UCL EUROPEAN INSTITUTE

BREXIT INSIGHTS

EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?

Oliver Patel and Dr Nathan Lea

August 2019

EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?

Oliver Patel and Dr Nathan Lea[1]
August 2019

CONTENTS

Key Messages

◊ EU-UK data flows underpin the services economy and are vital for virtually any business with customers, suppliers or operations in the EU. Disruption to EU-UK data flows would be unprecedented and extremely damaging for business and the UK economy.

◊ For data to continue to flow freely between the EU and the UK, the EU needs to issue an 'adequacy decision'. This would exclude the UK from the EU's data protection governance framework but would avoid costly disruption.

◊ The adequacy assessment would happen during the transitional period that follows the ratification of the Withdrawal Agreement and would be separate from the wider Brexit negotiations.

◊ There is no guarantee of a positive adequacy decision. EU concerns could include:

» potential incompatibility of the UK's Investigatory Powers Act 2016 with EU law

» membership of the Five Eyes intelligence sharing alliance

» no fundamental right to data protection in the UK post-Brexit, as the UK is not retaining the EU Charter of Fundamental Rights

» potential for unprotected onward data transfers, especially to the US

» incompatibility of the 'immigration exemption' in the UK's Data Protection Act 2018 with EU law

◊ Unless the UK changes its national security and surveillance practices, it may not meet the threshold for adequacy. EU Member States can pursue independent national security policies, but those policies could become a problem (for data flows) when the UK becomes a third country.

◊ There are three possible 'no-deal on data flows' scenarios which would leave the UK without an adequacy decision:

Scenario 1) No Withdrawal Agreement: 'cliff edge' Brexit

Scenario 2) Withdrawal Agreement but no adequacy decision

Scenario 3) Adequacy decision after the transition period ends

◊ Even a positive adequacy decision could be revoked by the European Commission or invalidated by the Court of Justice of the European Union (CJEU) at any time.

◊ In the absence of an adequacy decision, UK to EU data flows should not be affected, as the UK has pledged. EU to UK data flows would not stop completely either, but they would be significantly disrupted, due to the costs, resources and bureaucracy which individual organisations would have to direct towards enabling data transfers to continue.

◊ Many large companies will be prepared and able to absorb the cost, but it will be harder for SMEs and startups.

◊ No-deal will cause legal confusion and uncertainty. Many organisations will not have set up the necessary alternative legal arrangements by then and could therefore face enforcement action and large fines from EU regulators for unlawful EU-UK data transfers.

1 **Oliver Patel** is Research Associate and Institute Manager at the UCL European Institute. **Dr Nathan Lea** is Senior Research Associate at the UCL Institute of Health Informatics. **Dr Uta Staiger**, Executive Director of the UCL European Institute, and **Anton Gromoczki**, Research Intern at the UCL European Institute, also made significant contributions to the writing of the paper.

The findings of this paper were, in part, derived from over fifty anonymous interviews with EU and UK politicians, civil servants, ambassadors, regulators, lawyers, businesses leaders and policy professionals conducted over the past two years. We thank UCL's Laidlaw Scholarship Programme for their generous support for this research.

1. Introduction

What are cross-border data flows?

Cross-border data flows encompass any situation where personal data is transferred from an entity in one country to an entity in another. The entities can be part of the same organisation, which is typical for large multinational corporations, or entirely different organisations. Although the concept of data flows is abstract, the phenomenon is tangible. Personal data is transferred over the internet from the IT servers of one entity, which are physically located in one jurisdiction, to the IT servers of a second entity, which are physically located in a separate jurisdiction.

The free flow of personal data underpins the modern economy, and there are countless examples of such data flows in every sector. Services sectors, which comprise 79% of the UK economy, are particularly reliant on data flows – especially finance, banking, retail and hospitality.[2] Digital technology companies are often the most reliant, and techUK describes the issue of data flows post-Brexit as 'mission critical' to the technology sector.[3] Given the UK's strength in services, and the fact that digital technology sectors contribute disproportionately to growth, any disruption to the free flow of data would be damaging.[4] This issue affects any UK organisation with suppliers, operations, or customers abroad. The tech sector is particularly exposed due to its use and monetisation of large volumes of data.

It is not easy to measure data flows, due to their ubiquity and virtual nature. Also, unlike trade, there are no legal obligations to monitor the volume of data flows. In consequence, it is not easy to measure the importance of data flows to the economy, nor the economic impact of disruption to data flows. However, its importance can be inferred from proxy measures. For example, half of all trade in services is enabled by seamless cross-border data flows.[5] Also, global data flows are estimated to have raised global GDP by 3% ($2.8 trillion) in 2014, and the UK is ranked as the third most connected country in the world for cross-border data flows.[6]

There are innumerable EU-UK data flows occurring each day to give a comprehensive account of them all. They permeate every sector and every type of organisation. Large multinational companies like banks often streamline all data processing in one European location then transfer data to offices in the UK. Also, all internet and software companies transfer data across borders to provide cloud-based services like email, calendar, file storage and social media timelines. University College London's email system, Microsoft Outlook, only works because data can be seamlessly transferred from servers in Ireland to servers in the UK.

Smaller companies like AI startups might use data centres in Nordic countries to process their massive data sets and run their predictive algorithms, the results of which are then transferred to clients' servers in the UK. Finally, a boutique UK retailer selling to customers in the EU might have to transfer customer data from a website hosted in Belgium to servers in the UK in order to process sales.

How could Brexit affect cross-border data flows?

This paper addresses data flows between the EU and the UK, focusing on the economic sphere. Data flows in the realm of national security and law enforcement are a separate matter, as are non-personal data flows.

Data flows freely between the EU and the UK, and it has done since the emergence of the modern internet and digital economy. The free flow of data within the EU is enabled by harmonised data protection rules and common systems of regulatory enforcement. EU Member States also have shared arrangements for data flows with non-EU (i.e. third) countries.

75% of the UK's international data flows are with the EU, and much UK economic activity is dependent on these flows.[7] For example, 46% of UK exports are to the EU, and services account for 40% of these exports.[8] Given that data has always flowed freely, it is difficult to predict the impact of disruption to EU-UK data flows. But disruption would place immense compliance burdens on individual organisations, which would have to invest in legal and administrative fees to ensure EU-UK data transfers remained lawful. Increasing the cost of business slows the growth of many organisations and undermines innovation. Over the long term, it could also lead to the UK being less attractive to investors and thus generate negative knock-on effects for the economy at large.

There has been intense political focus on the issue of trade in goods, particularly as regard the border with Ireland. By comparison, issues relating to data flows and trade in services more broadly have been neglected. Yet they may be as important for the economy, especially in future. In the same way that disruption to trade in goods, in the form of border checks and delays at ports necessitated by divergent regulatory regimes, could have damaging knock-on effects for the UK economy, compliance costs and reduced investment caused by disruption to EU-UK data flows would do too.

In the following, the paper outlines the EU's legal and policy approach to data protection, giving an overview of the GDPR and the EU data governance framework. It then gives an overview of EU-third country data relationships, including the EEA, adequacy decisions, partial adequacy and countries with no formal arrangement. Finally, it places the post-Brexit UK in this context, assessing whether or not the UK is likely to get an EU adequacy decision, and what it means for the economy if it does not.

2 House of Commons Library, 'Services industries: Key Economic Indicators' (09/08/2019).
3 House of Commons Exiting the European Union Committee, 'The progress of the UK's negotiations on EU withdrawal: Data' (2018), p. 7.
4 techUK and Frontier Economics, 'The UK Digital Sectors After Brexit' (2017).
5 *Ibid*, p. 6.
6 Mckinsey Global Institute, 'Digital Globalization: The New Era of Global Flows' (2016), p. 12.
7 techUK and Frontier Economics, 'The UK Digital Sectors After Brexit' (2017), p. 10.
8 House of Commons Library, 'Statistics on UK-EU trade' (24/07/2019).

2. EU Data Protection Landscape

What is the EU's approach towards data protection?

All data protection policies need to strike a balance between privacy, economic activities (e.g. innovation) and security. By international standards, the EU is tilted towards privacy as its legal framework embodies high levels of data protection. Also, EU citizens increasingly value privacy, which is reflected in the EU's policy approach.

The protection of data is a fundamental right in the EU's constitutional system. The EU's Charter of Fundamental Rights (the Charter), which has the status of an EU Treaty, has Articles relating to the respect for private life (Article 7) and the protection of personal data (Article 8).[9] This means that the right of EU citizens to privacy and protection of personal data are enshrined not only in law, but in its constitutional order, and are equivalent to other fundamental rights, like the right to liberty and freedom of thought. The fundamental right to protection of data has been vigorously upheld by the CJEU.

What is the GDPR?

The GDPR is the EU's landmark legislation on the protection of personal data. It came into effect on 25 May 2018, and was first proposed by the European Commission in 2012.[10] The GDPR represented an updating – and strengthening – of the previous legislation (the 1995 Data Protection Directive.)[11] As a regulation, the GDPR (and its derogations) has direct effect and is automatically applied across all EU Member States, who have drafted their own laws to implement GDPR.

The GDPR governs the processing and use of personal data in the commercial and civil realm, but not in the realm of national security and law enforcement (there is a separate law enforcement Directive).[12] GDPR has a broader and more dynamic definition of personal data than the 1995 Directive. It creates additional responsibilities and places a greater emphasis on accountability for organisations (i.e. data processors/controllers). It also gives individuals (i.e. data subjects) more rights. For example, organisations can only process personal data if they have a legal basis for doing so, such as the consent of data subjects, as a public task or if there exists a 'vital interest'. Also, data subjects have increased rights to access their data, have it transferred, and have it erased.

A new feature of the GDPR is that it has extraterritorial applicability, meaning that it applies to non-EU organisations which handle EU citizens' data. This includes every major internet company which EU citizens use, and many more organisations. There are significant financial penalties for GDPR non-compliance. The maximum fine is €20m or 4% of an organisation's annual global revenue. The biggest fine so far is £183.39m, given to British Airways by the UK's ICO.[13] Additionally, GDPR encourages the development of codes of conduct and achieving data protection certification from accredited, independent expert organisations for greater compliance assurance and accountability.

It is too early to judge the success of the GDPR, as this will depend on how it is enforced, as well as its overall impact on privacy, organisational culture and consumer trust. However, its adoption was a major achievement of the EU's political system. Nearly 4,000 amendments were laid, and it took four years of negotiation.

What is the EU data governance framework?

The GDPR created a new system of data governance in Europe. The European Data Protection Board (EDPB) is a powerful new body which consists of the heads of each Member State data protection authority (DPA). It is currently chaired by Austrian Information Commissioner Andrea Jelinek. The role of the EDPB is to foster cooperation between the DPAs through a 'consistency mechanism', which ensures that they collaborate on cases which cut across multiple jurisdictions. If the DPAs cannot come to agreement, the EDPB issues binding decisions which must be followed. As a quasi-judicial body, the EDPB plays a pivotal role in interpreting and enforcing the GDPR. Its predecessor, the Article 29 Working Party, was an advisory body without legal force.

The EDPB, and the national DPAs, are the most important actors in the new EU data governance framework, as they interpret, enforce and therefore shape the new data protection regime. DPAs will investigate and rule on all GDPR-related cases, via the EDPB if they are international in nature. As the ultimate arbiter of EU law, the CJEU is also a key player, and is expected to rule on many GDPR-related cases which are referred to the courts. The European Commission's Directorate-General for Justice and Consumers (DG JUST) is also powerful, as it is responsible for international data flows and monitors Member State data protection legislation and GDPR implementation. The European Data Protection Supervisor (EDPS) provides secretariat to the EDPB, and it is the DPA of the EU institutions. Now that the GDPR has been passed, the role of the European Council, the Council and the European Parliament is minimal.

The GDPR applies to all EEA countries (Iceland, Liechtenstein and Norway), which are also members of the EDPB, albeit without voting rights. The European Commission is also a member without voting rights.

The GDPR also created the 'One-Stop-Shop'. This new system ensures that organisations processing data from citizens' in multiple Member States are only regulated by one DPA, meaning they can only be fined for GDPR non-compliance in one EU jurisdiction and only need to liaise with one DPA.

Not all DPAs are equal. Some are much more influential and important than others, due to divergent levels of staffing, resources and expertise. The UK, France, Germany, Ireland and Spain are widely recognised as the key players.

9 Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union.
10 Regulation (EU) 2016/679 (General Data Protection Regulation)
11 DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
12 DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
13 ICO, 'Intention to fine British Airways £183.39m under GDPR for data breach' (08/07/2019).

What is the global impact of GDPR?

The EU may not be a traditional superpower with military might, but it is an economic and regulatory superpower. The 'Brussels Effect' is a phenomenon of upward regulatory convergence, whereby non-EU companies conform with EU regulatory standards as it is in their commercial interest to do so.[14] This is because it facilitates market access and trade with the EU. As the EU's market of 500 million consumers is so large, and the EU enforces its regulations in such a robust way, it is often more beneficial for non-EU companies to follow stringent EU regulatory standards than more lax local standards. In this sense, the EU is a 'regulatory hegemon', on par with the US and China, due to the 'extensive externalization of its standards worldwide'.[15]

The GDPR is a classic example of the Brussels Effect in action, as it is an EU regulation with truly global reach. Because any organisation which processes EU citizens' data has to be GDPR compliant, many non-EU firms follow the GDPR. It is impractical for companies to implement different data protection standards for their EU and non-EU customers, so they opt to follow GDPR globally. Furthermore, many data protection laws around the world are strongly influenced by the EU's approach, which is often seen as the 'gold standard'.[16] Several countries are expected to model future data protection laws on the GDPR, rather than reinventing the wheel. As such, the GDPR is raising data protection standards and inspiring legislation worldwide.[17]

3. EU-Third Country Data Flows

How does data flow between the EU and third countries?

Data flows freely within the EEA. By virtue of the EEA Agreement, Iceland, Liechtenstein and Norway follow the GDPR and benefit from unrestricted data flows with the EU. This means that entities in any EEA country can transfer data to other entities across the EEA without restriction. This is vital for businesses across Europe, and makes it easier for companies to trade, access new markets, operate in multiple countries and serve customers internationally.

The free flow of data within the EEA is enabled by a shared legal framework (i.e. the GDPR) and a common system of enforcement (i.e. the EDPB and the CJEU). As third countries have different legal systems, there is a stringent system in place whereby entities in the EEA can only transfer data to entities in third countries if certain requirements are met. One such requirement is an adequacy decision.

What is an adequacy decision?

An adequacy decision is the EU's way of 'protecting the rights of EU citizens by insisting upon a high standard of data protection in foreign countries where their data will be processed'.[18] The European Commission's DG JUST assesses the data protection landscape in third countries. If it is satisfied that the protection of data is sufficiently robust, it issues an adequacy decision, which has legal status.

Once an adequacy decision is in place, data can be freely transferred from the EEA to that third country, as if it was in the EEA. This is economically beneficial as it significantly lowers transaction costs for companies, opening up new business and trade opportunities. Given the high standards of data protection in the EU, not many countries are recognised as ensuring an 'adequate level of protection'.

There are adequacy decisions for thirteen countries: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Mann, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA. As will be explained below, Canada and the USA have partial adequacy decisions.[19] Talks are currently ongoing with South Korea, as part of the EU's strategy to engage with East and South-East Asia on data protection.[20]

The criteria for how adequacy decisions are made is outlined in the GDPR and corresponding CJEU case law. The European Commission assesses the data protection laws in the third country and the way in which those laws are enforced. It also looks at wider factors such as the country's judicial system, the rule of law and its national security policies. The overall system for data protection must be deemed 'essentially equivalent' to the EU's for a positive decision to be made. Adequacy decisions are living, breathing documents. Once an adequacy decision is

14 Anu Bradford, 'The Brussels Effect' (2012) *Northwestern University Law Review,* p. 7.
15 *Ibid*, p. 42.
16 Graham Greenleaf, 'Global data privacy laws 2015: 109 countries, with European laws now in a minority,' (2015) *Privacy Laws & Business International Report.*
17 Privacy International, 'Why and how GDPR applies to companies globally' (25/5/2018).
18 Graham Greenleaf, 'Questioning 'Adequacy' Part II – South Korea' (2018) *Privacy Laws & Business International Report*, p. 6.
19 European Commission, 'Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection' (2019).
20 European Commission, 'Exchanging and Protecting Personal Data in a Globalised World' (2017).

in place, it is periodically reviewed by the European Commission and it can be revoked at any time. It can also be invalidated by the CJEU. The European Commission has never revoked an adequacy decision following a review, but the CJEU has.

The adequacy process is unconventional. It has been described as a "two-way negotiation that leads to a one-sided decision by the Commission".[21] It is a process of 'gap bridging', where the EU tells the third country what it needs to do to get an adequacy decision. This typically involves demands to re-write its data protection laws, or reform its systems of enforcement, so that it more closely resembles the EU's. For example, the EU asked Japan to set up new enforcement and complaint handling mechanisms. The process, which is done 'in secret, behind closed doors' by the European Commission, has been criticised for lacking in transparency.[22]

The balance of power is usually with the EU in this process, as countries are keen to reap the economic benefits of unrestricted data flows, despite the fact that they become rule-takers. However, a positive decision does not require the third country to completely copy the EU's rules, and the two systems do not need to be identical.

Two of the thorniest issues in the adequacy process are enforcement and onward transfers. The EU cannot enforce its laws in other jurisdictions. If EU citizens' data is transferred from an EU entity to a non-EU entity, and that entity does not protect the data properly, the EU often relies on the third country's institutions to enforce the law. This is why the EU assesses the quality of a country's judicial system and regulatory institutions. Several EU officials we interviewed described enforcement as a major challenge of the adequacy process.[23] On onward transfers, once EU citizens' data has been transferred to an entity in an non-EU country, it might then be transferred again by that entity to another entity in a country which is not deemed adequate by the EU. Because of this, adequacy decisions contain strict rules relating to onward transfers, so that EU citizens' data is protected as it travels.

What if there is no adequacy decision?

An adequacy decision means the entire country is deemed adequate, and data can be freely transferred from the EEA to any entity in that third country. If there is no adequacy decision in place, data can still flow from entities in the EEA to entities in third countries. However, they cannot flow to any entity, and additional measures -- safeguards of a legal and administrative nature -- must be put in place by individual organisations to facilitate lawful data transfers.

The two main measures are Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). SCCs are template contracts, pre-approved by the European Commission, which must be signed by both entities engaging in an EEA-third country data transfer. Once the contract is in place, data can flow freely, as the entity in the third country has legally committed to a level of data protection which meets EU standards.

BCRs are a legal mechanism, requiring approval from the relevant EU DPA, to facilitate data transfers within a company or group of companies. Once in place, they require the entire organisation or group to adhere to EU-approved data protection standards. They are almost exclusively used by large multinational corporations operating in multiple jurisdictions.

SCCs and BCRs are relatively costly and burdensome for organisations to set up, as they require significant administrative and legal work. Also, SCCs and BCRs cover individual organisations, whereas an adequacy decision covers the entire economy. As such, it is far better for business if there is an adequacy decision, so that no additional compliance obligations are necessary. Nonetheless, the vast majority of countries are not recognised as 'adequate' by the EU, and data transfers between the EU and the rest of the world still occur. They are simply more difficult.

When choosing which countries to assess for adequacy, the Commission considers the commercial relations and extent of data flows with the third country, as well as the overall political relationship. Its current focus is on East and South-East Asia, and future plans relate to South America. The EU is open about its strategy to 'encourage convergence of legal systems' around the world, and it uses the adequacy process to encourage upward convergence towards its own data protection standards.[24]

What about the US and Canada?

The US and Canada have partial adequacy decisions, which means that only parts of their economy are recognised as offering an adequate level of data protection. Canada's adequacy decision is much broader than the US's, as it applies to all private companies processing data for commercial reasons.

The EU-US data relationship is a different beast and has been notably rocky. The EU-US Safe Harbour Principles were the result of an adequacy decision made by the European Commission in 2000, which enabled the free flow of data between EU and US companies. In October 2015, following a case brought to the CJEU by Austrian privacy activist Max Schrems, Safe Harbour was invalidated by the Court. The CJEU argued that when making the Safe Harbour decision, the Commission did not properly evaluate the data protection landscape in the US, as it neglected the mass surveillance undertaken by intelligence agencies for national security purposes.[25] This mass surveillance was revealed by National Security Agency (NSA) whistleblower Edward Snowden, and prompted the Schrems case. Schrems argued that his Facebook data was not protected when it was transferred to the US, as the Snowden files revealed that this data was routinely passed from Facebook to the NSA.

After the Schrems case, there was a period of uncertainty where it was unclear whether EU-US data flows could continue. A halt to data flows and ensuing economic disruption was a real prospect. In July 2016, the EU-US Privacy Shield – an updated and more robust adequacy decision – was approved by the European Commission.[26] Regulators were pragmatic and allowed a transitional period in the intervening months, so the economic disruption was minimal.

21 Interview with European data protection regulator.
22 'Graham Greenleaf, 'Questioning 'Adequacy' Part I – Japan' (2017) *Privacy Laws & Business International Report*, p. 2.
23 Various interviews with EU data protection officials and regulators.
24 European Commission, 'Exchanging and Protecting Personal Data in a Globalised World' (2017).
25 Judgement of the Court (Grand Chamber), 'Maximilian Schrems v Data Protection Commissioner' (06/10/2015).
26 EU-US Privacy Shield

Unlike other adequacy decisions, Privacy Shield only covers companies which sign up to it (just under 5000), as opposed to the whole US economy. With the help of the US Department of Commerce, those certified companies then apply higher data protection standards than US law requires. Privacy Shield is reviewed annually by the European Commission, which views it favourably. However, like Safe Harbour was, it is currently being challenged and reviewed in the CJEU. It is plausible that it will be invalidated in the coming months, throwing the entire EU-US data flows system into disarray.

EU-third country data relationships

	EEA Norway, Iceland, Liechtenstein	**ADEQUACY DECISION** Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Mann, Japan, Jersey, New Zealand, Switzerland and Uruguay	**PARTIAL ADEQUACY** USA and Canada	**NO FORMAL ARRANGEMENT** Rest of the world
EU-THIRD COUNTRY DATA FLOWS	Completely unrestricted	Completely unrestricted	Unrestricted for certified organisations and/or sectors	Unlawful unless organisations set up alternative legal arrangements
ECONOMY	Economies heavily integrated, full participation in the Single Market	Data flows facilitate trade and economic integration	Data flows facilitate trade and economic integration in some sectors	Trade and economic integration impeded
BUSINESSES	Don't need to do anything to transfer data	Don't need to do anything to transfer data	Certified US businesses need to adopt Privacy Shield standards	Heavy legal and compliance burden on businesses
REGULATORY COOPERATION	Members of EDPB without voting rights and part of One-Stop-Shop	Not in EDPB or One-Stop-Shop	Not in EDPB or One-Stop-Shop	Not in EDPB or One-Stop-Shop
SOVEREIGNTY	Rule-takers, follow GDPR entirely	Rule-takers, adopt similar data protection framework to EU	More scope for independent rule-making	More scope for independent rule-making
LONGEVITY	Permanent arrangement	Permanent but reviewed periodically and can be revoked	Permanent but reviewed periodically and can be revoked	EU currently assessing South Korea, focused on East and South-East Asia

4. Brexit, No-Deal and EU-UK Data Flows

What is the current situation?

Data flows freely between the EU and the UK. It is one of the many ways in which the two economies are deeply integrated. As the UK joining the EU long predates the digital economy and the modern internet, data has always flowed freely across the Channel. The UK has followed EU data protection law since the 1995 Data Protection Directive, when the internet was in its infancy. Common legal frameworks have enabled the free flow of data since then.

Post-Brexit, the UK will become a third country in EU law. The previous section highlighted several available models for EU-third country data relationships, such as the EEA, adequacy, partial adequacy and ad hoc legal arrangements.

Thus far, the question of data flows has received minimal attention in the Brexit debate, and has barely been discussed at political level in the Brexit negotiations. The European Commission team conducting the negotiations, TF50, considered it an issue for the future relationship. The EU plans to negotiate the future EU-UK relationship in the transitional period, which will commence if and when the Withdrawal Agreement is ratified. The transitional period ends on 31 December 2020, but it can be extended once for one or two years. The longer the Brexit impasse continues and the longer it takes for the Withdrawal Agreement to be ratified, the shorter the transitional period will be.

The Political Declaration, which accompanies the Withdrawal Agreement, is a non-binding document outlining EU-UK aspirations on the future relationship. The section on data protection gives an indication of what has been discussed so far, and it is not very detailed. However, it does state that the European Commission will assess the UK with a view to making a potential adequacy decision by the end of the transitional period. A positive adequacy decision is not guaranteed.

B. Data protection

8. In view of the importance of data flows and exchanges across the future relationship, the Parties are committed to ensuring a high level of personal data protection to facilitate such flows between them.

9. The Union's data protection rules provide for a framework allowing the European Commission to recognise a third country's data protection standards as providing an adequate level of protection, thereby facilitating transfers of personal data to that third country. On the basis of this framework, the European Commission will start the assessments with respect to the United Kingdom as soon as possible after the United Kingdom's withdrawal, endeavouring to adopt decisions by the end of 2020, if the applicable conditions are met. Noting that the United Kingdom will be establishing its own international transfer regime, the United Kingdom will in the same timeframe take steps to ensure the comparable facilitation of transfers of personal data to the Union, if the applicable conditions are met. The future relationship will not affect the Parties' autonomy over their respective personal data protection rules.

10. In this context, the Parties should also make arrangements for appropriate cooperation between regulators.

Taken from '*Political Declaration Setting Out the Framework for the Future Relationship Between the EU and the UK*' (2018)

What is the UK's position?

The UK government's position on this issue has been outlined in official speeches, position papers and technical notes published by Theresa May's administration. Boris Johnson's government has not said or published anything substantive on this topic as yet, but is ostensibly more comfortable with a no-deal Brexit than the previous administration.

The UK wants the free and unhindered flow of data between the EU and the UK to continue, as it believes it is crucial for the economy. Although an adequacy decision would enable this, the UK has argued that the adequacy approach 'would not reflect the breadth and depth of the UK-EU relationship'.[27] It has called for something more bespoke than adequacy. A UK government official argued that "adequacy agreements are for third countries, with all due respect, like Uruguay and Argentina, which are outside of the EU framework. The difference is that we have fully implemented GDPR while Uruguay hasn't."[28]

Instead of adequacy, the UK has called for a 'legally binding' EU-UK data agreement.[29] This bilateral treaty would encompass mutual recognition of data protection standards and would have status in international law. It also wants 'a continued role' for the ICO in the EDPB (preferably membership), as well as UK participation in the One-Stop-Shop, which would be good for UK businesses.[30]

In short, the UK has asked for more than what any other third country has. A bilateral treaty differs from an adequacy decision because a decision can be revoked by the Commission or invalidated by the CJEU at any time. This would leave large sections of the UK economy in a precarious position. However, the Commission would be unable to revoke a treaty once ratified, and it would be harder for the CJEU to invalidate it, rendering it a more stable arrangement for the UK. The UK argues that this stability would be beneficial for both sides.

On regulatory cooperation, the UK wants the ICO to retain membership of the EDPB. Because of the power and influence of the EDPB in interpreting and enforcing the GDPR, the UK is reluctant to lose its seat at the table. However, no third country DPAs are full EDPB members. The EEA DPAs are EDPB members, but without voting rights. This is presumably what the UK seeks. The UK's justification for this request is that it would be invaluable for the EDPB to retain the expertise and resources of the ICO, which is indisputably one of the most well-resourced and effective European DPAs.

Finally, no countries outside the EEA benefit from the One-Stop-Shop mechanism, which allows businesses to only be regulated by one EU DPA. The UK is reluctant for its businesses to be regulated, and potentially fined, by EU DPAs and the UK's ICO. Put simply, the One-Stop-Shop would prevent UK companies from receiving multiple fines for the same data breach.

The UK intends to recognise the EU's data protection system as adequate, even in a no-deal scenario, which means that Brexit should not affect UK to EEA data flows.[31]

27 HM Government 'Framework for the UK-EU partnership: Data protection' (2018), p. 15.
28 Interview with UK government official.
29 HM Government, 'Technical Note: Benefits of a new data protection agreement' (2018), p. 1.
30 *Ibid*, p. 2.
31 HM Government, 'Using personal data in your business or organisation if there's no Brexit deal' (2019).

What is the EU's position?

The EU's position is that, post-Brexit, the UK should be treated as any other third country. This means that the preferred option is an adequacy decision, which can only be made by DG JUST. When asked about a potential bilateral treaty, several EU officials remarked that adequacy is the only game in town for the UK.[32] Without an adequacy decision, organisations will have to rely on ad hoc legal mechanisms to facilitate lawful EEA to UK data transfers.

As previously discussed, adequacy decisions do not result from conventional negotiations, hence the term 'decision'. Also, the EU does not negotiate adequacy like it does trade, because it does not negotiate fundamental rights like privacy and data protection as if they were commodities. This is why it rejects the idea of a mutual recognition agreement in the form of a bilateral treaty. It also wants to retain the flexibility to revoke any adequacy decision, especially if the UK's data protection laws or practices change and diverge from EU standards. It is highly unlikely that the EU will compromise on fundamental rights to do the UK a favour. [33]

EU Chief Negotiator Michel Barnier also rejected the idea of ICO membership of the EDPB and UK participation in the One-Stop-Shop. He argued that the former would undermine the 'autonomy of EU decision-making', which has been a core principle of the EU's Brexit position. This is because such an arrangement would mean that the ICO, and by extension the UK, would continue to influence the EU's regulatory and enforcement framework via the EDPB. This would be especially problematic during any adequacy process, as the EDPB issues a formal opinion on the adequacy of the third country.

Barnier said that decision-making can't be shared with a third country, and that the EU 'can't change how it works' to accommodate the UK.[34] It is possible, however, that the UK could negotiate observer status (i.e. no voting rights) for the ICO in the EDPB. Several EU officials we interviewed agreed that the ICO is highly respected and that they want to continue working with it. One argued that the ICO plays "an extremely important role in the EDPB, and it would be good if it could continue to participate in some capacity".[35]

The Political Declaration suggests that, so far, the EU's position is prevailing. This is because it states the future data relationship will be based upon the EU's existing adequacy framework, with no mention of mutual recognition or a new UK-EU data treaty.

The UK and EU positions on data protection, and the gulf between them, are emblematic of wider Brexit dynamics. The UK wants to retain its seat at the table and negotiate a bespoke and favourable model, whereas the EU is unwilling to deviate from what is outlined in EU law today. The UK government's technical note even has a section titled '*Why the UK should be treated differently*', where it outlines why pre-existing EU-third country models will not work.[36] The EU is unwilling to countenance the idea of differential, special treatment for a country on its way out of the EU, as it wants to maintain the integrity of its legal system and not set new precedents or disrupt relations with other third countries. It is difficult to see the EU budging on this.

Will the UK even get an adequacy decision?

There is no guarantee that a positive adequacy decision will be forthcoming, only that the Commission will conduct the process of assessment with haste. It is possible that the Commission will assess the UK's data protection framework and conclude that it does not offer an 'adequate level of protection'.

There are various reasons why the UK might not get an adequacy decision from the EU, or if it does, that it might be invalidated by the CJEU. Numerous scholars have argued that the UK's prospects are rather bleak.[37] Also, nearly everyone we interviewed mentioned that the UK is worried about not getting an adequacy decision, which helps to explain its desire for a bilateral treaty instead.

From the UK's perspective, a positive adequacy decision from the EU should not be an issue. The Data Protection Act 2018 is the UK legislation which implements the GDPR.[38] The UK government has committed to maintaining high levels of data protection and alignment with EU standards post-Brexit, and the Data Protection Act indicates that this is likely to be the case.

As UK data protection laws will thus offer a level of protection which is 'essentially equivalent' to the EU's, there should be sufficient grounds for an adequacy decision, so the argument goes. Furthermore, the UK's legal system and regulatory enforcement is robust and trusted. The ICO is one of the most respected DPAs in the EU, so the Commission are unlikely to doubt its independence or capacity to enforce the UK's data protection laws.

However, even if the UK's data protection laws align with the EU's, and its legal and regulatory system continues to robustly enforce those laws, the Commission might still have doubts as to whether EU citizens' data would be sufficiently protected when it is transferred to the UK. This is because the Commission will not just look at data protection laws and institutions. It will also consider the UK's national security policies and corresponding legislation and practices, as well as its approach to human rights.

In the 2015 Schrems case, the CJEU invalidated Safe Harbour, arguing that the Commission overlooked relevant national security policies and mass surveillance practices carried out by US intelligence agencies.[39] Post-Schrems, the Commission is legally required to evaluate the broader context of data protection in the third country when making adequacy decisions. This means that UK's national security framework, including relevant domestic legislation, will be under the microscope.

As one analyst writes, 'post-Snowden, it is widely believed that GCHQ participates in mass surveillance that is as widespread and as indiscriminate as that in the US, and moreover that GCHQ freely shares this intelligence with the Americans.'[40] Absurdly, whilst in the EU, this is not as much of a problem, as EU Member

32 Various interviews with EU data protection officials.
33 Interview with academic specialising in data protection and EU adequacy.
34 http://europa.eu/rapid/press-release_SPEECH-18-3962_en.htm
35 Interview with European data protection regulator.
36 HM Government, 'Technical Note: Benefits of a new data protection agreement' (2018), p. 3.
37 See Andrew Murray, 'Data transfers between the EU and UK post Brexit' (2017) *International Data Privacy Law.*
38 Data Protection Act 2018
39 Judgement of the Court (Grand Chamber), 'Maximilian Schrems v Data Protection Commissioner' (06/10/2015).
40 J Scott Marcus and Georgios Petropoulos, 'Brexit and its potential impact on international data transfers' (2016) *Bruegel.*

States can pursue independent national security policies, which are not EU competences. However, those same policies could become a problem (for data flows) when the UK becomes a third country.

Schrems is not the only relevant CJEU case law. In 2014, following a landmark case brought by privacy campaign group Digital Rights Ireland, the CJEU ruled that the EU Data Retention Directive 2006 was incompatible with EU law, and it was repealed as a result.[41] The Directive required internet service providers to indiscriminately collect and retain subscriber's personal data. The CJEU ruled that this was incompatible with the right to data protection in Article 8 of the Charter, arguing that such indiscriminate surveillance and retention of data was disproportionate and required additional safeguards.

In a subsequent case in 2016, brought by Labour MP Tom Watson, the CJEU ruled that the UK's Data Retention and Investigatory Powers Act 2014 (DRIPA) was incompatible with EU law, as it was in breach of Articles 7 and 8 of the Charter. In its judgement, the CJEU argued that the general and indiscriminate retention of personal data, without exception, was disproportionate, and that more precise rules and safeguards had to be implemented.[42] DRIPA has since been repealed and replaced with the Investigatory Powers Act 2016 (IPA). In July 2019 the UK High Court ruled that the IPA did not breach the European Convention on Human Rights (which is distinct from EU law).[43]

The case law and legal precedents which emerged from these judgements do not bode well for the UK in its quest for a positive adequacy decision. The main problem areas which undermine the prospects of a positive adequacy decision are outlined below (although this list is non-exhaustive).

a) Investigatory Powers Act 2016

The European Commission will need to assess whether the IPA is compatible with EU law and the Charter. It will take note of the way in which the CJEU has interpreted compatibility of surveillance laws and the fundamental rights to privacy and data protection in previous cases. Those cases have set the bar fairly high, so it is plausible that the Commission will decide that the IPA is not compatible with EU law, despite the recent High Court judgement. Even if the Commission does grant the UK an adequacy decision, the IPA and associated practices could provide grounds for it to be invalidated by the CJEU.

Commission officials will be concerned about what happens to EU citizens' data once it is transferred to entities in the UK. Part four of the IPA entails indiscriminate collection and retention of personal data which actually goes beyond DRIPA, encompassing 'wider and more intrusive powers' than before; therein lies the problem.[44] In April 2018, the UK's High Court ruled that the IPA was incompatible with the EU Charter, giving the government six months to amend it.[45] The law was then amended to define a 'serious crime' as one with a minimum 12-month sentence, and additional oversight judicial oversight mechanisms were added.

It remains to be seen whether the reforms will be sufficient for EU adequacy.

b) Five Eyes alliance

The Five Eyes alliance is an intelligence sharing arrangement between Australia, Canada, New Zealand, the UK and the US. Several interviewees noted that Five Eyes could be a problem, with one positing that "all of the Five Eyes countries should be worried about possible legal challenges".[46] Given that some of these countries are not deemed adequate by the EU, the Commission will worry that EU citizens' data could be transferred to third countries, via the UK security services, where it may not be sufficiently protected.

c) Not retaining the Charter of Fundamental Rights

The EU (Withdrawal) Act 2018 transposes all EU law into UK law post-Brexit, to ensure legislative continuity. Controversially, the EU's Charter of Fundamental Rights is not retained. As such, the right to data protection will no longer be a fundamental right for UK citizens, upheld by UK courts. Moreover, the whole system for human rights in the UK will change, as all rights will depend on – and could be taken away by – Parliament, free from the constraints of the EU Charter.[47] However, the UK will remain a signatory to the European Convention on Human Rights post-Brexit, although Conservative politicians have flirted with the notion of withdrawing.[48]

There is an important difference between an Act of Parliament, which can be repealed, and fundamental rights upheld by the Charter, which has EU treaty status.[49] In sum, there will be no fundamental right to data protection in the UK post-Brexit, and the Commission might take a dim view of this in their adequacy assessment.

d) Onward transfers

The Commission will be concerned as to whether EU citizens' data transferred to the UK can then be transferred to a third jurisdiction where it may not be sufficiently protected, as shown by the Five Eyes concern. Post-Brexit, the UK will be free to decide which countries it deems adequate, and what arrangements it has with those countries. If the UK deemed countries adequate which the EU did not, this could undermine prospects for a positive UK adequacy decision.

The future UK-US relationship is significant, given the extent of data flows across the Atlantic. The US and UK governments have confirmed that, post-Brexit (deal or no-deal), Privacy Shield will continue to enable UK-US data flows, so long as certified US organisations update their public commitments.[50]

However, if this situation ever changes, and the UK-US data relationship becomes less stringent than Privacy Shield, or Privacy Shield is invalidated by the CJEU, the EU would worry about 'backdoor' transfers to the US via the UK, and its citizens' data not being sufficiently protected.

41 Judgement of the Court (Grand Chamber), 'In Joined Cases C-293/12 and C-594/12' (08/04/2014).
42 Judgement of the Court (Grand Chamber), 'Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others' (21/12/2016).
43 Natasha Lomas, 'UK High Court rejects human rights challenge to bulk snooping powers' (July 2019) *TechCrunch.*
44 Laurens Cerulus, 'UK's data flows under EU surveillance' (24/08/2017) *Politico.*
45 UK High Court Judgement (27/05/2018).
46 Interview with J Scott Marcus, Bruegel (June 2018).
47 Vernon Bogdanor, 'Beyond Brexit: Towards a British Constitution' (2019) *UCL Brexit Blog.*
48 Anushka Asthana and Rowena Mason, 'UK must leave European convention on human rights, says Theresa May' (25/04/2016) *The Guardian.*
49 Andrew Murray, 'Data transfers between the EU and UK post Brexit' (2017) *International Data Privacy Law.*
50 www.privacyshield.gov/article?id=Privacy-Shield-and-the-UK-FAQs

e) Immigration exemption in the Data Protection Act 2018

The Data Protection Act 2018 contains provisions exempting data subjects from various GDPR rights, such as the right to be informed and the right of access, if their personal data is processed by public bodies for immigration purposes. Several interviewees said that this exemption could undermine a positive UK adequacy decision, as it may not be compatible with the GDPR. There are exemptions in Article 23 of the GDPR, where the rights of data subject rights can be restricted, but there is no immigration exemption.[51] More broadly, it has been argued that the UK's 'minimal implementation' of the GDPR in domestic law could jeopardise an adequacy decision.[52]

—

It is impossible to predict whether the Commission will grant the UK an adequacy decision, and, if it does, whether it will be upheld by the CJEU. The problem areas outlined above will undoubtedly be considered by the Commission. One interviewee said that "if there were a new Schrems-style case assessing GCHQ instead of the NSA, the answer from the Court might well be the same".[53] Analysis of the Charter, the GDPR and relevant CJEU case law suggests that, unless the UK changes its surveillance laws and national security practices, it may not meet the threshold for adequacy.

However, the European Commission still found a way to grant the US a partial adequacy decision after Safe Harbour was struck down, and it will work on a new framework if Privacy Shield is invalidated, due to the importance of transatlantic data flows. Post-Brexit, perhaps realpolitik and economic considerations will prevail over rigid interpretation of EU law, like it did for the US when the reality of significant disruption to data flows became apparent. Whatever happens, the path to adequacy will be turbulent at best, and any future UK adequacy decision will be challenged in the courts, which would rule based on precedent.

The UK government has not acknowledged that this is an issue and has confidently asserted that an adequacy decision should be straightforward. The reality is more complicated.

What happens if there is no-deal on data flows?

There are several scenarios which render the UK without an adequacy decision.

Scenario 1) No Withdrawal Agreement: 'cliff edge' Brexit

The UK and EU might never ratify the Withdrawal Agreement, and Brexit could happen, without a transitional period, on 31 October 2019, or at a later date. This scenario would be the most disruptive and would only arise if EU-UK relations had irreparably fractured, or the UK was no longer willing to seek an orderly way forward. As of August 2019, this is looking increasingly likely, given Boris Johnson's firm commitment to leave on 31 October 2019, come what may.

No transitional period and a sudden shift to third country status would entail significant legal, economic, political and social disruption in the UK. The UK would immediately become a third country in EU law, and instant disruption to EU-UK data flows would ensue. The EU would not even begin assessing the UK for adequacy in this scenario, and there would certainly be no prospect of a positive adequacy decision in the foreseeable future, as the UK government has acknowledged.[54] As such, this is the worst outcome for data flows.

Scenario 2) Withdrawal Agreement but no adequacy decision

The UK and EU might ratify the Withdrawal Agreement, facilitating an orderly Brexit. At this point, the transitional period would begin. It lasts until 31 December 2020 and can be extended once for one or two years. During the transitional period, the UK continues to follow all EU law, and EU-UK cooperation continues unchanged, meaning that there is no disruption to EU-UK data flows.

The EU has committed to assessing the UK for adequacy during the transitional period, endeavouring to 'adopt a decision by the end of 2020'. This does not mean that the UK will get an adequacy decision by then, only that the EU will engage in the process.

It is possible that EU-UK relations could be amicable during the transitional period, with broad agreement on various issues, and the EU still fails to grant the UK an adequacy decision. This is because the EU will not negotiate adequacy as part of the trade talks, as it considers it a matter of fundamental rights. Therefore, it is possible that there could be an EU-UK Withdrawal Agreement, Trade Agreement and Future Partnership Agreement – but no adequacy decision. Although this is not no-deal for Brexit, it is no-deal for data flows (albeit at a later date).

Scenario 3) Adequacy decision but after the transitional period ends

Despite best intentions, there might be insufficient time for an adequacy assessment and decision during the transition. The length of time it takes for the EU to adopt an adequacy decision varies. The fastest was eighteen months, but the process can take up to five years.[55] As such, as soon as the transitional period starts, the clock starts ticking. The 'deadline' is 31 December 2020, but given that the transitional period can be extended, potentially up to December 2022, there might be more time.

Nonetheless, the EU might not be in a position to grant the UK an adequacy decision until after the transitional period, which means there could be a temporary period of disruption to EU-UK data flows, followed by an eventual adequacy decision. If it was clear that the Commission intended to grant an adequacy decision relatively soon, the regulators might show some flexibility and pragmatism, as they did after the invalidation of Safe Harbour. Even a positive UK adequacy decision could be revoked by the Commission or invalidated by the CJEU at any time.

51 Article 23 of the GDPR
52 Amberhawk Training, 'How UK's GDPR law might not be judged adequate' (16/03/2017) *The Register.*
53 Interview with J Scott Marcus, Bruegel (June 2018).
54 HM Government, 'Using personal data in your business or organisation if there's no Brexit deal' (2019).
55 Institute for Government, 'Explainer: Data Adequacy' (2018).

What happens if there is no UK adequacy decision?

Although no adequacy decision for the UK would not mean an end to EEA to UK data flows, these will be significantly disrupted and could be legally challenged. EEA to UK data flows are likely to decrease or increase at a slower rate than now. This will have a detrimental impact on the UK economy, especially over the mid- and long-term, as it increases transaction costs for businesses and renders the UK less attractive for inward investment.[56] This will be most damaging for the services and tech sectors, given the reliance on cross-border data flows. The impact will principally be on the UK, as UK-EEA data flows should remain unrestricted, as per the UK's no-deal policy.

It is difficult to quantify the cost of no adequacy decision to the UK economy, and the economic impact is unlikely to be felt immediately. It is also difficult to imagine what disruption to EU-UK data flows would mean, as data has always flowed freely between the two sides. An analogy with trade in goods might help. If the UK leaves the Customs Union and Single Market, it does not mean that goods cannot be traded across EU-UK borders, only that doing so becomes more burdensome, due to disruptions associated with new, legally-required border checks. In the same way that barriers to trade in goods, in the form of regulatory compliance and rules of origin checks and delays at ports necessitated by divergent regulatory regimes, could have damaging knock-on effects for the UK economy, compliance costs and reduced growth and investment caused by disruption to EU-UK data flows would do too.

The analogy with goods is imperfect. The main problem with data protection is flows from the EEA to the UK, whereas border checks on goods go both ways. Also, there will be no extra tariffs or taxes on data flows; increased costs come in the form of corresponding legal and compliance fees. Finally, the data flows themselves would not be slower, they would just require significant background work to be lawful. Despite these differences, the fundamental point stands true: disruption to data flows in the form of no adequacy decision means increased costs for businesses, which will negatively impact the UK economy. In this domain – and most others – Brexit means more red tape, not less.

No adequacy decision means that every EEA to UK data transfer would have to be covered by an alternative mechanism which rendered it lawful, and these mechanisms need to be set up by individual organisations. The EU has stated that the only option is for organisations to set up Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs).[57] This requires companies to direct immense costs and resources towards enabling (previously unrestricted) data transfers.

This will cause legal confusion and uncertainty, especially if the UK exits with no-deal. Immediately afterwards, due to the extra-territoriality of GDPR, UK firms could face large fines for unlawful EEA-UK data transfers, and it is likely many firms will not be ready. Many firms will not have set up the appropriate SCCs or BCRs in time or might be unaware that they must do so. It remains to be seen how flexible EU regulators will be, but the government has acknowledged the risk of enforcement action against UK companies.[58]

SCCs are extremely complex to set up, and a new contract is required for each point-to-point data transfer. Consider a large organisation with suppliers and customers across Europe. There might be thousands of different data transfers linked to the organisation's operations each day. These all need to be identified and mapped out, and SCCs need to be set up (and signed by both parties) for every transfer. Following the collapse of Safe Harbour, one large company had to put in place 2 million SCCs in one month, to ensure that their EEA to US data transfers remained lawful.[59] The legal fees and resources required to set up SCCs can be immense.

BCRs allow large organisations to adhere to a common set of data protection policies, legally binding on the entire entity at all times, which meet EU standards.[60] They are only available to organisations with operations in the EU, and are typically used by multinational companies to enable data transfers between subsidiaries or different business divisions. Business leaders report that BCRs require a 'daunting amount of effort to implement' and are 'wholly inaccessible to smaller companies'.[61] On average, they cost £250,000 to set up and the process can take several years.[62] Post-Brexit, existing BCRs approved by the UK's ICO would need to be resubmitted to the relevant EU DPA for approval.

Although many large companies will be well prepared and able to absorb the cost, it will be much harder for SMEs and startups. Many smaller organisations will not have the money, resources or expertise to deal with these new compliance burdens. As such, their business models and future growth could be undermined, and they could be at risk of large GDPR fines.

To further complicate matters, there is an ongoing court case which could threaten the validity of all SCCs. In what is known as 'Schrems II', the Irish High Court referred to the CJEU the question of whether SCCs are a valid tool for EEA to US data transfers. This is due to concerns that data transferred to the US (by Facebook) via SCCs is not sufficiently protected, as there is no legal remedy for citizens to access in case of illegal misuse of their data in the US.[63] If the CJEU does eventually rule that SCCs are invalid, this would be highly problematic for the UK if there was no adequacy decision, given that SCCs are the most used tool for international data transfers. This case highlights the importance of obtaining an adequacy decision, which is highly improbable in a no-deal scenario.

The UK's ICO has provided guidance on no-deal and what businesses of all size should do to prepare for this outcome:

- Data protection and no-deal Brexit for small businesses and organisations (ICO, 2019).
- Data protection if there's no Brexit deal (ICO, 2019).

The ICO has also developed a generator tool which helps organisations understand how to set up SCCs:

- Keep data flowing from the EEA to the UK – interactive tool (ICO, 2019).

56 techUK and Frontier Economics, 'The UK Digital Sectors After Brexit' (2017).
57 European Commission DG JUST, 'Notice to Stakeholders: Withdrawal of the United Kingdom from the Union and EU Rules in the field of Data Protection' (2018).
58 Sam Coates, 'UK faces potential 'consumer panic' and 'security gaps' under no-deal Brexit, says government document' (02/08/2019) *Sky News*.
59 Comments by Giles Derrington to Exiting the European Union Committee oral evidence session (09/05/2018).
60 techUK 'No Interruptions: Options for the Future UK EU data-sharing relationship' (2017).
61 Hunton & Williams and US Chamber of Commerce, 'Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity' (2014), p. 24.
62 HM Government, 'The exchange and protection of personal data: a future partnership paper' (2018), p. 12.
63 Alex Roure, 'Data Flows: What's Really at Stake in the Schrems II case' (15/07/2019) Disruptive Competition Project.

ADEQUACY vs. NO-DEAL

EU-UK data transfers remain unrestricted	EU-UK data transfers are heavily restricted
Companies don't need to do anything to keep transferring data	Companies need to set up new legal and contractual arrangements
Organisations will not be fined for EU-UK data transfers	Organisations could face large fines for EU-UK data transfers
UK economy unaffected – business as usual	UK economy damaged from disruption to data flows
Adequacy decision can be revoked at any time	Adequacy decision could, in theory, be issued in future
UK is a data protection rule-taker	UK could adopt a different data protection framework

What about taking back control?

Brexit has been presented as an opportunity for the UK to 'take back control' of legislative and regulatory powers, unshackled from EU interference. However, Brexit has always entailed an intractable trade-off between sovereignty and economic integration with the EU. If the UK seeks to break free from the EU's economic model and pursue divergent regulatory standards it can, but there will be economic costs in the form of reduced market access, trade and investment. If the UK aligns itself to the EU's regulatory standards, trade and economic cooperation could continue unhindered and grow, but the UK would be a rule-taker, with diminished sovereignty.

This trade-off is starkly highlighted in the domain of data protection. Not many people argue that the UK should diverge from EU data protection laws and pursue its own model. Indeed, the consensus among politicians and business is that the UK should continue to follow the GDPR, in part to enable the continuation of unhindered EU-UK data flows. Many businesses would comply with the GDPR regardless, in order to process EU citizens' data. Having to comply with a separate UK regime would be costly and bad for business.[64]

Indeed, countries like Japan and South Korea accept becoming data protection rule-takers as the benefits of free data flows with the EU are so great, and the UK is no different. Furthermore, if the UK wants to retain a future adequacy decision, it will have to dynamically align with EU data protection laws as they change over time. The scope for UK data protection sovereignty is therefore minimal.

5. Conclusion

Cross-border data flows are vital for the functioning of the modern economy, especially for services sectors and technology industries. Disruption to EU-UK data flows, which could occur post-Brexit, would be damaging for the UK economy, and a novel situation, given that data has always flowed freely across the Channel. As the protection of data is a fundamental right, enshrined in EU law, the EU has stringent rules regarding EU-third country data transfers. Adequacy decisions enable free flow of data between the EU and third countries, but require approval from the European Commission, which holistically assesses whether the third country offers an adequate level of data protection.

Although the UK wants to go beyond adequacy for its data relationship with the EU, there is a risk that it might not even get a positive adequacy decision. Although the EU has agreed to assess the UK for adequacy during the transitional period, there are several reasons why the Commission might decide that the UK is not adequate. If there is no adequacy decision, or a no-deal Brexit, EU-UK data flows could still occur, they just require individual organisations to set up costly legal arrangements to facilitate them. No adequacy decision means more red tape for businesses, which could be absorbed by larger firms but will be a challenge for most others. It also puts firms at risk of large fines from EU regulators. Increased costs and decreased investment stemming from disruption to EU-UK data flows would negatively impact the UK economy, and has received minimal attention in the Brexit debate thus far.

Once it loses its seat at the EU table, the UK is likely to become a data protection rule-taker and no longer a rule-maker. With the EU setting the global gold standard, the scope for meaningful UK sovereignty in this domain is minimal.

64 Karen McCullagh, 'Brexit: potential trade and data implications for digital and 'fintech' industries' (2017) International Data Privacy Law.

Oliver Patel
Research Associate & Institute Manager
UCL European Institute
Email: oliver.patel@ucl.ac.uk
www.ucl.ac.uk/european-institute/people/oliver-patel

Oliver is an expert on the legal, political and constitutional aspects of the Brexit negotiations and withdrawal process. He is also an expert in EU data protection law and policy, cross-border data flows and EU-US Privacy Shield.

Dr Nathan Lea
Senior Research Associate
UCL Institute of Health Informatics
Email: n.lea@ucl.ac.uk
www.ucl.ac.uk/health-informatics/people/nathan-lea-0

Nathan's areas of expertise include information governance and regulatory oversight in healthcare and medical research. His research focus is on the role of information systems in supporting healthcare delivery and empowering patients. He is also an expert on GDPR.

Brexit Insights Series
UCL European Institute
16 Taviton Street
London WC1H 0BW
Email: european.institute@ucl.ac.uk
www.ucl.ac.uk/european-institute

The UCL European Institute is UCL's hub for research, collaboration and engagement on Europe. Our Brexit Insights series provides in depth, policy-focused analysis on technical aspects of Brexit and European policy.

UCL EUROPEAN INSTITUTE

BREXIT INSIGHTS

Design: davidlovelock.com