU27 alike over the longer term.

The reason for this is straightforward: On March 29th 2019, the UK will leave the European Union and become a third country. As such, personal data can no longer be transferred automati-cally between the UK and the Single Market. The General Data Protection Regulation (GDPR), which took effect in May 2018, places strict requirements on how to transfer data from the EU to third countries. With the adequacy procedure, it also provides a framework for how a country's data protection regime can be declared equivalent to EU standards, which in turn allows businesses to transfer personal data to that country.

It is far from certain, however, that the UK will be able to secure a positive adequacy decision in due time, if at all. Furthermore, the UK and the EU have to negotiate the extent of their future institutional collaboration on data protection. Companies which regularly transfer data between the two will probably have to take additional precautions if they wish to shield themselves from potential economic damage, especially in the event of a "no deal"-scenario.

This paper examines these challenges in more detail. It first provides an overview of the role of data and data exchanges in modern economies. The following section outlines different scenarios for the transfer of personal data post-Brexit and explains how the adequacy procedure works. The final section concludes by examining further options for cooperation on data protection post-Brexit.

TABLE OF CONTENTS

1 . DATA FLOWS BETWEEN THE UK AND THE EU: WHAT'S AT STAKE?

1.1 The importance of data flows for trade

Brexit threatens to hamper the frictionless exchange of personal data for businesses: As a third country the UK's data protection regime will no longer be considered automatically adequate to the European level of protection. Personal data from European citizens cannot be transferred automatically any longer from the Single Market to the UK and processed there. Without new arrangements in place, businesses face legal uncertainty and even temporary disruption of services if they are unprepared.

> TRADE INTEGRATION IS MORE AND MORE DRIVEN BY DIGITAL CROSS-BORDER SUPPLY CHAINS

Even though there is less news coverage on this particular Brexit-induced issue, this problem might turn out to be much larger in the event of a "no deal"-Brexit than most politicians and government officials currently anticipate. Trade integration is more and more driven by digital cross-border supply chains, which rely on the frictionless transfer of personal employee or cus-tomer data. From multinational companies with back-end data centres across the Single Market to medical start-ups analysing X-ray pictures from all over Europe, cross-border business activity has become intimately linked to the uninterrupted flow of personal data across borders. Industries that are especially data-reliant for exporting services are telecommunications, finance and entertainment. As a result of higher connectivity, better computer processing power, the rise of the data economy and increasing data-enabled trade in services, global cross-border data flows (measured in bandwidth usage) increased 45 times between 2005 and 2014 and are expected to increase a further ninefold by 2021. It has been estimated that up to 3.8 percent of global GDP depends on cross-border data flows.[1]

Within Europe, the structure of the British economy stands exemplarily for this changing trade landscape. The country is heavily focused on services (in particular finance); 43 per cent of total exports are services-related. The country is also the European frontrunner in the development of digital applications. The British digital technology business segment contributes roughly ten percent of the entire UK services output, which is the highest share in the G20. About one third of all European AI start-ups are located in the UK, and London is considered the European capital for fintechs.[2] Europe's largest (and the world's third largest) data centre is located in the UK.[3]

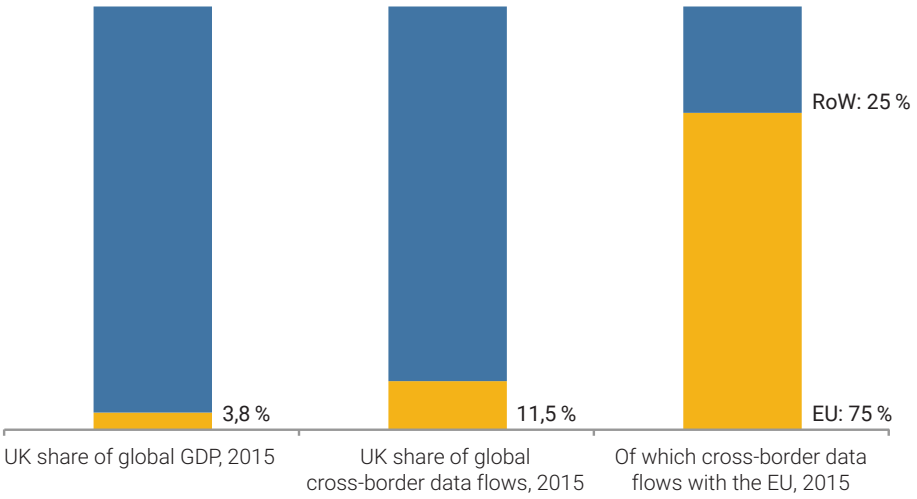
A growing volume of trade between UK and EU is digitally enabled. Private online shoppers as well as large corporations relying on physical and digital supply chains regularly transfer personal data across the Channel. The UK has not only a very high share of global data flows trans-ferred via its territory compared to its GDP (see chart on the following page), but most of these flows are connected to the EU: An estimated three quarters of all UK data flows are with the EU.[4] Such flows provide information, communications, search, audio and video, financial transactions or inter- and intra-company traffic. It is impossible to say with any precision to what extent these flows convey personal information linked to European data subjects. It is

1. McKinsey Global Institute, "Digital Globalization: The new Era of Global Flows", 03.2016.
2. Roland Berger, "Artificial Intelligence – A Strategy for European Startups", 2018.
3. Aditya Kishore, "Should UK data centres fear Brexit?, DatacenterDynamics", 26.04.2016.
4. UK House of Lords, "Brexit: The EU data protection package", 3rd Report of Session 2017–19, 18.07.2017.

equally difficult to pinpoint down the exact economic fallout for the EU if they were interrupted. However, the majority of trade in services is underpinned by cross-border data flows.

The economic fallout consequent upon this legal uncertainty would probably be worse for the UK than the EU, given the make-up of its economy, which is much more reliant on services and services exports than most other European economies as we have seen. However, European companies will also face uncertainties and bureaucratic requirements in the event of a Brexit with no agreed future framework. Investment decisions might be delayed or called off entirely due to uncertainty concerning the rules of transferring personal data from the EU to the UK. First signs of data-related divestment in the UK are already emerging in the news.[5]

FIGURE 1 . The UK is deeply integrated in global and European data flows



Source: Frontier Economics and Eurostat.

2 . DATA FLOWS AFTER MARCH 29TH

How exactly does Brexit threaten to disrupt data flows? In a nutshell, the underlying problem is the following: As a member of the EU and the Single Market the UK's level of data protection is considered to be adequate (consistent) with EU standards and businesses can move personal data around and process it (store, analyse, combine etc.…) without any further safeguards. After Brexit, this will no longer automatically be the case. Instead, the UK is likely to be considered a "third country" and its data protection regime will no longer be considered to be safe for the automatic transfer and storage of personal data of European citizens to the UK.[6] For the unhampered transfer of personal data to be restored UK data protection will have to be considered adequate to EU levels of protection.

5. Aliya Ram, Nicolas Megaw, Mehreen Khan, "Companies review arrangements for data transfer after Brexit", Financial Times, 11.08.2018.
6. European Commission, "Notice to Stakeholders, Withdrawal of the United Kingdom from the Union and EU Rules in the Field of Data Protection", 09 January 2018.

The future relationship on data flows will depend on the type of Brexit, i.e. the degree of any future political, legal, institutional and economic tie-up of the UK with the bloc. The options range from a continuation of current data transfer practices (with the UK joining the European Economic Area or EEA) to a temporary disruption of flows in a no-deal scenario. The most likely outcome, however, is that the EU will review the UK's data protection framework during the transition phase and eventually declare it adequate.

2.1 EEA membership: An unlikely scenario

If the UK stayed in the Single Market post-Brexit (for example within the EEA, similar to Norway) and remained under the jurisdiction of the European Court of Justice (ECJ), personal data could be exchanged across borders without any further restriction.[7] The current provisions on data exchange (regarding the free flow of data and security cooperation) would stay in place. As an EEA member, the General Data Protection Regulation would be fully applicable to the UK and the country might thus also be able to participate in the European Data Protection Board (EDPB). The EDPB is comprised of members of the national data protection agencies of the member states and the European Data Protection Supervisor (EDPS). One of its main tasks is to provide guidance in cross-border data protection disputes within the Single Market. While full membership is reserved to member states, the UK could, like Norway, become an observer state. However, an EEA-style scenario appears highly unlikely at this juncture as it would depend on a domestic turnaround in the UK, where currently the leadership of both parties has rejected anything resembling full participation in the Single Market under ECJ jurisdiction.

2.2 How to gain adequacy as a third country

If EEA-style membership is the least likely option for the future relationship between the UK and the EU, Britain will almost certainly become a "third country". The process is as follows: If the European Parliament and the House of Commons approve the Withdrawal Agreement, the so-called transition period starts after Brexit Day on March 29th. European rules of the acquis communitaire and hence rules on data protection and exchange will continue to apply until December 2020. Thereafter, the UK will be considered a "third country" and Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) rules for the transfer of data into third countries and the processing of personal data of European origin in third countries will govern future relations. The respective rules, most of them introduced already with the Data Protection Directive from 1995 (95/46/EC), have been revised, clarified and expanded with the GDPR.

> "THE GDPR ALLOWS FOR SEVERAL WAYS OF TRANSFERRING PERSONAL DATA TO A THIRD COUNTRY

Art. 44–Art. 50 of the GDPR govern the rules and provisions under which personal data may be transferred to and processed in non-EU/non-EEA third countries. The GDPR allows for several ways of transferring personal data to a third country. The most comprehensive tool to ensure the free flow of personal data between the EU and a given third country is for the EU Commission to take a so-called adequacy decision (Art. 45 GDPR).[8] Once the Commission has declared the given data protection level to be fully adequate to EU-standards, companies and

7. Apart from a small, but considerable number of national data localization measures, which in some member states for example force companies to store tax and other accounting data in the country they were generated. For more information see ECIPE, "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", Policy Brief No. 03/2016.
8. European Commission, "Adequacy of the protection of personal data in non-EU countries", Official Homepage.

authorities are allowed to transfer and process personal data from the EU without restrictions. This can cover the entire third country, a defined territory or a sector and is subject to continuous revision by the Commission.

The possibility of gaining adequacy status from the Commission already existed in the framework of the 1995 Data Protection Directive and is designed to ensure both the protection of personal data of European citizens outside EU territory and retain a frictionless flow of data across-borders. The regular procedure (based on Art. 45 GDPR) for acquiring adequacy is as follows: After the third country has approached the Commission to request an adequacy decision, the Commission reviews the data protection framework, supervisory bodies and compliance of the third country's data protection regime with the EU equivalent – as of May 25th 2018, the GDPR. After an adequacy decision is granted, the respective country is still subject to ongoing Commis-sion monitoring to ensure the lasting adequacy of the country's data protection regime with that of the EU. The European Parliament and the Council can request changes in the status of the adequacy decision (amend, withdraw).

> SO FAR, ONLY TWELVE DATA PROTECTION REGIMES OF OTHER COUNTRIES ARE FULLY RECOGNIZED AS ADEQUATE TO EUROPEAN STANDARDS

So far, only twelve data protection regimes of other countries (some of them Crown dependencies like Jersey) are fully recognized as adequate to European standards i.e. that they have introduced data protection provisions similar to those of the EU.[9] The US (with the Privacy Shield framework which replaced the Safe Harbour adequacy decision) and Canada (for commercial organizations) have been granted partial adequacy. The last country to receive adequacy status was Japan, following the conclusion of the EU-Japan Free Trade Agreement.[10] The two sides will mutually recognize their data protection regimes as adequate. The process took on average 28 months to be completed for each third country[11], and, in the case of the US, has been the subject of repeated legal battles over the legality of the data transfers. The minimum time needed to review, negotiate and eventually adopt an adequacy decision is estimated to be two years.

2.3 Towards a UK-EU Privacy Shield?

How likely is a swift and positive Commission decision on adequacy for the UK? The latter's case is unique as it has been part of the European regulatory framework and hence the Single Market's data protection regime. Hence, prospects for a swift process are high on the one hand. Some observers think that negotiations between the UK and the EU could be completed much faster and might take only between twelve and 18 months due to the proximity of the two data protection regimes. Primary reason for this optimism is the continued application of GDPR-standards of data protection post-Brexit and the new British Data Protection Act, which received Royal Assent on 23 May 2018.[12] The bill does not transpose the GDPR into UK law before or after the country leaves the EU. As a regulation, the GDPR took effect in the UK on 25 May 2018 as in every other member state. The transposition after Brexit will be achieved with the European Union (Withdrawal) Bill). However the bill assists and supplements the adoption of the GDPR and addresses areas where the regulation left room for national discre-

9. The European Commission lists the following countries and Crown dependencies on its website: Andorra, Argentina, Canada (limited to commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States (within the Privacy Shield Framework)
10. European Commission, "The European Union and Japan agreed to create the world's largest area of safe data flows", Press release, 17.07.2018.
11. Pieter Lamens and Evelyn Caesar, "GDPR & Brexit: Is there a need for an adequacy decision?", Deloitte.
12. HM Government, "Data Protection Act 2018", Official Homepage.

tion.[13] The country also has a well-respected and experienced data protection agency (Information Commissioner's Office). Most observers hence believe that the UK might in principle be able to get a swift adequacy decision.[14]

> SOME FACTORS SPEAK AGAINST AN EASY AND SWIFT PROCESS TO GAIN ADEQUACY

On the other hand, some factors speak against an easy and swift process. Since the 2015 ECJ decision on Safe Harbour[15] and the introduction of the GDPR any adequacy decision requires the protection of fundamental rights (one of which is data protection) as a precondition when it comes to third countries. The UK will have to prove that its level of protection is adequate to the status of a fundamental right. This process involves a review of any British legislation and practices connected to activities of the national security agencies and intelligence services.

The UK intelligence services have wide-ranging authorizations to access email data, tap telephone conversations or break into social media accounts, especially following the introduction of the Investigatory Powers Act 2016.[16] Moreover, the UK is part of the Five Eyes programme and might thus end up sharing intelligence data on European citizens with its four Anglo-American partners. During the review procedure for the adequacy decision, the Commission will examine the national security legislation of the UK. As a full member state, the country could rely on national security exemptions enshrined both in European data protection legislation and the Treaty on the Functioning of the European Union whenever its data surveillance programmes came under scrutiny by the ECJ.[17] Article 4(2) of the TFEU states that "In particular, national security remains the sole responsibility of each Member State".[18] The material and territorial scope of the GDPR explicitly excludes data processing carried out outside the scope of EU law, thus excluding national security.[19]

However, such exemptions do not apply for third countries. Thus, the UK might have difficulties getting an adequacy decision. Even if the Commission grants it the decision could eventually end up like the US whose Safe Harbour Decision taken by the Commission in 2000 was revoked by the ECJ in 2015 (Schrems case).[20] The UK and the EU might then have to negotiate an arrangement similar to Privacy Shield or even a bilateral agreement on data. The EU-American framework replaced the Safe Harbour adequacy decision, which was declared invalid in 2015 by the ECJ. In its essence it consists of informal guarantees given by the American administration and the Commission Implementing Decision (EU) 2016/1250. The rationale behind the frame-work is to restrict government's access to personal data (at least formally agreed) and to install a system for annual review as well as possibilities for redress in case of infringements. In this context it is also important to note that the UK, by leaving the EU, will also no longer be part of the EU-US Privacy Shield and will have to renegotiate a data-sharing agreement with the US. Any new agreement, however, will also be tightly scrutinised by the Commission and might well put any adequacy decision at risk.

13. Information Commissioner's Office, "An introduction to the Data Protection Bill", May 2018.
14. House of Commons, "The Progress of the UK's negotiations on EU withdrawal: Data", Seventh Report of Session 2017-19, 26.06.2018.
15. Judgement of the Court (Grand Chamber) of 6 October 2015, "Maximilian Schrems v Data Protection Commissioner".
16. UK Government, "UK-EU security cooperation after Brexit: EU data-sharing".
17. Karen Mc Cullagh, Brexit: "No 'clean break' for data protection law", University of East Anglia, International Law Blog.
18. EUR-LEX "Treaty on the Functioning of the European Union", Consolidated Version.
19. European Parliamentary Research Service, "Data protection rules applicable to the European Parliament and to MEPs Current regime and recent developments", Briefing, June 2018.
20. EUR-LEX "Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v Data Protection Commissioner".

2.4 What companies have to do in case of a "no deal"

From the perspectives of UK and EU businesses and other private entities transferring private data to Britain, there is also a worst-case scenario. If there is no deal on the parameters of the future relationship (and the Withdrawal Agreement) approved by the House of Commons and the European Parliament by March 29th, the UK would "crash out" of the Single Market. Accordingly, there would be no transition period during which the acquis still applies. The UK would immediately become a third country without any further safeguards in place. Such an outcome would cause disruptions for the exchange of business data post-Brexit.

It is also likely that in a "no deal"-scenario the Commission would start an adequacy procedure and eventually declare the data protection regime of the UK equivalent. However, this process will take time and political effort, even more so since leaving without a deal might further damage the political and diplomatic goodwill between the UK and the EU. In case of a no deal, businesses and other private entities would thus have to apply additional safeguards, if they seek to transfer all personal data (ranging from employee to customer data). Under the GDPR, transfer of personal data to countries whose level of data protection is not adequate to the EU is possible in the case of individual companies.

"THERE ARE TWO MAIN WAYS FOR INDIVIDUAL COMPANIES OR ORGANIZATIONS TO SECURE THEIR RIGHT TO TRANSFER DATA

In order to do so, the processor must give legal guarantees that the personal data in question will be sufficiently protected by the recipient through applying safeguards that ensure conformity with European data protection legislation. It is for example possible to transfer personal data if individuals have given their informed consent over the transfer and processing of their data. Companies can also transfer data in order to fulfil contractual obligations. Besides these possibilities, there are two main ways for individual companies or organizations to secure their right to transfer data from the EU to a third country.

1. EU-Standard contractual clauses

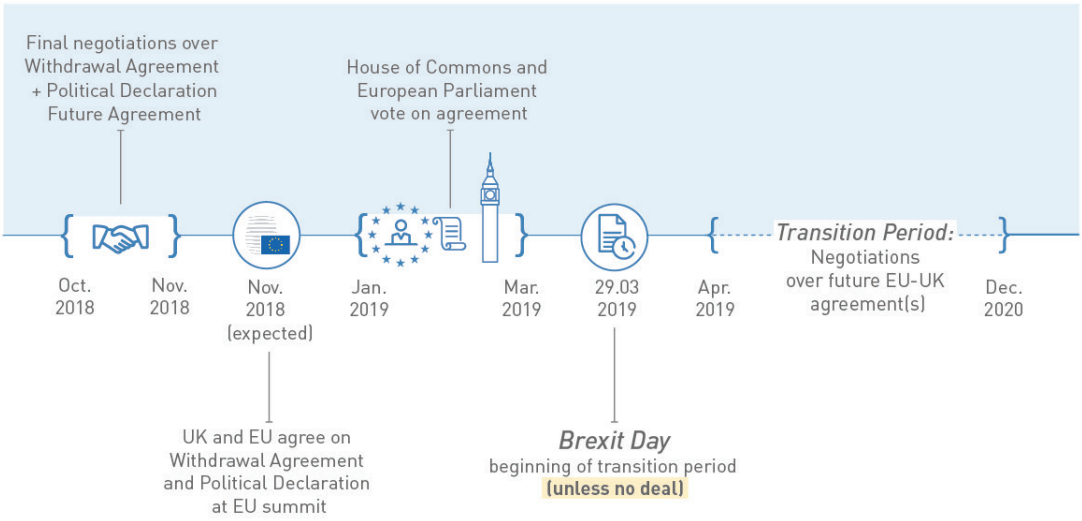
Companies can ensure the transfer of data to countries with no EU-level of data protection by adding EU-approved Standard Contractual Clauses (SCCs) to their service contracts and abiding by them (Art. 46 GDPR). The relevant Clauses (Commission Decisions 2001/497/EC, 2004/915/EC and 2010/87/EU) can be downloaded on the Commission website.[21] Their advantage is that they allow data transfer relatively easily. On the other hand, they are subject to regular changes and are for example being updated with the GDPR leading to additional bureaucratic procedures. The problem with SCCs is that they not really feasible for larger integrated companies which routinely have to transfer in-house large amounts of data between countries.

2. Binding Corporate Rules

The second common solution for intra-company data transfers to third countries is the use of Binding Corporate Rules (BCR, Art. 46 GDPR). As with a Code of Conduct, an international company can draft rules for internal data transfers in compliance with the provisions of the Eu-ropean data protection legislation.[22] National Data Protection Authorities must authorize BCRs (Art. 47 GDPR), a process that can be time-consuming and take up to a year. They are more flexible as they are written for each individual corporation. That makes them mainly attractive for larger corporations and less feasible for smaller companies.

21. European Commission, "Model Contracts for the transfer of personal data to third countries".
22. European Commission, "Binding Corporate Rules".

FIGURE 2 ▪ Timeline of Brexit negotiations and transition period



Grafik: Burak Korkmaz

3 ▪ POSSIBLE FUTURE RELATIONS BEYOND ADEQUACY

Two things are key for British-EU data relations post-Brexit. If and when the UK is granted adequacy and what the future cooperation will look like beyond the adequacy decision, i.e. the degree to which the UK will still be involved in European data protection governance and security cooperation.[23] The adequacy decision is the first and most important milestone on the road to a frictionless exchange of personal data post-Brexit. It is also the pre-condition for any other future arrangement on data protection. The British position during the Brexit negotiations has so far been that the UK should get a form of "special relationship" reflecting its historic economic and political/regulatory involvement with the EU.

> "THE COMMISSION HAS CONTINUOUSLY EXPRESSED THE VIEW THAT ANYTHING OTHER THAN THIRD COUNTRY STATUS WOULD PUT THE EU'S REGULATORY AND DECISION-MAKING AUTONOMY IN PERIL

This special relationship should have two components: An "economic partnership" that goes beyond the trade integration found in existing FTAs and covers institutional cooperation in more sectors, and a "security partnership", which maintains and develops existing mechanisms and channels for data exchange related to security cooperation. The Commission on the other hand has continuously expressed the view that the UK will become a third country after leaving the EU and that anything other than third country status and a future relationship based on an FTA would put the coherence of the four freedoms and the EU's regulatory and decision-making autonomy in peril. With regards to data and data flows there are two critical areas for the nature of the future relationship:

1) The political process and the nature of the agreement

Even though the UK will most likely leave the regulatory regime of the Single Market, the British government and Theresa May have outlined the UK's desire to stay in a special relationship with the EU, one which transcends the status of a mere third country. The White Paper mentions the adequacy decision as a mechanism to avoid "the need for other costly and burdensome

23. HM Government, "The Future Relationship between the United Kingdom and the European Union", 23 July 2018.

legal mechanisms, such as Standard Contractual Clauses".[24] It acknowledges the adequacy procedure as a starting point. From there, the UK seeks to negotiate a legally binding bilateral deal instead of a unilateral decision taken by the Commission on behalf of the member states. The Commission, concretely Chief Negotiator Michel Barnier,[25] has repeatedly made it clear that the UK will become a third country upon leaving the Union. It therefore rejects the idea of a "special status", i.e. any deeper integration beyond a Free Trade Agreement, in various policy areas. For data protection this means that the Commission has so far shown little willingness to negotiate any arrangements or treaties outside existing procedures for third countries. The future relationship on data protection should only be governed by the existing rules on adequacy described in the last section.[26]

2) The degree of integration into European data protection coordination post-Brexit

The UK would like to negotiate privileged access to the Single Market also with regards to the GDPR governance framework, in particular to the role of the UK's data protection agency, the ICO. Initially, the UK held out hope of keeping its membership and say on various boards of European agencies – the most important one in the area of data protection being the former Article 29 Working Party, which was replaced by European Data Protection Board on 25 May 2018 following the GDPR.[27] The UK still has a seat at the EDPB which it will lose after Brexit. It also hopes that a deal better than just third country status will ensure UK businesses are effectively represented under the EU's new 'One Stop Shop' mechanism for resolving data protection disputes. This allows companies operating in several countries of the Single Market to deal with only one data protection authority whose decision in a dispute will apply to all member states. The Commission by and large rejects the British proposals on future institutional governance for the same reasons it rejects a "special status" on data in general. Keeping the legal integrity of the Single Market means there cannot be a supervisory authority with a third country as a full member. Crucially, decision-making autonomy will have to remain exclusively with the EU. The UK argues that it will not interfere with the decision-making autonomy of the Union and accepts the ECJ's jurisdiction over the EDPB.[28] The EU, however, views the UK's position as an attempt to retain influence over the EU's jurisdiction post-Brexit.

CONCLUSION: TOWARDS ADEQUACY AND CAUTIOUS COLLABORATION?

The final adequacy decision given by the EU Commission is unilateral after it secures the green light from the Member States. Recent political signals, for example by Commissioner Vera Jourova, have been cautiously optimistic on a positive adequacy decision.[29] Even though the

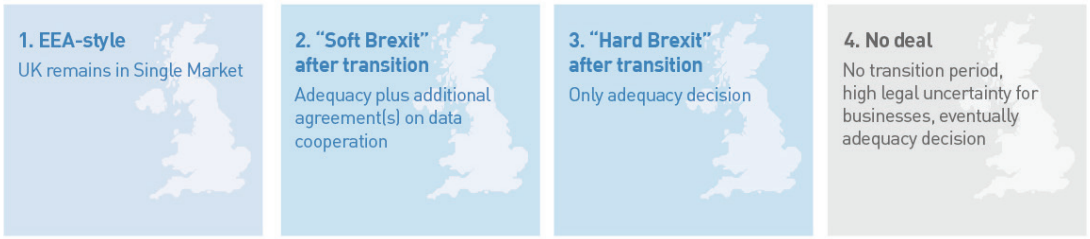
24. Ibid.
25. For example, European Commission, "Speech by Michel Barnier at the 28th Congress of the International Federation for European Law (FIDE)", Lisbon 26 May 2018 and "Speech by Michel Barnier at the European Union Agency for Fundamental Rights", Vienna 19 June 2018.
26. Ibid.
27. European Data Protection Board, Homepage.
28. House of Commons, "The Progress of the UK's negotiations on EU withdrawal: Data", Seventh Report of Session 2017–19, 26.06.2018.
29. Aliya Ram, Nicolas Megaw, Mehreen Khan, "Companies review arrangements for data transfer after Brexit", Financial Times, 11.08.2018.

Commission has to investigate British data protection legislation and practice, the political will in the EU favours such a positive decision. In the end, however, a positive adequacy decision could still be challenged by privacy activists on the grounds of mass surveillance practices of British intelligence services.

If the UK really wants to enjoy the benefits of European security information exchange systems or the European Data Protection Board, it must give up many of its red lines and accept the jurisdiction of the ECJ in those areas even after the transition period ends. It is very unlikely that the EU will move its negotiating position on this core issue and the Commission is in a much better bargaining position. Hence, it should not soften its position that anything other than third-country status for the UK with regards to data and data exchange would put the legal integrity of the Single Market and the decision-making autonomy of the EU in peril and is thus non-negotiable.

Common ground could possibly be found on some of the institutional issues. The ICO could, for example, become an observer member of the EDPB, just like Norway. Cooperation between the ICO and other EU data protection authorities should also not stop with Brexit. The ICO has played a significant part in the development of EU data protection laws and there should be ongoing cooperation between the ICO and EU Data Protection Authorities.

FIGURE 3 ▪ What will the future relationship look like? – Different scenarios



Grafik: Burak Korkmaz

ON THE SAME TOPIC

▪ Prof. Dr. Henrik Enderlein, "Twelve Thoughts on Brexit, An interim Review", Blog Post, Jacques Delors Institut – Berlin, 29 March 2018.

▪ Nicole Koenig, "Towards Norway plus? EU-UK defence cooperation post-Brexit", Blog Post, Jacques Delors Institut – Berlin, 7 February 2018.

▪ Dr. Funda Tekin, "The Area of Freedom, Security and Justice: Brexit does not mean Brexit", Policy Paper, Jacques Delors Institut – Berlin, 13 September 2017.

▪ Valentin Kreilinger, Sophia Becker, Laura Wolfstädter, "Brexit: Negotiation Phases and Scenarios of a Drama in Three Acts", Policy Paper, Jacques Delors Institut – Berlin, 25 January 2017.

NOTRE EUROPE JACQUES DELORS INSTITUTE
Hertie School of Governance

Friedrichstraße 194, D – 10117 Berlin
info@delorsinstitut.de
www.delorsinstitut.de