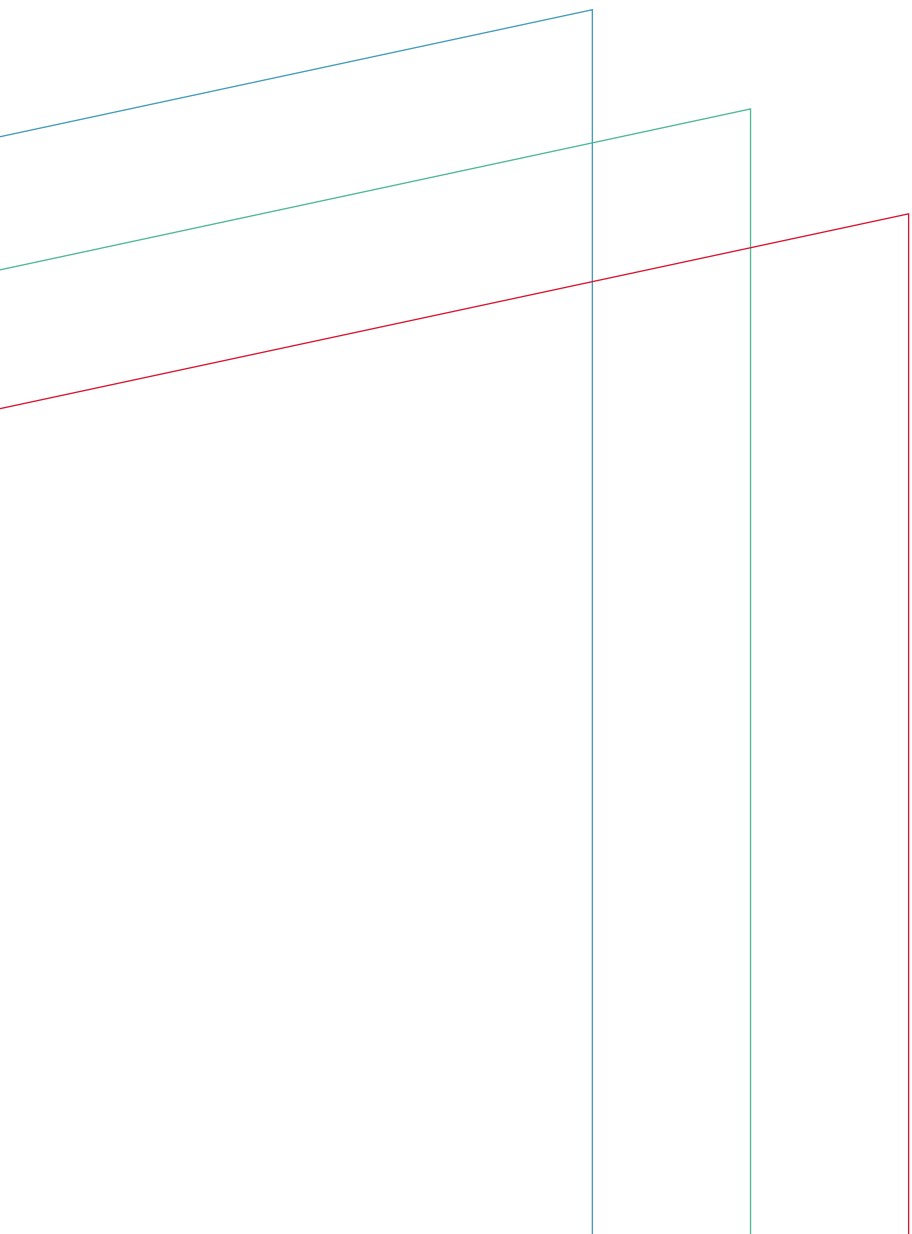
NEW ECONOMICS FOUNDATION

UCL EUROPEAN INSTITUTE

THE COST OF DATA INADEQUACY

THE ECONOMIC IMPACTS OF THE UK FAILING TO SECURE AN EU DATA ADEQUACY DECISION



CONTENTS

SUMMARY

Following the end of the Brexit transition period on 31 December 2020, the legal basis for transferring personal data across the Channel fundamentally changes. Unless the UK receives an adequacy decision from the EU, businesses and other organisations will no longer be able to freely transfer data from the EU to the UK, without putting in place their own additional measures. These measures can be costly, bureaucratic, and time-consuming to implement.

Although the UK has high standards of data protection via the Data Protection Act 2018, which enacted the General Data Protection Regulation (GDPR) in UK law, an EU adequacy decision is not guaranteed. Potential EU concerns with UK national security, surveillance and human rights frameworks, as well as a future trade deal with the US, render adequacy uncertain. Furthermore, EU-UK data flows are at the whim of the wider Brexit process and negotiations.

This landmark report outlines the economic cost and implications of the UK not receiving an adequacy decision from the EU. We look at the impact on businesses, different economic sectors, and the wider economy. We believe that this is the first comprehensive report analysing this issue from an economic perspective.

Through extensive interviews with over sixty legal professionals, data protection officers, business representatives, and academics, from both the UK and EU, we found that the risk of the UK failing to secure an adequacy decision is both real and serious, and that the impacts would be complex, leading to significant uncertainty.

New modelling prepared for this report estimates that the aggregate cost to UK firms of no adequacy decision would likely be between £1 billion and £1.6 billion. This extra cost stems from the additional compliance obligations – such as setting up standard contractual clauses (SCCs) – on companies that want to continue transferring data from the EU to the UK. We believe our modelling is a relatively conservative estimate as it is underpinned by moderate assumptions about the firm-level cost and number of companies affected. We estimate that the average compliance costs for a business that is affected would be:

- £3,000 for a micro business
- £10,000 for a small business
- £19,555 for a medium business
- £162,790 for a large business

This overall figure of between £1 billion and £1.6 billion represents money that companies would have been free to spend to meet the requirements of the business by, for instance, investing in new equipment, staff, or processes, but are now required to channel into compliance activities or additional costs for goods and services, due to EU-UK data flows disruption.

No adequacy decision would also have a range of other economic implications, including:

- Increased risk of GDPR fines, due to the new compliance requirements
- Reduction in EU-UK trade, especially digital trade
- Reduced investment (both domestic and international)
- Relocation of business functions, infrastructure, and personnel outside the UK

We explain in detail why no adequacy decision would have these implications and why they matter – but we do not model the wider macroeconomic cost. Further research is required on this. Indeed, there is very little research on the value of data flows and adequacy decisions in general. However, EU-UK data flows are a crucial enabler for thousands of businesses. These flows underpin core business operations and activities which add significant value. This is not just a digital tech sector issue – the whole economy relies on data flows.

The combination of a potential no-deal Brexit, coupled with the ongoing Covid-19 pandemic, means that business and the economy can ill afford more cost, complexity, and risk. Although the adequacy decision is in the hands of the European Commission, the UK government still has a large part to play.

All parties hope that the outcome of the last few years of Brexit negotiations will be a comprehensive partnership agreement. This will be an important achievement of huge social and economic significance. Without a wider agreement on the future relationship, adequacy will be very hard to attain.

RECOMMENDATIONS

To help mitigate future uncertainties around the economic effects of restrictions to data transfers, we propose that:

1. The government should make relevant data and modelling tools available to support empirical research on the social and economic impacts of data protection, digital trade, and the value of data flows, in order to improve the quality of public policy and democratic engagement in these areas.

2. The government should update its published 'Explanatory Framework for Adequacy Discussions' considering the issues raised by the *Schrems II* and *Privacy International* cases.

The UK government has expressed a commitment to maintain a world-class data protection system and remain broadly aligned with the EU's GDPR, while developing its own "pro-growth data rights regime", as explained in the National Data Strategy. To have the best chance of obtaining adequacy, the UK should consider demonstrating how it will maintain a regulatory level playing field with the EU on data protection, both domestically and in its trade agreements:

3. The government should further explain how the changes to the UK's data protection regime outlined in the National Data Strategy, designed to promote growth and innovation, will also strengthen and enhance the rights of UK and EU citizens.

4. The government should consider the impact of future trade agreements on data protection, and carefully review the trade-offs involved when liberalising cross-border data flows with different countries.

The UK government should also strengthen measures to support business if the UK fails to secure an adequacy decision. We recommend that the UK government should:

5. Continue to raise awareness of the risks and costs of a lack of adequacy within the business community, both inside the UK and in the EU.

6. Provide simple, practical tools, including information on additional safeguards, to enable UK organisations to continue to use SCCs, given the issues raised by *Schrems II*.

7. Set aside funds to ensure that struggling UK businesses, especially small and medium enterprises (SMEs), can afford to comply with the new requirements.

Our report concludes that no adequacy decision has the potential to be a contributing factor which undermines the competitiveness of key UK services and digital technology sectors, which have performed extremely strongly in recent years. Although we do not want to exaggerate the impacts – and no adequacy decision is far from economic armageddon – this outcome would not be ideal.

1. INTRODUCTION

This report looks at the economic impact of the UK failing to maintain the current regime for personal data flows with the EU. Data transfers are an integral part of doing business in the twenty-first century. People and businesses use data transfers across a wide range of services from file storage and hosting, which require interaction with data centres that remotely store personal data, to content publishing, where each person accessing the site triggers a data transfer, to using online tools such as e-mail or video conferencing.

The UK economy has developed, especially since the implementation of the General Data Protection Regulation (GDPR), the landmark EU legislation regulating the data economy, in an environment that did not impose any additional regulatory obstacle to moving data between the EU and the UK. This means that many UK companies have grown to rely on data being transferred to and from EU companies and data centres in order to carry out their business.

When the Brexit transition period ends on 31 December 2020, the legal basis for freely transferring personal data between the EU and the UK goes, too. While the UK government has said that transfers of data from the UK to the EU, or rather the European Economic Area (EEA), will not be restricted either through regulation or additional administration, such as the need to amend contracts, the EU has made no such commitment.[1]

The UK wants unrestricted EU-UK data transfers to continue. This would ideally be achieved via an EU adequacy decision, whereby the European Commission formally recognises the UK as providing the equivalent data protection regime for the personal data received from the EU as EU citizens would get in the EU itself.

It is tempting to think that because the UK passed the Data Protection Act in 2018 and has implemented the GDPR, that it would easily pass the adequacy test. Unfortunately, this is no guarantee of success. There are several factors contributing to this.

It has long been argued that the UK's legislative environment poses potential challenges, especially around national security and the mass surveillance regime, but also in relation to domestic data protection arrangements[2] and the UK's departure from the EU Charter of Fundamental Rights.

This is further complicated by a recent judgement by the Court of Justice of the European Union (CJEU) in the *Schrems II* case on the EU-US Privacy Shield, a partial EU adequacy decision which enabled unrestricted EU-US data transfers for certified companies. The mechanism was declared invalid under EU law, partly around concerns over the US surveillance regime. The court also elaborated on the basis by which the EU should make decisions about international data-sharing arrangements. The risks for the UK from this ruling are two-fold: similar principles used to invalidate Privacy Shield could be used to deny the UK adequacy, but also the more stringent conditions set out for transfers could complicate any alternative mechanisms.

The other new risk to adequacy comes from the UK's ongoing trade negotiations with the US, along with other third countries, especially those from the Five Eyes intelligence network,[3] to create a free flow of data regime between the two countries with lower regulations. This creates potential risks for the EU, as the UK could be perceived as a 'backdoor' for onward transfers of EU citizens' personal data to the US, which the CJEU has ruled does not meet the requirements for unrestricted personal data transfers.

In theory, adequacy is an administrative decision by the European Commission, independent of the new EU-UK trade and security agreement. But, in reality, it is also a political decision where the Commission could take some legal risks to maintain the status quo. Any breakdown in negotiations, or an acrimonious no-deal scenario, would not be conducive to the Commission granting an adequacy decision.

Readers who are familiar with the topic of adequacy decisions and the legal issues might wish to skip to Section 4 where we start to focus in on the economic analysis.

1.1 A NOTE ON METHODOLOGY

This report focuses on the economic impacts of data protection. While data protection is a fundamental right and privacy should not be traded like a commodity, keeping the legal and economic perspectives completely siloed hinders public debate. We see bombastic claims about the costs of protecting consumers or the 'value of data' go unchallenged because academia and civil society lack the tools to engage in these debates. At the same time genuine concerns about the economic impact of data protection regulation on certain sectors, such as small businesses, are ignored by privacy advocates unable to look outside the legal and policy prisms. Brexit and the growth of digital trade make this situation untenable.

This report presents original research in addition to our analysis of the legal and practical issues that arise from a lack of adequacy. We have carried out over sixty interviews with legal professionals, business representatives and policy makers to understand the risks and associated costs.

We have developed an economic model to quantify some of these impacts. There is limited methodological consensus and data available on these areas. As such we had to take the plunge and make assumptions and inferences, but at every step we have tried to be conservative and subtle. The figures presented in this report are an estimate based on the best available information. We have also looked at current approaches to measuring data flows and digital trade, available UK data, and other indicators of costs.

This model takes a partial and limited view at the impacts of a lack of an adequacy decision. More work is needed, and we modestly hope that this report will be a useful contribution to the field. We are looking forward to critiques and suggestions.

We understand that there is a parallel process for adequacy under the Law Enforcement Directive, which is very relevant in the context of the UK-EU security partnership; however, we do not consider it in this report.

2. EU-UK DATA TRANSFERS TODAY AND POST-BREXIT

The ability of UK companies to transfer data freely and without legal obstacles with EU companies is an important feature of EU membership and the digital single market. At the end of the transition period on 31 December 2020, the UK will become a third country, defined as any country outside of the EU, and businesses will no longer be able to rely on the existing regulatory regime to freely transfer data from the EU to the UK.

The UK government has already committed to not putting any new regulatory barriers or administrative burdens on data transfers from the UK to the EU. The EU, however, perceives the risks differently, because the UK government has publicly stated its desire to diverge from the GDPR[4] and also sign a free trade agreement (FTA) with the US, which could potentially commit the UK to unrestricted UK-US data transfers.[5]

Today, data transfers involve everything from search queries and social media posts to payroll information and health records. In fact, pretty much every company and all business operations involve some form of data transfer. As companies increasingly use cloud IT services, this further increases a company's reliance on data transfers.

2.1 HOW DOES DATA FLOW FROM THE EU TO A THIRD COUNTRY?

There are three main ways in which data could be legally transferred from the EU to the UK after the transition period, which we will discuss in turn.

1. The most desirable result, and the result that the UK government is actively seeking, is for the UK to receive a full adequacy decision, which would allow business as usual to continue.

2. Third countries without adequacy decisions can have data transferred from the EU provided that specific additional safeguards, such as contractual obligations, are set up by firms, that ensure the ongoing protection of the transferred data.

3. Even when there is neither an adequacy decision nor bespoke contractual provisions, Article 49 of the GDPR does allow for exceptional and strictly non-repetitive or systematic transfers to non-EU countries when certain criteria, like strong public interest, are met.

2.2 ADEQUACY DECISION

Organisations can transfer data freely from the EU to organisations in a third country if that country has an adequacy decision in place. An adequacy decision is the EU's way of 'protecting the rights of its citizens by insisting upon a high standard of data protection in foreign countries where their data is processed'.[6] For companies, an adequacy decision ensures that they do not have to comply with additional administrative and compliance requirements. The assessment of whether a third country meets the necessary standards of data protection is undertaken unilaterally by the European Commission's Department for Justice (DG JUST), following an Opinion from the European Data Protection Board (EDPB) and then member state approval in the Council. The only opportunity to challenge adequacy decisions is through the courts, as Max Schrems has done by challenging the legal basis on which Facebook was transferring his data from the EU to the US.[7, 8]

For the UK, an adequacy decision is the most economically beneficial because it maintains the status quo. In our interviews we were told repeatedly that adequacy is critical and that all other alternatives are problematic in comparison. An adequacy decision ensures that data transaction costs and barriers remain as low as possible while offering the opportunity of opening up new business and trade opportunities. Currently, only 12 countries have positive adequacy decisions from the EU: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay.[9] The US has been granted two partial adequacy decisions by the EU, both of which have been invalidated by the CJEU: Safe Harbour, which was invalidated in 2015, and Privacy Shield, invalidated in 2020.

2.3 DATA TRANSFERS WITHOUT ADEQUACY

Without a blanket decision covering all data transfers, as adequacy provides, organisations wishing to transfer data from the EU to the UK will be required to put additional safeguards in place. The two main measures are standard contractual clauses (SCCs) and Binding Corporate Rules (BCRs).

2.3.1 Standard contractual clauses

SCCs are template contract terms that require the organisation receiving the data to commit to EU-equivalent standards of data protection, even where none exists in domestic legislation. In addition, they also set out who is liable, state in which jurisdiction disputes will be settled, and give data subjects legal standing to pursue complaints. Although theoretically once the contract is in place data can flow freely, the recent CJEU ruling in *Schrems II* has cast a shadow of doubt over their long-term viability.[10]

SCCs require both parties engaging in an EU to third country data transfer to agree and sign in order for that transfer to be lawful. SCCs are the principal method used to transfer personal data to third countries where there is no adequacy decision. Following the invalidation of the EU-US Privacy Shield, evidence from our interviews highlighted that most data transfers from the EU to the US are being done through SCCs.

2.3.2 Binding corporate rules

Whereas SCCs are primarily intended for data transfers involving two distinct legal entities, BCRs are a legal mechanism to facilitate data transfers within a company or group of companies. The BCR places an obligation on the entire organisation to comply with and adhere to pre-approved data protection standards. Due to their structure, complexity, and high cost, BCRs are almost exclusively used by large multinational corporations operating in multiple jurisdictions. There is, however, evidence that many large corporations are using SCCs to transfer internally as well as externally because they are easier to establish and maintain.[11]

BCRs are more costly and burdensome for organisations to set up than SCCs. Both require administrative and legal work, such as mapping all data flows and amending and renegotiating contracts. However, once a BCR system is in place, further transfers are easier to carry out, while new SCCs are required for every new data transfer. One of the data protection lawyers we consulted raised concerns about the legalities of companies signing contracts with themselves in internal SCCs but admitted it was widespread.

In our interviews we found a lot of scepticism about BCRs. They are perceived as requiring too much work, costing hundreds of thousands of pounds, and taking a long time, at least two years, often more. The critical factor though seems to be the need for data protection authorities (DPAs) to approve them. The BCR for Phillips, based in the Netherlands, even involved consultations with Singapore's regulator, for example.

> "BCRs are a headache because you need to be audited and approved. It is easier to move than to open up your systems." (interview with data protection lawyer)

> "BCRs would be good but given the work and role of the DPAs it is easier and cheaper to do SCCs. There is only one BCR in Sweden, Tetra Pak." (interview with data protection lawyer)

> "Nobody is doing BCRs. The ICO's [Information Commissioner's Office] site lists 20-30. A friend who works at a large firm says they have the resources to do it, but an invitation to an audit is very dangerous as there are many small breaches everywhere." (interview with data protection lawyer)

2.3.3 Other safeguards for transfers

The GDPR also allows international transfers under codes of conduct and certification regimes, together with legally binding commitments on the organisations involved. To date no one has implemented such systems anywhere in Europe. Our interviewees were not convinced that these mechanisms were a realistic alternative, with some exceptions. Certification was perceived as unrealistic and 'theoretical' for practising lawyers who just want simple solutions. Some interviewees were concerned that the CJEU could also declare

those invalid after all the work. However, others thought that good GDPR compliant certification schemes were close to being developed that deliver the required safeguards. These approved certification schemes, if diligently followed, could reduce the risk of fines.

We were told that there is some discussion at the International Organisation of Standardisation (ISO), which is not advancing. One reason is the need for organisations to administer the codes or certification regimes that can risk being liable to fines up to 2% of their turnover if they fail to discharge their duties properly.

The GDPR also outlines the possibility for codes of conduct to be used, although this has not yet happened.

2.4 USING ARTICLE 49: 'DEROGATIONS FOR SPECIFIC SITUATIONS' TO TRANSFER DATA

The final means by which data could be transferred from the EU to the UK is on the basis of Article 49 of the GDPR. There are several relevant legal bases on which Article 49 can be used. The main ones are:

1. When explicit, specific, and informed consent of the data subject is given.

2. When it is necessary for the performance of a contract and the data transfer is only occasional.

3. When data transfers are in the public interest. These can be made using Article 49 derogations. The UK established 23 public interest areas, from the prevention of fraud to the safeguarding of children in Schedule I of the Data Protection Act 2018 which could be used a rationale for transferring data.[12]

Although Article 49 derogations initially seem a viable way to proceed, the EDPB, an independent body that brings together all the European DPAs and issues guidelines and decisions on the GDPR, makes clear that their use should 'not become "the rule" in practice, but need to be restricted to specific situations and each data exporter needs to ensure that the transfer meets the strict necessity test.'[13]

This reinforces the notion that being granted adequacy is required to allow data to continue to flow freely and to avoid significant additional compliance costs.

3. WHY THE UK IS AT RISK OF NOT GETTING ADEQUACY

Over the years, the European Commission has been flexible and pragmatic in maintaining the free flow of data with key economic partners. The US, for example, despite lacking federal data protection legislation, was granted two partial adequacy decisions by the Commission. This bodes well for the UK[14], which has much higher data protection standards than the US and has implemented the GDPR. Furthermore, the UK's ICO is respected in EU circles, and the Commission does not want to induce economic disruption for EU companies in the form of no adequacy decision.

On these grounds, it is plausible that the Commission may grant the UK an adequacy decision. However, if it does, there is a strong possibility that it will be challenged in the courts, and potentially invalidated by the CJEU, just like Privacy Shield.

Furthermore, there are also reasons why the Commission might not grant the UK an adequacy decision, despite the UK's Data Protection Act 2018 and implementation of the GDPR.

For our economic analysis, whether the Commission does not grant an adequacy decision, or whether it does but then it is subsequently invalidated, these two outcomes are in the long-term the same. Both result in serious disruption to EU-UK data flows.

The assumption that adequacy is guaranteed can be questioned by the following factors:

1. Concerns as to whether the UK's national security, surveillance and human rights frameworks meet the standards of EU law.

2. Any potential breakdown of the wider Brexit negotiations, or a no-deal Brexit more broadly.

3. The UK's desire to have a comprehensive FTA with the US, and the problem of onward transfers.

4. The judgement by the CJEU in the *Schrems* and *Schrems II* cases, invalidating data-sharing arrangements between the EU and the US, and setting out detailed criteria for future adequacy decisions and other data transfer mechanisms.

3.1. UK NATIONAL SECURITY, SURVEILLANCE AND HUMAN RIGHTS FRAMEWORKS

There are a number of ways in the which the UK domestic legislative environment could make getting an adequacy decision more difficult.

The main points of concern are the following:

- The UK's Investigatory Powers Act 2016.
- Derogations from the GDPR in the UK's Data Protection Act 2018.
- Departure from the EU Charter of Fundamental Rights.

The main potential problem is the UK's Investigatory Powers Act 2016, which allows for the broad interception of communications and equipment interference. This Act may contravene EU fundamental rights law, although this is yet untested. This also needs to be interpreted in light of the recent CJEU ruling in the *Privacy International* case, which some scholars have argued raises doubts that the UK's bulk surveillance programme is not in line with EU law.[15]

The CJEU recently ruled in the *Privacy International* case that elements of the surveillance regimes of member states must comply with EU fundamental rights law.[16] This ruling does not explicitly declare the UK regime as unlawful, but it raises the bar and could be used by the Commission in its adequacy assessments.

The various issues raised by the potentially problematic domestic legislative framework actually creates a largely unforeseen consequence of Brexit. While the UK was a member of the EU, the bloc had to accept the UK's state surveillance apparatus because national security is within the prerogative of member states and outside the powers of the EU. However, this same apparatus will now be assessed

by the Commission when granting an adequacy decision. Additionally, while the UK was under the jurisdiction of the CJEU, EU citizens had the potential to seek redress for any abuses, but being outside the single judicial space of the EU, this becomes a problem.

As well as the issues that we have highlighted, there is another important way in which the UK could make getting adequacy difficult for itself. Boris Johnson has confirmed to Parliament that "the UK will in future develop separate and independent policies in areas such as […] data protection"[17] as evidenced by the recent launch of the National Data Strategy.[18] The risks in this approach are clear with the European Data Protection Supervisor (EDPS) noting that "any substantial deviation from the EU data protection acquis that would result in lowering the level of protection would constitute an important obstacle to the adequacy findings."[19]

3.2 THE POTENTIAL OF A NO-DEAL BREXIT

Another risk to highlight is the potential of a breakdown in the negotiations between the EU and the UK over the future relationship agreement, resulting in a no-deal scenario in 2021.

Although the rhetoric from both sides has been that they want to avoid a no-deal Brexit at all costs and previous insurmountable deadlines have been achieved, as UK Prime Minister Boris Johnson did when he was able to alter the Withdrawal Agreement and get it through Parliament, actions by the UK government have exacerbated the situation.

The highest profile action is the introduction of the Internal Market Bill, with its provisions that government ministers have admitted 'breaks international law'[20] by unilaterally departing from the Withdrawal Agreement, an international treaty signed with the EU.

Despite strongly worded statements from both sides, as well as the mini fallout over the Internal Market Bill and even a pause in negotiations, as of November 2020 negotiations have once again resumed, and some form of agreement remains plausible. Whatever happens, an adequacy decision, which is fundamentally a political decision for the EU, is at the whim of the wider Brexit process.

The adequacy decision is a piece on the wider Brexit chess board, which represents negotiating leverage for the EU. If the negotiations go well from the EU's perspective, then an adequacy decision may be forthcoming. If they do not, and especially if there is no-deal, then adequacy is highly unlikely.

Although the outcome of the Brexit negotiations is impossible to predict with any certainty, what is clear is that the UK is engaging in a high-risk strategy, which could force the EU into concessions enabling an agreement to be reached in time, but could also lead to a breakdown in the negotiations thereby leading to an acrimonious no-deal Brexit.

3.3 FUTURE UK-US TRADE DEAL AND ONWARD TRANSFERS

The US pushes hard for unrestricted data flows in its trade negotiations. If the UK agrees to significantly liberalise regulation around data flows with the US in a future trade agreement, this could undermine its prospects for gaining EU adequacy.

The EDPB recently stated that "when it comes to a possible adequacy decision for the UK, the EDPB considers that the agreement concluded between the UK and the US will have to be taken into account by the European Commission in its overall assessment of the level of protection of personal data in the UK, in particular as regards the requirement to ensure continuity of protection in case of 'onward transfers' from the UK to another third country."[21]

The primary concern of the EU will be that, even if the UK maintains the data rights of citizens, it will all be for nothing if at the same time the UK allows the free flow of data to the US. In short, the UK risks not being granted adequacy if it is perceived to be an avenue for unrestricted onward transfers of personal data to the inadequate US.

The EU's concerns may be valid, because leaked documents show that the US has stated that the "(EU GDPR) adequacy is a flawed system that cannot become a global standard."[22]

We do not know yet the exact content of the UK-US agreement, but we do know that the UK's proposed text for the future partnership with the EU contains proposals on digital trade lifted

straight from US trade policy. These include a positive obligation to allow cross-border transfers of information that would bypass adequacy. The UK is also proposing to create flexibilities to adopt other legal frameworks for data protection following international principles and guidelines. The proposed UK text says 'for greater certainty' that 'voluntary undertakings' by enterprises would be allowed as valid data protection frameworks.[23] This would create interoperability among various legal regimes and would make the UK a global data hotspot able to transfer data across currently incompatible legal boundaries.

The European Commission has a set of fixed clauses on data flows for all its trade agreements agreed with the European Parliament and Council. These "horizontal provisions for cross-border data flows and for personal data protection"[24] cannot be changed on a whim. The Commission cannot include the free flow of data in a trade deal bypassing the adequacy process and cannot agree to making the GDPR interoperable with other regimes. By necessity, the UK proposals must be rejected by the EU, and it is unclear what their purpose could be other than to signal future UK digital trade policy, and raise a red flag for the future of data flows with the EU.

UK officials argue that there are countries that have both an EU adequacy decision and free flow of data trade agreements with third countries, Japan being the prime example. Japan is party to various treaties, including with the US, that commit the country to enable unrestricted personal data flows with very limited exceptions. The Japan adequacy decision has attracted criticism and, in any case, contains clauses specifically excluding EU-imported data from further onward transfers, with specific mention of the kind of voluntary undertakings the UK has proposed. The UK and Japan have just signed an FTA that includes the same US-inspired policies on data flows and interoperability of privacy regimes that the UK had presented to the EU.[25]

One of the lawyers we spoke to mentioned unprompted that "laundering" data via Japan could be an option to bypass *Schrems II* and in the future the same could be done with the UK.

> "In reality, you can launder data. Lawyers will advise you to do it. For example, the Isle of Man adequacy could be key for data laundering, as it won't automatically change. UK companies will get push from European companies. Although European data protection legal teams are more cautious than in the UK. The UK will face more scrutiny." (interview with lawyer)

3.4 *SCHREMS* AND *SCHREMS II* JUDGEMENTS

The CJEU judgement in *Schrems II* provides a serious challenge to the UK being granted adequacy because it sets out criteria that the Commission will use to judge whether particular regulatory environments are adequate. All the people we spoke to after the ruling saw it as a game changer and said it had already had a huge impact on their work.

The *Schrems II* case builds on existing EU case law, such as *Digital Rights Ireland* in 2014, [26] *Tele2 Sverige/Watson* in 2016,[27] and informs the judgement in *Privacy International* in 2020,[28] which may be used to cast doubt on the conformity of the UK with EU data protection and fundamental rights law.[29]

Austrian privacy advocate Max Schrems originally brought a complaint against Facebook where he alleged that his data was not protected once it was sent to the US. The outcome of the case was more decisive than many expected and represents one of the most significant judgements on global data flows. The CJEU ruled that EU-US data transfers under Privacy Shield were illegal because ultimately no matter what obligations the US-based company signed up to, they would not be able to protect the data of EU citizens. The CJEU held that the nature and extent of US state surveillance powers was incompatible with EU law, and together with a lack of legal redress for individuals affected, this meant that Privacy Shield did not provide adequate protections for the personal data of EU citizens.[30]

There are conflicting views on the implications of the ruling. For some, EU data transfers to the US are dead, legally speaking. As privacy law expert Daniel Solove noted, 'a close look at the decision reveals that the SCCs don't really survive, at least not for the US and the logic of the decision also indicates that BCRs are in the same position.'[31]

On the other hand, Article 49 is not really suitable because it should only be used for ad hoc and occasional transfers. Several people we spoke to were of this view and thought that the only way forward is to shift operations away from the US, and in the future probably the UK.

An alternative view is that transfers can continue with added safeguards around areas like encryption and avoiding cloud services liable to surveillance, following advice from some German DPAs. However, even those who take this view are not certain whether these arrangements will be deemed legally sufficient, which is yet to be decided and will likely be the subject of future court challenges.

We uncovered evidence as part of our interviews that some companies are already using SCCs together with extra technical safeguards. Several lawyers told us that in the event that adequacy is denied to the UK, they would be using SCCs, despite their misgivings.

Importantly, the ruling also makes SCCs more costly and complex, which we discuss in more detail in the following sections.

A further impact of the judgement is to influence the basis on which the European Commission makes future adequacy decisions. Put simply, there is now much more heat on the issue. This is because the CJEU elaborated in detail on the criteria by which future adequacy decisions should be made. The Commission will want to avoid another high-profile defeat and reversal of its decision, and so it will incorporate the criteria and judgement into its UK adequacy assessment.

3.5 SUMMARY OF RISKS

What our analysis of the risks demonstrates is that there are no easy outcomes, and any decision will be subject to a varying degree of uncertainty. The only clear conclusion from the assessment of these myriad risks is that there is likely to be legal uncertainty around any adequacy decision, whether granted in full, partially, or refused and that this uncertainty is likely to last for years.

Under the best-case scenario where the UK is granted full adequacy, there will be the constant threat of invalidation of the whole decision following direct legal challenges or partial invalidation due to individual assessments by national DPAs. This looming threat is likely to result in many concerned companies and organisations seeking to implement SCCs and BCRs even in the case of the UK receiving a full adequacy decision.

If the UK fails to get an adequacy decision, companies and organisations wishing to transfer data from the EU to the UK will have to put in place SCCs or BCRs. However, as we have noted earlier in this section, SCCs and BCRs are also vulnerable to challenge since they cannot offer protection against foreign governments' surveillance and intelligence-gathering activities.

Therefore, given the shaky legal standing of SCCs, it could lead to a collapse in confidence from data exporters and regulators in the UK domestic data protection regime and lead to 'severe disruption to EU-UK data flows in the long-term. This would be damaging for the UK's services-based economy and especially problematic for the finance, life sciences and digital tech sectors, particular data centres and cloud service providers.'[32]

Ultimately, doubt and confusion over whether SCCs and BCRs are compliant or whether extra measures are needed could mean that some EU-based companies relocate some of their operations within the EU, or other adequate countries, while others will charge UK companies more to compensate for the complexity and risk.

4. SCOPE, SCALE, AND VALUE OF EU-UK DATA TRANSFERS

Of the UK's international data flows, 75% are with the EU. Much UK economic activity is dependent on these flows.[33] This is especially true for the services sector, which comprises 79% of the UK economy. To illustrate the potential importance of EU-UK data flows, 46% of UK exports are to the EU, of which services account for 40%.[34]

Unfortunately, these are relatively blunt indicators for assessing the true value of EU-UK data flows. There is a significant gap in the literature and evidence base on the scale, scope, and value of cross-border data transfers in general. This evidence gap is bad for public policymaking, especially as data flows climb up the political and trade agendas.

Given the centrality of cross-border data flows to society and the economy, it is striking that there is no established method for measuring their value, scale, and scope. Much of the required information is not being collected in the national accounts by statistics bodies, although there is work to provide new guidance.[35] Firms are typically not obliged to measure or report on their cross-border data flows. Therefore, unlike indicators such as trade and investment, relevant information on data flows is not captured in official or mandatory surveys. The Organisation for Economic Co-operation and Development (OECD) reports that "intra-firm transactions in cross-border data flows are unlikely to be recorded at all in official trade statistics."[36]

This evidence gap means it is difficult to accurately assess and predict the economic implications of the UK not getting an adequacy decision. Without knowing the value of data flows, it is hard to say exactly what the economic hit of a disruption to EU-UK data flows will be.

The contribution of this report is to outline and detail the different economic variables which will be impacted by a disruption to EU-UK data flows. Although we cannot say exactly how much these variables will be impacted, we hope that our conceptual discussion and analysis adds to the emerging literature on the value of data flows.

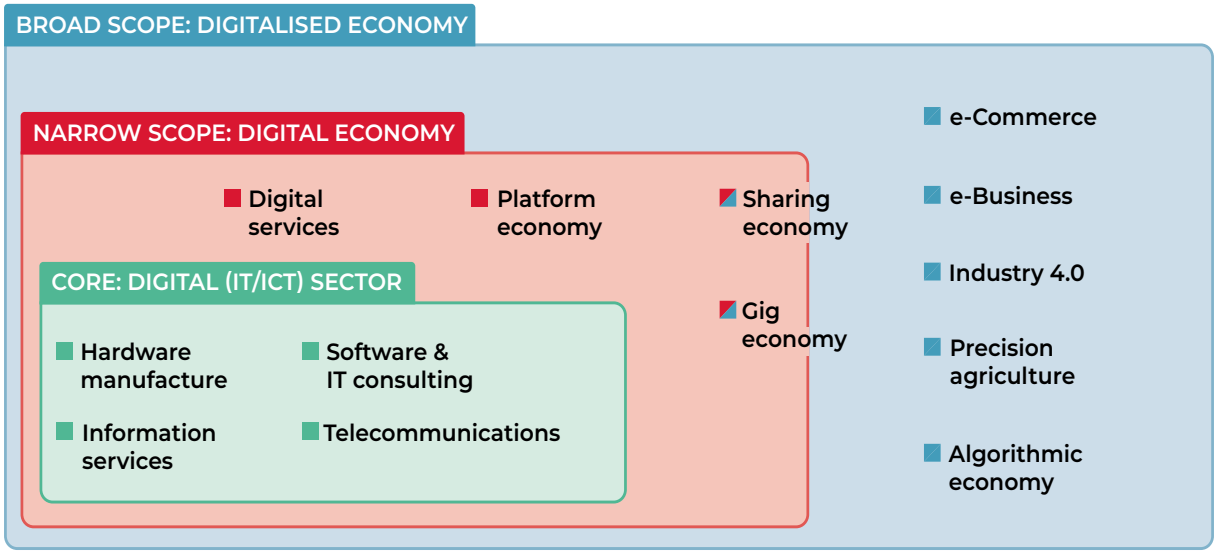
4.1 HOW THE DIGITAL ECONOMY IS MEASURED

Evidence-based policy on data and digital trade has relied on an intuitive understanding that data flows are important for economic development, but concrete figures on attribution and the specific impact of individual policies are elusive. Understanding the potential impact of EU-UK data flow disruption requires us to situate our discussion in the wider efforts to measure the value of personal data flows and the digital economy.

Part of the reason why measuring the value of the digital economy is difficult is because digitalisation affects almost every area of economic activity, and for a large proportion of people in the world it is transforming the way we work, relax, and communicate.

At the international level, the United Nations Conference on Trade and Development (UNCTAD) and the OECD are the leading organisations building methodologies that enable us to value the economic activity of the digital economy. UNCTAD's model,[37] following the work of UK academics Bukht and Heek,[38] is useful because it provides three different levels upon which the digital economy can be analysed (Figure 1). UNCTAD's model has at its core the infrastructure, from hardware to software, that facilitates the digital economy. Surrounding the core is a narrow ring of digital services and platforms, the key components of what most people understand by the digital economy. The broader "digitalised economy" scope includes all the 'digitally enabled sectors', from finance to travel and retail, and extends the remit of the digital economy into almost all sectors of the economy.

FIGURE 1: SCOPING THE DIGITAL ECONOMY



Source: UNCTAD (2019) *Digital Economy Report 2019: Value creation and capture*

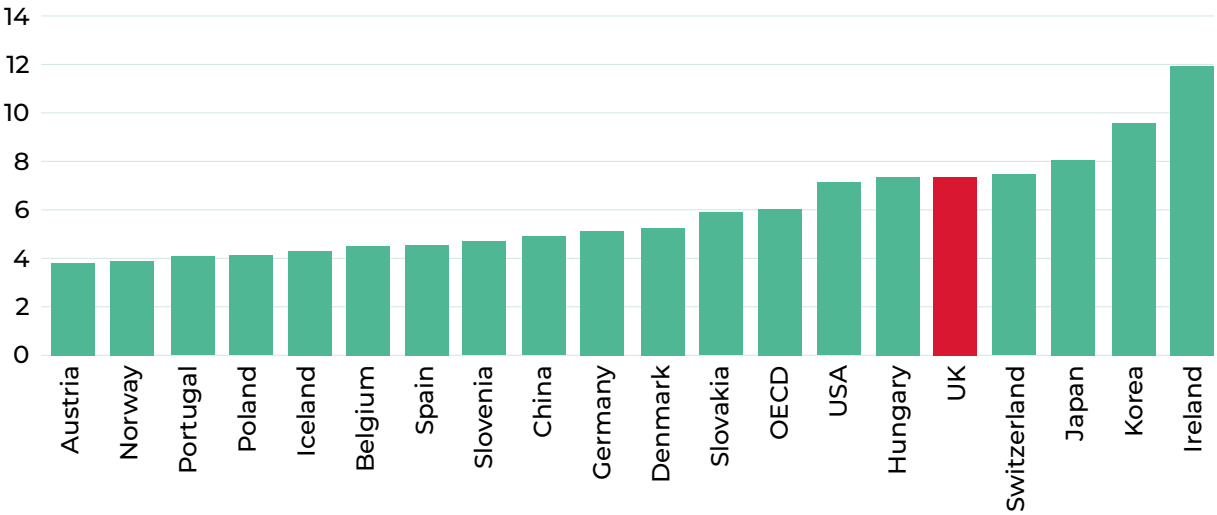
The OECD has gone further and developed a classification for all sectors of the economy by defining and measuring their 'digital intensity', defined as the proportion of investment in relevant areas from ICT investments to robotics, to skills and online delivery channels.[39]

The wider framework for measuring the digital economy of a country includes infrastructure, such as broadband penetration, use of technology, adoption of cutting-edge technologies, jobs, and productivity.[40] Estimates of the contribution of the digital economy to global gross domestic product (GDP) range between 4.5 and 15.5%.[41]

The broader digitalised economy is even harder to determine. UNCTAD calculates the global volume of e-commerce in 2018 at $25.6 trillion, equivalent to 30% of global GDP, with a majority being business to business (B2B). The UK is ranked fifth in the world, with 32% of GDP generated through e-commerce, ahead of other European countries.[42] However, this is only one aspect. There is also digital value added in manufacturing or agriculture, for example.

One additional problem is that many digital activities are excluded from GDP and any traditional economic indicators if there is no

FIGURE 2: THE DIGITAL ECONOMY/GDP - NARROW DEFINITION (IN PERCENT)



Sources: OECD, Natixis

monetary transaction. Creating free advice videos on YouTube or editing Wikipedia clearly adds economic value but this is not reflected anywhere. Data flow disruption could have a notable impact on these activities, but we would struggle to quantify it.

The UK has an exceptionally strong digital economy and is one of the most digitalised countries worldwide. According to the narrow definition of digital, the UK's digital economy comprises between 7 and 8% of GDP. As can be seen in Figure 2, this is well above the OECD average.[43]

4.2 WHAT IS DIGITAL TRADE?

We want to narrow down our perspective to cross-border activities in the digital economy, such as digital trade. There is no single definition of digital trade. There is also a lack of data on the scale, nature, and trends of cross-border digital trade.[44]

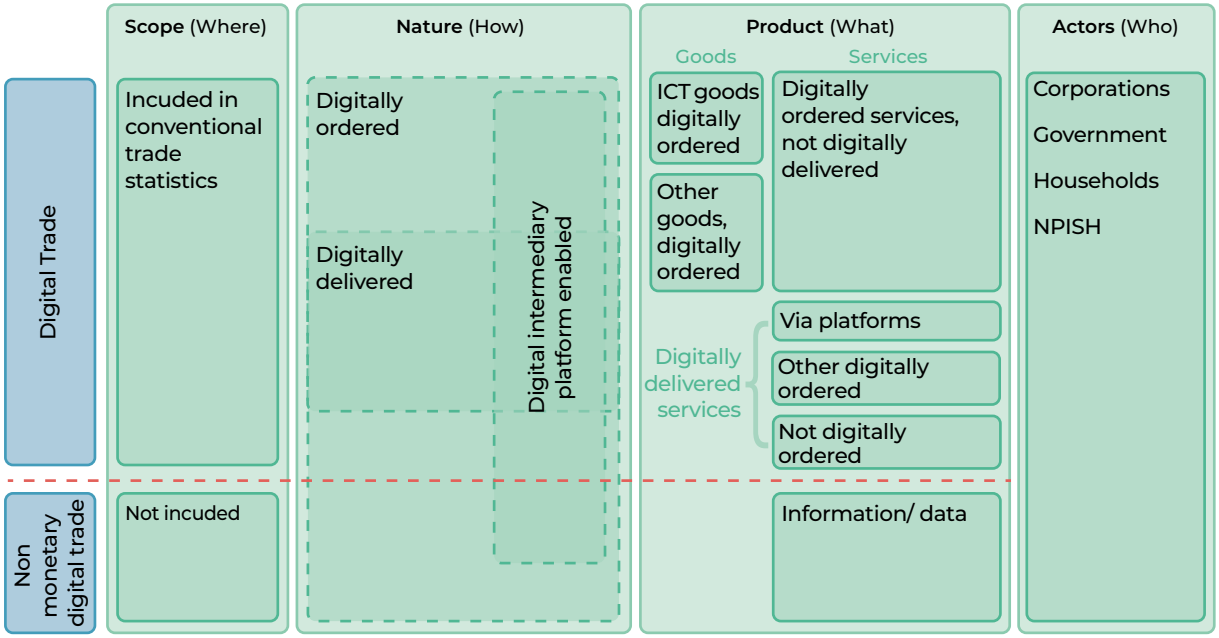
The OECD's conceptual framework for digital trade (Figure 3),[45] co-produced with the International Monetary Fund (IMF) and World Trade Organization (WTO), carries the broadest consensus and focuses on the nature of the transaction, defining digital trade as encompassing both digitally ordered and digitally delivered products and services.

Digitally ordered transactions are equivalent to e-commerce, and involve delivery of both services and goods, while digitally delivered transactions can only include services. Most e-commerce is B2B, which in the UK context is more vulnerable to the EU data adequacy negotiations. There is some debate on how to deal with 3D printing and downloaded purchases, but the growing consensus is to focus on services delivered through digital systems. This covers a huge range of activities, from graphic design to software development.

The OECD framework (Figure 3) includes services that are ordered digitally from abroad but not delivered digitally across a border and instead involve physical travel, such as tourist guides or data roaming.

There is growing evidence that digital trade encompasses an increasing proportion of global trade, is growing at a faster rate than non-digital trade, and is of greater value added to economies.[46] The Office for National Statistics (ONS) estimates that the UK exported £190.3 billion digitally delivered services (representing 67.1% of total UK services exports) and imported £91.1 billion digitally delivered services (or 51.7% of total UK services imports) in 2018.[47]

FIGURE 3: THE CONCEPTUAL FRAMEWORK FROM DIGITAL TRADE



Source: OECD, IMF & WTO (2017) *Handbook on Measuring Digital Trade*

4.3 HOW THE VALUE OF DATA FLOWS IS MEASURED

Measuring the value of data and data flows is the greatest challenge.[48] There is even less understanding of data flows than both digital trade and the digital economy, although it is widely agreed that cross-border data flows are a core component and an enabler of both.

Today, businesses are either data-enhanced, meaning that they use data to improve, or data-enabled, meaning that their business model depends on deriving and generating value from data.[49]

Data does not have an inherent value without the ability to monetise it, so the same dataset will be priced differently in different contexts. There are several approaches to measuring the value of data, but no consensus.[50] Without knowing the value of data, it is impossible to know the value of data flows.

Data flows are also not inherently valuable. Transferring data across borders does not alter the nature or content of data, so it does not necessarily add value to it. However, data flows enable and facilitate processes and activities through which organisations derive economic value from data. For example, the same data might become more valuable if is transferred abroad in order to be processed by more powerful computers or with more advanced artificial intelligence systems located elsewhere.

Put simply, cross-border data flows underpin and enable the activities which enable businesses to derive value from data, such as data aggregation, analysis, and ultimately monetisation.

Estimates of the value of global data flows have been provided by the McKinsey Global Institute by correlating GDP with volumes of data flows[i] and other economic variables. They valued the contribution of data flows to global GDP at $2.8 trillion in 2014, directly raising world GDP by 3%, mainly through productivity increases.[51] They also ranked the UK as the third most connected country in the world for cross-border data flows.

While the McKinsey approach provides a generic idea of the importance of data flows for a country, it remains a very broad estimate. Besides, most data flows by volume comprise audio-visual media of relatively low value transferred across content delivery networks such as Akamai, which accounts for between 15 and 30% of all web traffic.[52]

A more granular data flow mapping and valuation method is proposed by the OECD, where input-output tables are superimposed on data flows in order to track value added and capture the reliance of different industry sectors on inputs from data-intensive industries. However, we cannot yet reliably put a number on the value added by specific cross-border data flows to a nation's GDP. This would require granular firm-level data obtained through bespoke surveys.

However, an important finding from the OECD research is that the volume of transferred data is not necessarily a useful indicator when trying to establish the value of cross-border data flows.[53] Therefore, although not obtaining an adequacy decision could result in the large-scale disruption of EU-UK data flows, the exact scale of the disruption is not necessarily directly correlated to the scale of the economic impact.

For example, it could be that data transfers in some sectors or contexts are much more valuable than transfers in others, so the economic consequences would depend on which data transfers and sectors are disrupted, rather than merely the scale of the disruption.

This is important, because it is possible to estimate the volume of EU-UK data transfers, for example by analysing overall internet traffic and connectivity, or data centre construction patterns. However, these variables alone would be a blunt indicator for determining how important and valuable the data flows are.

Despite all of this, there is a growing body of evidence which indicates that restricting cross-border data flows can negatively impact trade, investment levels, and other key indicators.

i The volume of data flows is calculated by proxy by looking at the capacity of submarine fibre optic cables.

However, the relationship between data restrictions and macroeconomic indicators is not straightforward. The European Centre for International Political Economy (ECIPE) has produced the Digital Trade Restrictiveness Index (DTRI), which ranks 64 countries using variables like restrictions on data flows and establishment restrictions. China is ranked the most restrictive nation to digital trade, with New Zealand as the least restrictive. The UK is ranked favourably as the 44th most restrictive to digital trade, between Austria and Croatia.[54] Only one EU country (Ireland) is in the top ten nations least restrictive to digital trade, which is perhaps unsurprising given the strict system of EU-third country data flows. In the DTRI,[55] regulations restricting cross-border data flows are considered a key barrier to digital trade. The index paints a complex picture with some very restrictive countries like China doing well economically, showing that more research is needed; we may also need to look at other factors beyond GDP when examining digital trade policies.

ECIPE analysis predicts that if countries lifted their restrictions on cross-border data flows, the imports of services would rise on average by 5% across all countries, and there would be productivity gains of approximately 4.5% on average.[56]

It is important to note that not all data flows involve personal data subjected to GDPR.[57] Separating the component of personal data within data flows has eluded researchers, and may prove conceptually impossible, given that under the GDPR 'non-personal' data can become 'personal' when combined with other information that enables the identification of individual inferences.

Our report focuses exclusively on the economic implications of disruption to EU-UK transfers of personal data, as this is what is at risk if the UK fails to obtain an adequacy decision.

4.4 THE VALUE OF EU ADEQUACY DECISIONS

Given the limited evidence on the value of cross-border data flows, an obvious approach when considering the economic consequences of the UK not getting adequacy is to analyse the value of existing EU adequacy decisions. For example, when a country is granted an EU adequacy decision, are there discernible and measurable economic benefits? If so, it might be reasonable to assume that there could be negative impacts on the same variables if there is data flow disruption between the EU and a third country.

Unfortunately, and somewhat surprisingly, we are not aware of any comprehensive studies on the economic impacts of a third country receiving an EU adequacy decision. This is despite the fact that there are 13 countries that have received adequacy decisions, including Canada, Israel, Japan, and the US.

There are no studies which compare the economic 'before and after' of adequacy decisions and the associated data flow liberalisation. In terms of future research, the most promising candidates would be Japan and the US. Japan's adequacy decision was granted by the EU in 2019. Prior to the liberalisation of data flows, there were many years of EU-Japan economic relations in the digital economy era. As the EU-US Privacy Shield was invalidated this year, a long period of EU-US data flow disruption could ensue. These case studies could provide for insightful economic research on the value of data flows.

This lack of evidence has been frustrating for key stakeholders. For example, a senior EU official we interviewed complained that they do not know whether they should believe US technology companies when they argue how important transatlantic data flows and Privacy Shield are, as they do not have robust empirical data to back this up. Similarly, data protection lawyers we interviewed from Argentina complained that the bold claims made by local politicians about the economic benefits of their EU adequacy decision were never followed up with empirical studies.

Furthermore, there is virtually no precedent for significant disruption to previously unrestricted commercial data flows between two jurisdictions; no one knows exactly what this would entail. Although data localisation is common, such measures are usually not enacted from a starting point of full liberalisation of data flows, which is what could happen to EU-UK data flows. Evidence could emerge on the economic consequences of disruptions to EU-US data flows, although there is not much thus far.

When the EU-US Privacy Shield was invalidated, the immediate response from the US Department of Commerce was that they hoped to 'limit the negative consequences to the $7.1 trillion transatlantic economic relationship'.[58] The use of this headline figure indicates that data flows are considered to underpin all transatlantic economic activity. It also suggests that putting a number on the scale and value of EU-US data flows is neither possible nor useful.

Interestingly, the European Commission is currently funding a major research project on the economic value of data flows, but this is not exclusively on cross-border flows of personal data.[59] Given the lack of data and evidence on the economic value of EU-third country data flows and adequacy decisions, our report on the impacts of the UK not getting an adequacy decision provides novel research and understanding on an increasingly important public policy issue. We hope it will inspire future work in this area.

5. DEFINING THE ECONOMIC IMPACT OF THE UK FAILING TO GET EU DATA ADEQUACY

Our evidence indicates that the impact of the UK failing to get a data adequacy decision from the EU could be large. However, providing reliable estimations is challenging, for the reasons outlined in the previous section.

This section will outline and explain the principal ways in which the disruption of EU-UK data flows, via no adequacy decision, will impact business and the UK economy.

Before doing so, it is reasonable to say that not getting an adequacy decision will almost certainly have a net negative impact on the UK economy, at least in the short and medium term. This is why the UK government has an official policy of obtaining adequacy and has long considered it a priority issue. An adequacy decision is also strongly desired by a broad cross-section of the business community, major business groups like the Confederation of British Industry (CBI), techUK, and the Federation of Small Businesses (FSB), as well as virtually everyone we interviewed.

Furthermore, the disruption of EU-UK data flows will affect a vast number of UK businesses and economic activity. The Department for Digital, Culture, Media, and Sport (DCMS) reports that the UK digital sector contributes £149 billion[60] of global value added (GVA)[ii] and would be hit particularly hard by the failure to get adequacy. The largest single component is digital services, which contribute £28 billion of GVA.[61] According to the FSB, over one-third of their members trade across borders. Crucially, businesses of all sizes, in all sectors, engage in cross-border data transfers, but services sectors like finance and digital technology are most exposed.

We have identified five separate ways in which the lack of an adequacy decision would impact the economy and firms engaging in EU-UK data transfers:

- Increased cost of doing business, due to new compliance requirements.
- Increased risk of GDPR fines.
- Reduction in EU-UK trade and digital trade.
- Reduced investment (both domestic and international).
- Relocation of business functions, infrastructure, and personnel to outside the UK.

The increased costs of doing business, which would be driven by the new compliance requirements (e.g. firms having to set up SCCs), is the most significant impact in the short term. The increased risk of GDPR fines and enforcement action stems directly from these new compliance requirements.

The potential impacts on investment, trade volumes, and business relocation are all knock-on effects stemming from the increased compliance burden and regulatory enforcement risk. Put simply, not getting an adequacy decision means the creation of a substantial non-tariff barrier to EU-UK trade, which may cause a myriad of potential economic consequences. Our report does not model the macroeconomic impacts of no adequacy decision. However, it outlines in detail why there would be a negative impact across these macroeconomic indicators.

Our economic modelling focuses exclusively on the direct costs to business of compliance brought by the absence of an adequacy decision. Further work is required to establish the wider macroeconomic costs of disruption to EU-UK data flows. This would complement our work on firm-level costs.

ii GVA is Global Value Added, defined as GDP + Subsidies - taxes. This is a more accurate measure but harder to tally internationally where GDP is the main approach.

5.1 INCREASED COST TO BUSINESSES AND ORGANISATIONS, DUE TO NEW COMPLIANCE REQUIREMENTS

In terms of cross-border data flows, there is no practical difference between being granted an adequacy decision and actual membership of the EU/European Economic Area (EEA), which is why adequacy is so economically desirable.

If the UK does fail to get an adequacy decision, then all organisations engaging in EU-UK data transfers would be required to put in place alternative measures to ensure that the transfers are GDPR compliant. If firms continue to transfer data from the EU to the UK in this scenario, without setting up the required legal mechanisms, then those transfers would be unlawful. This issue does not apply to UK-EU data transfers, as the UK has committed to allowing the free flow of data from the UK to the EU to continue.

The 'new' legal mechanisms which firms will have to set up will be required by EU law (i.e. GDPR), not UK law, as they concern the protection of personal data transferred from the EU to the UK, i.e. data of EU citizens. Without an adequacy decision, the UK will be treated, under EU law, as any other third country.

All third countries, except the 12 that have been granted adequacy, can only receive data from the EU if the organisations transferring data set up SCCs or other legal safeguards. There are also the Article 49 derogations for exceptional circumstances, but these cannot be used for routine data transfers.

As we have outlined, the two most common EU data transfer mechanisms are SCCs and BCRs. We focus most of our economic analysis on SCCs, as this is what will be set up by firms in the overwhelming majority of cases. BCRs only apply to intra-company or intra-group transfers, whereas SCCs are contracts which enable lawful cross-border data transfers between distinct organisations. As discussed, most of the lawyers and companies we spoke to dismissed BCRs as an unviable option.

Overnight, on 1 January 2021, hundreds of thousands of EU-UK data transfers could suddenly be illegal, unless they are covered by additional legal safeguards like SCCs. This implicates at least tens of thousands of organisations, who will suffer from an increased cost of doing business due to these new compliance requirements.

Although certainly not an insurmountable barrier, this will be a costly bureaucratic and legal exercise for many firms, with some companies having to update, (re)negotiate, and sign thousands of contracts with their existing partners, suppliers, and vendors. These costs could be especially threatening to start-ups and small and medium enterprises (SMEs), who will be the least well-resourced to deal with the compliance burden; may lack the capital to invest in potentially expensive external legal capacity; and, where the EU company is larger and more powerful, they may have to concede to other demands as contracts are re-opened. It is certain that failure to get adequacy will increase the cost of doing business for all firms impacted, including any firm that trades with, has customers in, or operates within the EU.

An individual SCC will need to be set up or added to the contract between EU and UK parties for each point-to-point data transfer. This means that companies, especially those that are more data intensive, will have to establish or incorporate SCCs in literally thousands of different agreements with thousands of different companies. It is easy to see how this could quickly escalate into a significantly expensive, bureaucratic activity.

University College London, for example, would need to amend and update over 5000 contracts. Several UK-based cloud service providers with thousands of EU enterprise customers would also need to update contracts with each customer. These SCC numbers are actually quite moderate compared to some larger UK-based multinational companies.[62] The scale and volume of new compliance work across the economy could be vast, especially for UK-based firms with a sizeable European presence.

Having said that, it is important not to over exaggerate how much of a bureaucratic challenge this would be. The costs of setting up SCCs can easily be absorbed by large, multinational firms, many of whom are quite well prepared. Although costly and time consuming, this should not represent an existential threat to most firms but would add up to very large amounts overall.

However, given that EU-UK data flows have been completely unrestricted since the emergence of the modern Internet and digital economy, this is a completely new issue for many businesses. There is evidence that many smaller businesses are unaware of the threat to EU-UK data flows, the implications for their business, and the potential new compliance obligations.

For example, an FSB survey, published in November 2019, found that few small firms are aware of SCCs as a means to transfer personal data internationally.[63] Our interviews with business groups and data protection lawyers confirmed that the general level of business awareness and understanding of these issues is very limited. The director of one regional Chamber of Commerce told us:

> "This issue has never been raised in any meetings or by any of our members, despite many of them being digital technology startups." (interview with Chamber of Commerce director)

Also, a start-up policy advocate claimed:

> "No adequacy decision would be catastrophic for start-ups; their level of knowledge of this issue is painfully low." (interview with start-up policy advocate)

Some lawyers pointed out that even before we get to adequacy, the level of data protection compliance among SMEs is already very low, maybe 50%, with some having taken off-the-shelf advice but not quality tailored counsel.

The general lack of awareness is even more stark among EU firms. We were repeatedly told that this issue is not on their radar, and sometimes UK firms attempting to set up SCCs with EU firms struggle to get meaningful engagement on the issue. Lawyers in the EU told us that only companies very invested in the UK were considering taking proactive steps to comply. One partial exception is Ireland, where technology companies are vying for UK business and seem to be much more aware.

Dutch lawyers also told us that some UK-based Software as a Service (SaaS) companies began moving their hosting to the Netherlands when they saw that data adequacy was not in the Withdrawal Agreement. However, many organisations have not done anything though.

As well as a lack of awareness and of understanding, there is also a corresponding lack of preparation. The vast majority of impacted companies have not yet done the work needed to set up SCCs. In our interviews, we were repeatedly told that start-ups, SMEs, and even some larger companies are adopting a wait-and-see approach, and that they will not act, i.e. dedicate time and money, until they absolutely have to.

Not all the lawyers consulted had this perspective. One tech specialist told us that their clients were preparing statements for reassurance and that some are relocating work to the EU or setting up affiliates. Other lawyers told us that Brexit is already ramping up costs and adequacy will accelerate this process.

Most businesses will not even begin the work to set up legal mechanisms to cover EU-UK data transfers until it is definite that the UK will not receive an adequacy decision. The data protection lawyers and consultants we interviewed were surprised at how little client activity there was on the EU-UK data flows issue. Some UK lawyers told us that they have raised the issue with their clients, but most are too busy with the pandemic. The economic fallout from Covid-19 has placed this issue even further down the risk register and priority list, as many businesses are in survival mode. We were told that they expect a tsunami of work just before the end of the year as firms try to catch up. However, this will not be enough time, except for the larger companies that have already done their homework in terms of data mapping.

It is important to state that there have been concerted efforts by the Information Commissioner's Office (ICO), the UK government, and the European Commission to inform businesses and raise awareness of this issue. These engagement efforts have been consistent and wide-ranging since at least 2018. For example, the UK government has recently published guidance on 'Using personal data in your business after the transition period', which notes that from 2021, SCCs might need to be set up to receive data from the EU.[64]

5.2 *SCHREMS II* FURTHER COMPLICATES THIS

Arguably the most important outcome of the *Schrems II* case is the upholding of all SCCs and the simultaneous imposition of a stricter system of reviewing, on a case-by-case basis, whether an SCC actually delivers adequate levels of data protection in practice. This judgment means that using SCCs to transfer data to *any* third country that is not able to provide equivalent levels of data protection to EU standards could become problematic.

The judgement places greater responsibilities on data exporters (i.e. companies), as they now need to carefully review whether an adequate level of protection can be delivered to transferred data before signing an SCC. This may even include reviewing the national security and surveillance legislation of the country the data is being transferred to and outlining, in the SCC, why the data is still adequately protected post-transfer. Some legal experts think that this means data can no longer be transferred to US technology giants, like Facebook and Google, using EU-US SCCs.

Business representatives we interviewed have criticised this new reality, arguing that:

> "the CJEU is asking companies to deliver mini adequacy decisions every day, something which the European Commission has only managed to do 13 times in 25 years!"

Lawyers have said that the ruling puts them in an impossible position and it feels impossible to be compliant.

> "*Schrems II* creates a catch-22 where you must have a compliant mechanism but also a prior assessment of the country and the protections. How can UK lawyers assess the US?" (interview with data protection lawyer)

> "With GDPR and Schrems we will need experts on both US and EU laws, and even state laws. This could cost tens of thousands of pounds, but nobody is doing it at the moment, and even clients with money are reluctant." (interview with data protection lawyer)

> "The key is that third parties don't want to be associated with the transfer." (interview with lawyer)

Many data protection practitioners acknowledge that SCCs pre-*Schrems II* were a box-tick and a 'paperology' exercise which did not deliver enhanced data protection in practice, as most contracts were simply signed, stored, and forgotten about. This has all changed. The parties are now looking at the clauses while before they did not.

> "Everyone wants to understand their potential liability." (interview with lawyer)

> "Clients paying more are on the data exposed side, but US importers are also incurring costs. Both sides need to become experts on laws and their application, as SCCs are not just one way, both sides have obligations and costs." (interview with lawyer)

The future of using SCCs to transfer from the EU to third countries very much depends on the future approach of the DPAs. The EDPB and EU DPAs have recently published some detailed guidance.[65] EU Commissioner for Justice, Didier Reynders, recently said: "It's very important to say that it's not just possible to use SCCs without any changes."[66]

Some UK lawyers working with SMEs complained bitterly that the advice from DPAs is for academic lawyers. Companies cannot understand it. They need better practical advice. They were aware that the ICO has an SCC generator but did not know anyone using it. The feedback was that the material is either too high level or too detailed.

Businesses are continuing to use SCCs to transfer data to the US. If the UK fails to attain an adequacy decision, the vast majority of businesses transferring data from the EU to the UK would seek to use SCCs. However, the new legal reality means

that these SCCs may need to be bolstered with additional legal or technical safeguards, such as encryption, the use of internal networks, or detailed legal analysis and explanations of how the data is actually protected from eavesdropping and other risks when it is transferred to the third country.

In practical terms, this will likely increase the costs of setting up SCCs – sometimes dramatically – meaning the compliance burden on UK-based firms engaging in EU-UK data transfers could actually be far greater than originally thought.

Furthermore, if the UK was not recognised as adequate, then the concern would be that SCCs used to transfer data from the EU to the UK may also be unable to deliver an adequate level of protection. If the Commission does not grant an adequacy decision, it might explain and justify this decision in some detail. The Commission's official explanation could pose issues for the future use of SCCs, which would have to counter the negative assessment of the EU.

Depending on the approach of regulators and activists, EU-UK SCCs could become vulnerable and face suspension. Complaints, cases, and investigations are guaranteed. In an extreme scenario, the EDPB could suspend all data transfers to the UK based on SCCs, unless "supplementary measures" to protect the data were adopted.

This could particularly implicate telecommunications operators (e.g. Internet service providers, social media websites, email and cloud service providers) most affected by Investigatory Powers Act notices. But it could be much wider. As one of our interviewees explained, with powers around bulk datasets anything is in the scope of UK mass surveillance. In UK surveillance law, there is a difference between the person signing the SCC and those who could be forced to share data with government. There are powers to compel people to give up encryption keys, so even the most technically elaborate SCCs may not be enough of a guarantee.

SCCs impose a duty on the data importer, in our case the UK entity, to proactively report to the EU data exporter any legal issues that may prevent the data importer from complying with the SCC. These include any potential legal duty to disclose or transfer data to the security services, even if not actually asked to do so. If the UK importer fails to notify the EU exporter, then the whole transfer may be illegal. This leads to a situation in which the UK importer informing the EU exporter of the potential of UK security services accessing the data may render the SCC invalid and yet failure to inform may also render the SCC invalid. It is easy to see how this scenario may put EU exporters off transferring data to UK companies.

To summarise, the *Schrems II* judgement could greatly increase the cost of setting up SCCs. It also means that using SCCs for EU-UK data transfers is not a system that can be relied on long term, but there is also no viable alternative system. If SCCs cannot be used in the event of no adequacy decision, this will severely disrupt EU-UK data flows, with no obvious workaround.

5.3 OTHER COMPLIANCE REQUIREMENTS

5.3.1 Article 71 of the Withdrawal Agreement

The need to set up legal mechanisms, like SCCs, is not the only compliance requirement which could increase the cost of doing business in the event of no adequacy decision. Article 71 of the Withdrawal Agreement could become very relevant in this scenario. Under Article 71, any non-UK citizens' data which was transferred to the UK before the transition period will have to be processed as if EU data protection law and case law, as it stands on 31 December 2020, still applies after the transition period. This requirement also applies to the processing of non-UK citizens' data transferred to the UK after the transition period on the basis of the Withdrawal Agreement (e.g. as part of the citizens' rights arrangements).

This requirement does not come into force if the EU grants the UK an adequacy decision, as in this scenario the EU considers UK law to deliver sufficiently high standards of data protection.

However, if there is no adequacy decision, UK-based firms will be in a very complicated situation where they will have to differentiate between and potentially disaggregate various different categories of personal data: UK citizens' data, non-UK citizens' data received before the transition period, EU citizens' data received after the transition period, and non-UK citizens' data received after the transition period. This is because GDPR and the

corresponding CJEU case law may evolve, and UK data protection law and case law may also diverge from EU law.

With no adequacy decision, firms would be legally obliged to process these different categories of data under different standards and effectively three different legal regimes (UK law, EU law, and EU law as at 31 December 2020). This problem could become very complicated over time. This segregation of UK and non-UK datasets could entail a significant administrative burden for already stretched firms and would be further complicated if the UK law were to diverge substantively from the GDPR. [67]

5.3.2 Article 27 of the GDPR

A completely separate data protection compliance requirement on firms is the 'representative obligation'. Article 27 of the GDPR stipulates that organisations which are not established in the EU, but sell goods and services to EU citizens, or monitor their behaviour, must have a 'representative in the Union'. In practice, this means that after the Brexit transition period, many UK companies will need to establish some kind of representation in an EU country. At the very least, this includes an EU postal address and an appointed representative who can correspond with EU regulators and data subjects. This will not be of much concern for larger firms with an international presence but represents an additional cost for many start-ups and SMEs.

This additional compliance requirement is caused by Brexit alone, not by the lack of an EU adequacy decision. It will apply even if the UK is granted adequacy. Article 27 has been called the 'hidden obligation' by some experts, due to the lack of awareness and enforcement of it.

Several of the lawyers we talked to stressed that this will be a cumulative cost for small companies of a minimum between €500 and €1000 a year on a retainer fee plus extra work if there is an issue.

6. ESTIMATING COMPLIANCE COSTS FOR ORGANISATIONS IF THE UK FAILS TO GET AN EU ADEQUACY DECISION

If there is no adequacy decision, we calculate that there will be a cost to firms of between £1 billion and £1.6 billion due to the additional compliance obligations (i.e. setting up SCCs) on companies that want to continue to transfer data from the EU to the UK. The figures represent money that companies would have been free to spend to meet the requirements of the business by, for instance, investing in new equipment, staff, or processes but are now required to channel into compliance activities or additional costs for goods and services, due to the failure of the UK to secure an adequacy decision.

Some of this money may be spent on UK services and not cause a complete drop in UK gross domestic product (GDP), but overall, it will be an opportunity cost to investment in more productive value-generating activities. This sudden demand may alter the price of the required services but the supply of specialist legal and data services is unlikely to increase dynamically enough, which may mean that many companies cannot comply with the new requirements.

To calculate this number, we derived the average cost of compliance for an average micro, small, medium, and large company. Although SCCs are just standard terms to be inserted into directly into contracts, much of the real work needs to be done to map all of a company's data transfers, conduct risk assessments, and engage legal experts. Just mapping the data flows can be a massive and complicated task, depending on the sector and business model.

Mapping data flows is necessary not just to ascertain which entities need to have an SCC added to the contract but also because the SCC needs to describe the data which is being transferred. One lawyer we interviewed said that a client once engaged in such a vast data-mapping exercise that by the time it was completed, it was out of date and redundant, meaning hundreds of thousands of pounds were wasted.[68]

Once the data flows are mapped, the organisations identified, and the data points defined, the company is then ready to start setting up and incorporating the SCCs into their contracts. As noted earlier, the process of incorporating an individual SCC does not need to be complicated and can often be done with a minimum of fuss. However, it can also be an opportunity for one party to (re)negotiate other aspects of the commercial relationship, such as liability provisions, as SCCs can be inserted into broader contracts.[69]

Indeed, several of the practitioners we talked to said that SCCs opened a huge debate on liability that companies had never considered before. Also, many companies may not have clarity on whether they are mere processors or controllers, as their role and activities may have changed over time. This is critical to finding the right SCC model but will open a can of worms for many collaborations among companies.

> "It will be like when GDPR came into force. Every controller sent suppliers an s20 but not everyone was a processor. There will be confusion over what SCCs to use." (interview with lawyer)

We have used the costings produced by the European Commission when it estimated the cost of doing data protection impact assessments (DPIAs) as required by the GDPR.[70] The study estimated that a small-scale DPIA would cost €14,000, a medium-scale DPIA would cost €34,500, and a large-scale DPIA would cost €149,000. Setting up SCCs for data transfers could entail costs of a similar range. A study of the cost of data protection compliance by large multinational companies found that the cost of compliance can range from $1.4 million to $21.5 million.[71] Implementing SCCs would only be a fraction of that, but this provides an indication of the scale.

For our purposes, we used the broken-down cost of the DPIA to derive an amount for the data mapping exercise. We eliminated the stakeholder engagement and auditing lines, since these activities are not relevant to implementing an SCC, leaving just labour and IT costs. In order to account for the fact that an SCC will be less work than a DPIA we assumed just 50% of the labour costs and retained the full IT costs. However, the European Commission data does not give an estimate for a DPIA done at the micro-firm level. To get a value for micro-firms we took the midpoint in terms of employees for both micro and small, 5 and 25, respectively, and adjusted accordingly. This resulted in the micro average data flows mapping cost being 20% of the average small firm mapping costs.

In addition to the data flow mapping cost, the interviews we conducted revealed that there would almost certainly be a legal component to the activity that every company would need to go through. This could either be external legal costs, as would be the case for almost all micro and small businesses, and very often internal compliance in the case of large companies with in-house legal teams. We were told that data protection officers are rarely responsible for drafting these contracts, which are the job of the legal units. Interviews with lawyers and experts allowed us to estimate the legal costs across the four different scales of business. Practitioners we interviewed informed us that for a company requiring a small number of SCCs the cost would be between £2,000 and £15,000, whereas for a large company the cost would be between £50,000 and £250,000. For the model we estimated that legal costs would be £2,000 for a micro business, £5,000 for a small and £10,000 for a medium. For large businesses, we estimated legal costs of £100,000.

This results in average compliance costs for a business that is affected of £3,000 for a micro business, £10,000 for a small business, £19,555 for a medium business and £162,790 for a large business. These average costs are our estimations of what firms will incur if they wish to set up SCCs to cover EU-UK data transfers.

We have to stress that the lawyers and practitioners we interviewed said that costs were very variable and could go down with repeated agreements and a lower learning curve. For most, the costs of drafting the actual SCC annex were negligible, and the bulk of time and costs came from preparing the information, and negotiating and drafting the contracts. Some sectors, such as medical research, could be more expensive, such as £50,000 to £100,000 for negotiating a data-sharing agreement between a UK university and a US organisation receiving data and tissue samples.

As we discuss in the coming section, a lot of these services will need to be provided in the EU, and there is a huge variation of costs. However, in Sweden, the Netherlands, and Ireland, the costs we were given were similar to the UK or even higher, and these are some of the countries that do a lot of digital business with the UK.

Several lawyers said that a small company could go to a small data protection specialist outfit and get an off-the-shelf document for €/£1,000, but in most cases this is not enough because processor agreements, data documentation, tailored annexes, and privacy notice changes are needed. Once the clients start asking questions, the costs rise.

Having calculated the average costs of compliance, we then needed to define how many UK businesses would be affected by the lack of an adequacy decision, since not all businesses engage in cross-border data flows with the EU. To do this across all sectors we had to use a number of different data sets as proxies, as there is no publicly available data on the number and type of companies who transfer data from the EU to the UK.

The first dataset that we used was DCMS data on the share of UK businesses making website sales by geographical area from 2016. Within that dataset, we used the proportion of firms with orders received from the EU since this would almost certainly result in data being transferred along with the website sale. It is important to note that using this data did not allow us to capture all companies who engage in data transfers between the EU and UK since data can be transferred without requiring a website order. This provides a very conservative estimate of the number of firms implicated.

The DCMS dataset does not cover all sectors of the economy and so we also used the UK Goods and Services trade statistics to enlarge the industries for which we had proxies, allowing us to estimate the number of firms impacted. Here the proxy was the proportion of total exports that EU exports account for between 2016 and 2018. For these sectors we then looked at the data intensity of that sector, as reported by the UN, to allow us to eliminate sectors of the economy that have a very low data intensity. We therefore did not include sectors that were in the bottom quartile of data intensity.

Finally, we manually added in financial services and insurance companies which do not appear either in the DCMS data or the UK goods and services statistics. For these sectors we used two proxies. First, the proportion of economic activities that EU exports account for and second, the proportion of service exports that were digitally enabled in 2018.

Our final assumptions were that every firm we identified would seek to comply with the law. This is not the same as assuming that every company in the UK will comply in the event of no adequacy decision, or even that every company that should comply will, but instead assumes that the number of the firms we conservatively estimated in the model would comply. This is a small subset of all companies in the UK and also a subset of all companies that would need to take action if there is no adequacy decision. Although not everyone is likely to comply from day one, enforcement proceedings are likely to become much more common than they were historically. Over the coming years companies will either have to comply or change their business flows to circumvent the requirements, something which also has a cost to business.

During the interviews that we conducted we consistently heard that although much of the work would need to be done by companies located in the EU, since it is data transfers from the EU to the UK that are affected by the lack of an adequacy decision, much of the cost would be pushed onto UK companies. The size of companies was perceived as the determining factor in this decision, and the role of processors versus controllers is also critical.

> "On the question of who is going to bear the costs, with the US, the UK is bearing the costs as US organisations are bigger." (interview with lawyer)

> "If it is a big company you cannot negotiate and have to use their T&Cs. With SCCs whoever makes the first draft of the documents will take on these and build the terms. Controllers should be leading in theory but there are small controllers and large processors like Salesforce and you use their terms. GDPR responsibility is not the same as power in the relationship. Smaller UK processors will need to take the initiative or lose business." (interview with tech sector lawyer)

> "The driver for processors is to keep customers, so you need to package the information for the controller and be proactive. You need to look at the exact data to populate their risk assessment." (interview with 2nd tech sector lawyer)

> "*Schrems II* says that both parties need to assess but [the] controller is mainly responsible. However, processors need to get ahead; you need to lead the process as the framework for the controller will be heavier and less [of a] fit for your activities." (interview with 2nd tech sector lawyer)

> "UK companies have the main burden as they need to demonstrate compliance if they want EU data. Contracts could be voided anywhere in the EU. But there are costs for the EU partners in extra work. SCCs need to be justiciable under EU law which means lawyers in the EU. The City of London has many lawyers with knowledge of EU law, but these work on negotiations not actual legal work." (interview with lawyer)

As there was no clear consensus on figures from those we interviewed, we decided to use a range from 50% to 75% as the percentage of the compliance costs that will be borne by UK companies. Undoubtedly, no adequacy decision will also be negative and costly for many EU companies.

Despite our assumption of full compliance, our economic modelling of the increased cost of doing business, estimated at between £1 billion and £1.6 billion in total, is very conservative. In reality, the overall costs to business in the event of no adequacy decision are likely to be much higher. This is for three reasons.

First, we do not factor in additional compliance costs beyond setting up SCCs, such as those caused by Article 71 of the Withdrawal Agreement, which would require the complex separation of datasets in the event of no adequacy decision, or the GDPR's representative obligation. Also, some large firms may opt for the much more expensive BCRs.

Second, our assumptions on the average costs of setting up SCCs, as well as the number of companies affected, are conservative. For the average costs we always used figures at the lower end of the estimate ranges given during our expert interviews. When estimating the number of companies impacted, we used proxies that informed us about the lower bound. In many cases, the costs are likely to be higher, and a far greater number of companies are likely to be affected.

> "Some sectors never sign SCCs, e.g. individual researchers have informal agreements on data sharing without lawyers. Right now, this is kind of okay but with Brexit you will need written agreements, involving lawyers, which will have added costs. Now, the problem is that trivial transfers will require a legal basis." (interview with lawyer)

Finally, our model does not factor in the consequences of the *Schrems II* judgement, which could eventually lead to a radical increase in the cost of setting up SCCs by forcing a legal analysis of UK surveillance, redress mechanisms, and human rights compliance. Furthermore, if the use of SCCs for EU-UK transfers becomes vulnerable, this could lead to major economic disruption.

In the following section we explore the potential economic impact beyond the increased costs of business due to new compliance requirements.

6.1 INCREASED RISK OF GENERAL DATA PROTECTION REGULATION FINES

Beyond the obligations of being a good corporate citizen, the main reason why companies comply with data protection legislation is to avoid any potential fines that could be levied for non-compliance with the regulations. GDPR fines can be up to €20 million, or 4% of the firm's worldwide annual revenue in the preceding financial year, whichever amount is higher.

As outlined above, without an adequacy decision, all businesses in the UK that engage in data transfers with the EU will have an additional operational obligation to make sure these transfers are compliant. Such compliance obligations mean that there is an increased risk of GDPR fines. EU DPAs may investigate firms which engage in EU-UK data transfers post-Brexit and issue fines if those transfers are not lawful. Interviewees were clear that they expected EU data exporters to try to transfer financial liability for any fines incurred due to non-compliance with the GDPR on the part of the exporter caused by non-compliance with the SCC by the importer. This would even be the case where the non-compliance was forced upon the UK importer by UK law, such as the Investigatory Powers Act.

Therefore even if we do not see a notable rise in actual fines, which is what we expect in the short-term, it may be the increased risk of GDPR fines coupled with the transfer of liability that will have an impact on the UK economy. This would likely have knock-on effects for trade, investment, and other business decisions. It should also be noted that in addition to the risk of fines there is also a reputational risk for companies who are visibly seen to be avoiding or not complying with data protection legislation.

Data transfers have not been a big focus or priority for DPAs, who have been reluctant to investigate and enforce this issue. In fact, we are aware of only two fines issued by a DPA due to a non-compliant international data transfer, one by the French DPA and the other by the German DPA. In 2007, the Commission Nationale de l'Informatique et des Libertés (CNIL), the French DPA, fined Tyco Healthcare €30,000 for transferring human resources data to the US unlawfully.[72] We are aware

of no cases in which a DPA reviewed the use of SCCs and issued an enforcement fine for non-compliance.

However, in this domain, the past is not a great predictor of the future. After *Schrems II* and the invalidation of the EU-US Privacy Shield, data transfers is now top of the data protection agenda. The EDPS has forcefully stated that there must be a "meaningful before and after *Schrems II*".[73] Other DPAs have also taken a tough line. Most of the EU lawyers we talked to expected EU DPAs to take a tougher line on enforcement in this area and that this would drive companies to seek compliance.

Furthermore, the activism driven by Max Schrems, None of Your Business (NOYB) and others will impact the focus of regulators, who are obliged to respond to complaints. We do expect to see citizens and groups challenging the basis of international transfers of personal data with local DPAs and judicial systems. We therefore anticipate that these private actions will force national DPAs to ultimately take a more vigorous approach to enforcing compliance of international data transfers. After all, the threshold for using SCCs has become much more stringent, and activists will want to test the limits of this.

In this context, it would be very surprising to not see more investigations, suspensions, and fines linked to non-compliant data transfers. Furthermore, when DPAs investigate a company for one reason, such as a data breach, they can also audit their data transfers, even if this is not the focus of the investigation. Unlawful data transfers could potentially exacerbate fines for other matters.

UK firms are likely to get caught up in this from 2021 onwards. Theoretically, a company which on 31 December 2020 transfers data from the EU to the UK can do so without any administrative or legal obligations.[iii] That same company could be subject to fines on 1 January 2021 for completing exactly the same data transfer, if the UK has not received an adequacy decision. Realistically, if there is no adequacy decision, enforcement will not come instantly. EU DPAs, many of whom are quite pragmatic – and exceptionally under-resourced – will likely give businesses many months, if not years, to adapt to the new legal reality. Although there will be no official grace period if there is no adequacy decision, there will be a de facto grace period, during which enforcement on EU-UK data transfers simply does not happen.

As such, do not expect fireworks on 1 January 2021. However we should expect enforcement actions to increase over time, especially once it is clear that the UK will not be the recipient of an adequacy decision and the EDPB has issued an opinion.

The UK leaving the one-stop-shop mechanism further increases the risk of GDPR fines and increases the administrative burden faced by many UK businesses. All EU and EEA countries benefit from the one-stop-shop mechanism, which means that businesses operating in more than one EU country only have to liaise with and report to one DPA. Furthermore, in cases involving the data of citizens from multiple EU member states, the company can only be fined by one DPA, generally the lead supervisory authority.

Non-EEA companies, such as those from the UK post-Brexit, cannot benefit from the one-stop-shop mechanism. This is irrespective of whether the UK is granted an adequacy decision. The practical implications of this is that from January 2021, UK firms could face a regulatory double jeopardy. They could be fined by multiple EU DPAs for the same case of non-compliance. They could also be fined by the ICO and EU DPAs for cases involving the data of both UK and EU citizens. They will also face the administrative burden of having to potentially liaise with several DPAs, as well as the ICO, instead of just one lead supervisory authority. This means both an increased cost of doing business and an increased risk of GDPR fines.

There is a risk that UK companies will simply carry on as before. One of our interviewees explained that a UK entity receiving data without documentation may be processing personal data unlawfully. It would also have contractual liability as a processor, but the controller has the main responsibility in the EU. However, if this happens at volume it will depend on the bandwidth of the ICO and also their relationship with EU DPAs to tackle the problem.

For some lawyers consulted, the main enforcement risk will come less from the ICO and rather from contractual action. For example, a German

iii Assuming that they are currently compliant with GDPR obligations.

controller targeted by their DPA will try to pass on the liability to its UK processor. As noted earlier many experts expect liability to be transferred contractually as part of the SCC. Data risk will become a more significant liability and will affect the value of companies.

One of the lawyers we interviewed raised concerns about companies voiding their business insurance by making the false claim that they are GDPR compliant, which is a standard question.

It is important not to overexaggerate the extent of enforcement risk. Although there is now more heat on the issue of data transfers, and EU DPAs will likely respond accordingly, the hype surrounding the entry into force of the GDPR in 2018, and widespread business concerns about fines, was overblown. Furthermore, the enforcement risk is greater for large, multinational companies, who are much more likely to be the target of investigation (and which are also more risk averse and compliant).

Overall, privacy activists, advocates, and even EU officials have been very disappointed with GDPR enforcement levels, and this may well continue. However, it could only take one European DPA out of over 40 to declare a UK SCC invalid and cause huge commotion. As we discuss in the next section, perceptions of risk can have an impact on a company's behaviour even without widespread enforcement action.

7. WIDER ECONOMIC IMPACTS BEYOND COMPLIANCE

This section outlines the wider economic implications of the UK not receiving an EU adequacy decision. We have not performed economic modelling, or undertaken empirical research, to estimate the scale of these impacts. However, we have interviewed dozens of policymakers, data protection practitioners, business groups, and academics, and there was widespread consensus that no adequacy decision would impact the economy in these ways. These points are also supported by the (limited) literature on the value of data flows, outlined earlier.

No adequacy decision is highly likely to have a negative impact on the volume of international data transfers between the EU and the UK. The increased compliance costs, costing businesses at least £1 billion, and the increased risk of GDPR fines and regulatory double jeopardy, will have knock-on effects. Taken together, this could lead to a reduction in EU-UK digital trade, as it is a concrete non-tariff barrier. Also, this could impact the cost benefit analyses of investors seeking to grow or establish businesses in the UK. Finally, businesses may consider or execute the relocation of some infrastructure, functions, or personnel outside the UK.

We do not seek to estimate the level of impact on these additional factors in this report; this was not possible given the limited time and data currently available. A number of factors make it very hard to estimate the wider economic impact. As well as there being no widely accepted methodology to calculate the value of data and cross-border data flows, there is also the complexity of disentangling the impact of not getting adequacy with the wider economic impact of Brexit and the Covid-19 pandemic. Indeed, economic indicators like foreign direct investment (FDI) and exports are likely to be significantly impacted by a myriad of other factors. Disentangling and calculating the importance of different variables, like data flows, on these indicators, is beyond the scope of this report. We will therefore only elaborate these impacts in narrative form, drawing on our interviews and literature review.

7.1 REDUCTION IN EU-UK TRADE AND DIGITAL TRADE

The additional compliance costs, as well as the increased risk of fines, represent new non-tariff barriers to EU-UK trade. The Institute for Government states that "with the exception of a few sensitive products where tariffs remain high, it is non-tariff barriers that are the real impediment to international trade today."[74]

The following scenarios are all plausible if there is no adequacy decision, with negative consequences for EU-UK trade levels.

Many UK firms, especially start-ups and SMEs, supply services to EU firms, including large multinationals. Those EU firms may no longer want to trade with the UK firm, which could hurt UK exports. Instead, they may opt to work with an EU-based competitor, as this does not require the setting up of costly data transfer mechanisms and entails no risk in terms of complying with data transfer rules. One technology business leader we interviewed stated:

> "Over time, EU companies will prefer to keep data in Europe." (interview with technology business executive)

Alternatively, the EU firm could demand a lower price from the UK firm, to factor in the increased compliance cost and risk. This could be particularly damaging for the UK's data centre sector, which has a leading position in the EU.[75]

Similarly, many UK firms buy products and services from EU firms. Those EU firms may increase their costs to factor in the increased compliance cost and risk. This could be particularly problematic for start-ups and SMEs that rely on critical SaaS and cloud computing services. It is plausible that the costs could increase and that UK firms have less choice in the market. For example, Amazon Web Services (AWS) are likely to automatically update their contracts with UK companies. If they incur extra administrative costs, then it is likely that they will seek to recoup the costs from those companies.

The uncertainty surrounding SCCs exacerbates these dynamics. For example, if the European Commission suggests or explicitly says that the UK system does not meet the standards of EU law, then EU data exporters might be loath to set up SCCs with UK partners. Given the increasing likelihood of challenges and suspensions to SCCs post-*Schrems II*, not to mention the risk of enforcement action, setting up EU-UK SCCs in this scenario might be perceived as too risky.

Also, EU-based companies might use the situation as a marketing opportunity to attract new customers on the basis that there are no restrictions on data flows. Such moves have been seen post-*Schrems II*, whereby EU cloud service provides are making the case that the US cloud 'hyperscalers' should not be used by European companies, as they cannot protect data from US government surveillance. The US cloud industry has pushed back, with plans to create an EU Cloud Code of Conduct.[76]

Although we believe that overall, the impact of no adequacy decision will be to reduce EU-UK digital trade, there will also be opportunities under such a scenario. UK-based companies that feel like they are being squeezed by their EU negotiating partners or being overcharged may seek to relocate their business within the UK. This could mean that in some circumstances the reduction in EU-UK digital trade will be relocated domestically. We would expect this small boost to the economy to mitigate some of the impact of EU companies withdrawing some of their business.

These impacts will not be felt as a sharp shock on 1 January 2021 but instead will be felt over time as thousands of EU and UK businesses make decisions about which companies in which countries to partner with and transfer data to. Some of these decisions by EU and UK companies to relocate will have been part of business strategies separate to the issues raised in this report. However, in other cases the additional non-tariff barrier, along with the forecast risk, along with the uncertainty regarding the legal status of SCCs, could tip the balance in favour of an EU company dealing with another EU company rather than seeking to partner with a UK company. Over time we expect this to lead to reduced trade between the EU and UK.

Although we cannot predict the precise scale of the impact, we know that EU-UK digital trade is crucial for the economy. Experimental ONS data shows that £77.8 billion of services exports to the EU, and £40.1 billion of imports, could be "potentially digitally delivered",[77] and therefore potentially undermined by data flows disruption. More than 80% of financial services, telecoms, IT, insurance, and pensions exports are delivered digitally.[78]

Similarly, DCMS has stated:

> "Imports and exports of both goods and services heavily depend on the free flow of personal data between the UK and the EU. EU personal data-enabled services exports to the UK were worth approximately £42bn (€47bn) in 2018, and exports from the UK to the EU were worth £85bn (€96bn)."[79]

DCMS applied the "UN definition of digitally deliverable services (DDS)" to ONS data. Given that the UN definition (UNCTAD) covers a lot of non-personal data, this could be a high figure, but it gives an idea of the scale of the economic activities at risk.

ONS data shows that the UK exported £120 billion of services to the EU in 2019 and imported £92 billion,[80] with some 50% of those exports comprising financial and business services. As the UK will allow unrestricted UK-EU data transfers, it can be assumed that the impact of adequacy will be felt more strongly in the UK services export sector than in imports.

No adequacy decision is effectively no-deal for data flows, meaning the EU and UK will interact as the EU does with most other third countries. The Centre for European Reform (CER) has stated:

> "If the composition of UK services supplied to the EU matched those to the rest of the world, we estimate that financial services exports to the EU (minus insurance and pensions) would be around 60% lower. The export of insurance and pension services would be 19% lower. Business services (including law, accountancy and professional services) exports would be 10% lower."[81]

Interestingly, we were told by UK business representatives that the financial services sector is more concerned about no data adequacy than a loss of 'passporting', not least due to the potential hit on exports.

E-commerce would also be affected. According to government estimates, in 2018, 7.5% of UK businesses with 10 or more employees made website sales to EU countries.[82] Existing e-commerce statistics cannot identify the monetary value of UK cross-border e-commerce trade.

The UK is the second largest services trading partner with the EU after the US, accounting for some 20% of the bloc's share.[83] Even if a fraction of those exports is lost, this could translate to many billions of pounds. The hope would be that some would be replaced by trade with the US and other non-EU countries, but this may not always be possible. The UK government estimates that a future FTA with the US could increase UK GDP in the long run (over 15 years) by between 0.07% and 0.16% depending on the degree of liberalisation. This is equivalent to an increase of £1.6 billion or £3.4 billion compared to its 2018 level.[84] These calculations are based on having a zero-tariff FTA with the EU, but under less favourable conditions the assumption is that more trade would be redirected to the US. There is already evidence that UK companies are shifting exports of goods away from the EU.[85]

The impact could disproportionately fall on start-ups and SMEs without ample resources. A survey by Deloitte of Indian businesses shows that without EU adequacy the outsourcing sector dealing with the EU concentrates around large businesses, as SMEs cannot handle the costs of compliance with the GDPR and data transfer rules.[86]

An additional problem may come simply from the perception that the UK has a more complicated and riskier regime. An EU study on barriers to data flows within the EU before the GDPR came into force found:

> "[…] widespread misinterpretation of the legal framework governing cross border data flows […] 62% of respondents claimed to be aware of formal legal restrictions that prevent you from transferring data to other EU countries. However, they were unable to give any examples."[87]

This hints that the perception of the barriers to data flows may be higher even if measures are put in place in lieu of adequacy, causing problems for UK firms seeking to trade with the EU. One leading lawyer we interviewed claimed:

> "Data protection officers and boards might have a negative emotional reaction to the idea of sending data to the UK post-Brexit." (interview with lawyer)

We also have to make a special mention of Northern Ireland. The level of digital integration of the Northern Ireland border has received little attention but according to Irish lawyers it could be a huge issue if a digital border appears. During our interviews we heard that some experts consider that if the UK diverges from the GDPR and Irish companies cannot send data to Northern Ireland, some have even argued that this could lead to breaches of the Good Friday Agreement. Northern Ireland relies heavily on banking support call centres, which are data intensive and require the build-up of databases of EU citizens.

7.2 REDUCED INVESTMENT (DOMESTIC AND INTERNATIONAL)

The introduction of compliance requirements which raise the cost of doing business and increase the risk of regulatory enforcement and even regulatory double jeopardy – which are also new non-tariff barriers to EU-UK trade – will likely render the UK a less attractive investment destination and could restrict the investment capacity of UK-based firms.

The investments most at risk would be those where a domestic or international company wants to use the UK to provide products and services to the EU, or to act as a European hub, because these would be most likely to be affected by the change in regulatory environment for EU-UK data transfers.

Take for instance the example of a company thinking of investing in building a new data centre in the UK. The data sector is a real UK success story. However, even though some data centres are built to meet a purely domestic market, most in fact provide the infrastructure that enables digital exports and services, all possible thanks to international data flows.

Each new data centre is estimated to contribute between £397 million and £436 million GVA per year to the UK economy.[88] However, as a recent techUK report notes, one of the reasons for the success of the industry is "the UK has long been regarded as an attractive destination for inward investors, especially as a location for multinationals to site their regional HQs at a gateway to the European market."[89] Given the significant capital investment required to set up a data centre, anything that increases costs, including compliance costs, or that creates additional risk and uncertainty, as is the case with the current adequacy and SCC regimes, means that new investment in this critical and economically beneficial sector could easily reduce over time, especially where those data centres are destined to serve the EU market.

Although we would expect investment to drop for companies matching this profile, we would also expect there to be opportunities for domestic and international investment in products and services destined to serve the local UK market.

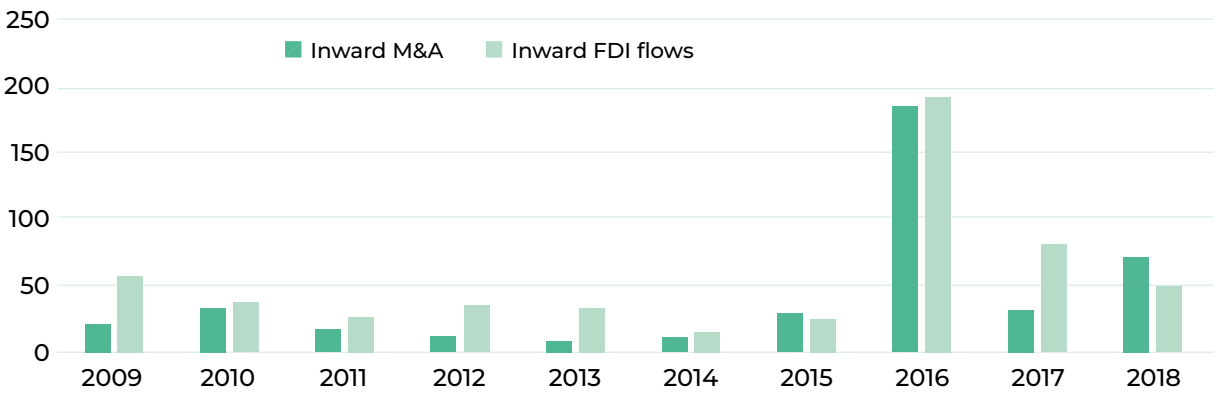
We cannot provide a reliable estimate for the extent to which investment levels will be impacted by no adequacy decision, but it is a point which consistently came up in our interviews. Also, the World Economic Forum highlights that restricting cross-border data flows has negative consequences for investment.[90]

Technology business groups we interviewed noted that their biggest concern with no adequacy decision was the prospect of reduced investment into their sectors. Furthermore, the general uncertainty over data flows and SCCs, even if there is an adequacy decision, was highlighted as a factor which would deter investment into the UK. As cross-border data flows underpin virtually all activities in the digital economy, the psychological impact on investors of no adequacy decision could be significant.

FDI is defined as 'investment in an enterprise operating in a foreign economy where the purpose is to have an 'effective voice' in the management of the enterprise, i.e. owning 10% or more of a company.'[91] Inward FDI measures investments made in the UK from another country.

Many economists have argued that Brexit will have a negative impact on the UK's FDI levels. For example, in 2016, economists from the London School of Economics (LSE) predicted that Brexit would reduce FDI inflows to the UK by 22%.[92] Also, there is a body of evidence on the positive impact that EU membership, especially the single market, has on FDI. One recent study by University College London (UCL) economists, who compared national FDI levels before and after EU membership, found that EU membership increases inward FDI levels by between 50 and 60%.[93]

FIGURE 4: UK INWARD MERGERS AND ACQUISITIONS ACTIVITY AND FDI FLOWS, 2009-2018 (£BILLIONS)



Sources: ONS and House of Commons Library

However, the evidence thus far is mixed as can be seen from the numbers in Figure 4. Although FDI levels in 2017 and 2018 were much lower than 2016, they were also higher than before 2016, which was an outlier year for inward FDI flows. As a percentage of GDP, FDI levels in 2017 and 2018 were actually higher than every year from 2009 to 2015. The House of Commons Library notes that the "discernible effects of Brexit on inward FDI flows are to date, mixed", and that this can be interpreted as either showing the UK remains an attractive investment destination despite the Brexit-related uncertainty, or that the fall in the value of the pound has boosted investment.[94]

To further complicate the picture, in EY's 2020 FDI Attractiveness Survey, the conclusion was that the UK performed strongly on FDI in 2019. The UK "surged ahead of its European counterparts in digital tech, attracting 432 projects, 30% of the European market."[95] EY also states that "analysis of changes in the UK's project origins over the three years since the 2016 referendum shows that the UK has been able to rebalance its investment to compensate for a decline in EU-originated projects."[96]

Brexit has therefore not (yet) had the decisively negative impact on inward FDI levels that many economists predicted. It would thus be naïve to predict that no adequacy decision will have a major impact on overall FDI levels.

However, the UK is exceptionally good at attracting investment to its digital technology sectors. Irrespective of the scale of impact, anything which undermines this strength is negative for the economy. We are certain that the uncertainty over data flows, as well as the increased compliance costs and non-tariff barriers to trade, will have some impact on investment decisions.

According to Tech Nation, 2019 was a record year, with £10.1 billion invested in UK technology companies. This was a 44% increase from the £6.3 billion invested in the sector in 2018.[97] It would be unfortunate for anything to undermine this success story.

7.3 RELOCATION OF BUSINESS FUNCTIONS, INFRASTRUCTURE, AND PERSONNEL OUTSIDE THE UK

Another potential effect of not getting an adequacy decision could be that multinational businesses decide to relocate specific business functions, infrastructure, and personnel outside the UK.

To be transparent, this is the economic impact we are least certain about, and the available evidence is limited. Nonetheless, it was consistently raised in our interviews as a possibility. Also, there is some anecdotal evidence that this has already happened, when services firms were preparing for no-deal Brexit in 2019.[98] However, one city lawyer we interviewed said that "although many firms and clients have talked about relocating, not many have done so". But another lawyer said that "relocation is a big issue. We are hearing from clients, particularly big EU firms, that they are moving out of the UK."

An Institute of Directors survey found that 29% of businesses could shift some of their operations because of Brexit, a figure raised to almost 50% of information technology firms.[99]

There is wider international evidence of relocation to ease data protection compliance. An empirical survey of Japanese firms on the effects of the GDPR, at the time when the country obtained an adequacy decision from the EU, found that more than 30% of multinational enterprise groups changed the location of their data processing and storage to affiliates located in the EU.[100]

One German financial services firm we interviewed said that they had moved their data centre / Cloud centre outside of the UK, because of the Brexit-related uncertainty. They decided to streamline all data processing in one EU cloud in Amsterdam. They confirmed that there are many big European multinationals that have done the same or will do so in the future. For large firms seeking to streamline data processing in one European data centre, keeping data in the UK may no longer make sense, and may be perceived as risky. This could have knock-on effects for the UK's strong data centre and cloud computing industry.

Companies with UK subsidiaries could easily move data processing to the EU. We were given the example of the retailer H&M, although we have not been able to confirm this independently. EU lawyers consulted mentioned various sectors that they knew were directly affected, particularly services such as such as online recruitment assessment platforms, where the UK is a big player because of the English language.

Irish data protection lawyers we interviewed mentioned that other threatened sectors could be insurance and re-insurance as you need personal information to assess risks and London is the global hub. Also, bulk financial products like debt and mortgages contain personal details of people.

> "It may be easier to just move out of London and open an office in Frankfurt or Dublin like Morgan Stanley and others." (interview with lawyer)

> "If I work with a UK system integrator that has an Indian subsidiary, it may be easier to deal with India directly." (interview with lawyer)

EU SMEs were seen as particularly at risk of moving business elsewhere:

> "They don't like cross-border. Even VAT is already an issue. The first time you look at new issues, there is a temptation to drop them." (interview with lawyer)

Restrictions on cross-border data flows will not just impact where companies store data. Virtually every business function of a multinational company, such as human resources, product development, and customer service, depends on seamless cross-border data flows. This means, for example, that product development teams in one jurisdiction may need to transfer personal data to engineering teams in other jurisdictions, in order for standard work to be done. These transfers are not even noticed, as the end result of remote access to data stored elsewhere is embedded so deeply in an organisation's daily work and 'multinational plumbing'. However, without these seamless data transfers, that remote access to data could be undermined, and it may be that multinationals either have to replicate business functions in different jurisdictions, which is costly, or they will streamline business functions in fewer jurisdictions, which could lead to relocation out of the UK.

Given that multinationals can most likely easily absorb the cost of setting up SCCs, such relocations of business functions would probably only be considered if the use of SCCs for EU-UK data transfers became unviable.

One option to moving would be maintaining parallel technical systems. This was mentioned in some interviews as not viable in most cases except for some critical situations. For example, Irish lawyers explained that they believe the Irish DPA, the Data Protection Commission (DPC), will eventually block Facebook's US transfers in some 18 months' time after the *Schrems II* ruling. They estimate the cost to Facebook of duplicating US processing capacity in the EU will be some $3 billion but think it is still worth it for the company.

8. CONCLUSION

We are confident that failing to secure an adequacy decision will have a negative economic impact, with many organisations dealing with the EU requiring between £3,000 and £162,000 in extra compliance costs. This will add to a significant cost to firms of between £1 billion and £1.6 billion, but will also have a wider economic impact, most likely negative, on EU-UK trade levels, inward investment to the UK, and the relocation of business operations outside the UK. We have not tried to calculate the exact economic impact in this report, because of our limited resources, the great level of uncertainty, and the lack of available data. Our first recommendation for the UK government is that:

1. The government should make relevant data and modelling tools available to support empirical research on the social and economic impacts of data protection, digital trade, and the value of data flows, in order to improve the quality of public policy and democratic engagement in these areas.

The combination of a potential no-deal Brexit, coupled with the developing Covid-19 pandemic, means that business and the economy can ill afford more cost, complexity, and risk. Although the adequacy decision is in the hands of the European Commission, the UK government still has a large part to play.

All parties hope that the outcome of the last few years of Brexit negotiations will be a comprehensive partnership agreement. This will be an important achievement of huge social and economic significance. Without a wider agreement on the future relationship, adequacy will be very hard to attain.

Equally important for adequacy will be to continue reviewing the national security and surveillance framework in light of the recent CJEU rulings we discuss in the report.

2. The government should update its published 'Explanatory Framework for Adequacy Discussions' considering the issues raised by the *Schrems II* and *Privacy International* cases.

The UK government has expressed a commitment to maintaining a world-class data protection system and remaining broadly aligned with the EU's GDPR, while developing its own "pro-growth data rights regime", as explained in the National Data Strategy. To have the best chance of obtaining adequacy, the UK should consider demonstrating how it will maintain a regulatory level playing field with the EU on data protection, both domestically and in its trade agreements:

3. The government should further explain how the changes to the UK's data protection regime outlined in the National Data Strategy, designed to promote growth and innovation, will also strengthen and enhance the rights of UK and EU citizens.

4. The government should consider the impact of future trade agreements on data protection, and carefully review the trade-offs involved when liberalising cross-border data flows with different countries.

The UK government should also strengthen measures to support business if the UK fails to secure an adequacy decision. We recommend that the UK government should:

5. Continue to raise awareness of the risks and costs of a lack of adequacy within the business community, both inside the UK and in the EU.

6. Provide simple, practical tools, including information on additional safeguards, to enable UK organisations to continue to use SCCs, given the issues raised by *Schrems II*.

7. Set aside funds to ensure that struggling UK businesses, especially SMEs, can afford to comply with the new requirements.

The main conclusion of our report is that no adequacy decision has the potential to be a contributing factor which undermines the competitiveness of key UK services and digital

technology sectors, which have performed extremely strongly in recent years. It is worth restating just how vital the digital economy is for the UK. Over the last eight years, the digital technology sector global value added (GVA) has increased by 43%, from £104.2 billion in 2010 to £149 billion in 2018, accounting for 7.7% of the UK economy. DCMS data shows that growth in the sector is nearly six times larger than growth across the economy as a whole, indicating that it will become increasingly important in the years ahead, including for the post-Covid recovery.[101]

ENDNOTES

1 Information Commissioners Office. (2020). *Information rights at the end of the transition period - Frequently Asked Questions.* Retrieved from https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/information-rights-at-the-end-of-the-transition-period-frequently-asked-questions/

2 Korff, D. & Brown, I. (2020). *The inadequacy of UK data protection law Part One: General inadequacy* Retrieved from https://www.ianbrown.tech/wp-content/uploads/2020/10/Korff-and-Brown-UK-adequacy.pdf

3 Tossini, J. (2020). *The Five Eyes – The Intelligence Alliance of the Anglosphere.* UK Defence Journal. Retrieved from https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/

4 Stolton, S. (2020). *UK to diverge from EU data protection rules, Johnson confirms.* Euractiv. Retrieved from https://www.euractiv.com/section/digital/news/uk-to-diverge-from-eu-data-protection-rules-johnson-confirms/

5 Lester, S. & Ikenson, D. (2020). *Core Principles for a U.S.-UK Free Trade Agreement.* Cato Institute. Retrieved from https://www.cato.org/blog/core-principles-us-uk-free-trade-agreement

6 Association of British Insurers. (2020). *Written evidence submitted by Association of British Insurers (FRE0047).* Retrieved from https://committees.parliament.uk/writtenevidence/7810/default/

7 *Maximillian Schrems v Data Protection Commissioner.* (2015). Case C-362/14 Court of Justice of the European Union.

8 *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties.* (2020). Case C-311/18 Court of Justice of the European Union.

9 European Commission. (2020). *Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection.* Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

10 Solove, D. (2020). *Schrems II: Reflections on the Decision and Next Steps.* Retrieved from https://teachprivacy.com/schrems-ii-reflections-on-the-decision-and-next-steps/

11 Since all BCRs need to be registered with DPAs, a cursory look at those from the major DPAs shows that there are very few. By default, this must mean that most transnational companies are using SCCs internally.

12 Information Commissioner's Office. (2018). *What are the substantial public interest conditions?* Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions/

13 European Data Protection Board. (2020). *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems.* Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en

14 Patel, O and Lea, N (2020). *EU-US Privacy Shield, Brexit and the Future of Transatlantic Data Flows*, UCL European Institute Policy Paper. Retrieved from https://www.ucl.ac.uk/european-institute/sites/european-institute/files/privacy_shield_brexit_and_the_future_of_transatlantic_data_flows_1.pdf

15 Privacy International. (2020). *Press release: Ruling by EU's highest court finds that UK, French and Belgian mass surveillance regimes must respect privacy, even in the context of national security.* Retrieved from https://www.privacyinternational.org/press-release/4205/press-release-ruling-eus-highest-court-finds-uk-french-and-belgian-mass

16 Privacy International. (2020). *Press release: Ruling by EU's highest court finds that UK, French and Belgian mass surveillance regimes must respect privacy, even in the context of national security.* Retrieved from https://www.privacyinternational.org/press-release/4205/press-release-ruling-eus-highest-court-finds-uk-french-and-belgian-mass

17 Johnson, B. (2020). *UK/EU relations: Statement made on 3 February 2020.* Retrieved from https://questions-statements.parliament.uk/written-statements/detail/2020-02-03/HCWS86

18 UK government. (2020). *National Data Strategy.* Retrieved from https://www.gov.uk/guidance/national-data-strategy

19 European Data Protection Supervisor. (2020). *EDPS Opinion on the opening of negotiations for a new partnership with the UK.* Retrieved from https://edps.europa.eu/sites/edp/files/publication/20-02-24_opinion-eu-uk-partnership_en.pdf

20 BBC News. (2020). *Northern Ireland Secretary admits new bill will 'break international law'.* Retrieved from https://www.bbc.co.uk/news/uk-politics-54073836

21 Jelinek, A. (2020). *European Data Protection Board letter to EU parliament on UK/US Trade Agreement.* Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf

22 Global Justice Now. (2019). *Leaked papers from the US-UK trade talks: A guide to the revelations.* Retrieved from https://www.globaljustice.org.uk/news/2019/nov/27/leaked-papers-us-uk-trade-talks-guide-revelations

23 UK Government (2020). *Draft working text for a comprehensive free trade agreement between the United Kingdom and the European Union.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/886010/DRAFT_UK-EU_Comprehensive_Free_Trade_Agreement.pdf

24 European Commission. (2018). *Horizontal provisions for cross-border data flows and for personal data protection.* Retrieved from https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf

25 UK government. (2020). *UK Japan Comprehensive Economic Partnership.* Retrieved from https://www.gov.uk/government/collections/uk-japan-comprehensive-economic-partnership-agreement

26 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.* (2014) Joined Cases C-293/12 and C-594/12. Court of Justice of the European Union.

27 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others.* (2016). Joined Cases C-203/15 and C-698/15. Court of Justice of the European Union.

28 Privacy International. (2020). *Press release: Ruling by EU's highest court finds that UK, French and Belgian mass surveillance regimes must respect privacy, even in the context of national security.* Retrieved from https://www.privacyinternational.org/press-release/4205/press-release-ruling-eus-highest-court-finds-uk-french-and-belgian-mass

29 Patel, O and Lea, N (2020). *EU-US Privacy Shield, Brexit and the Future of Transatlantic Data Flows*, UCL European Institute Policy Paper. Retrieved from https://www.ucl.ac.uk/european-institute/sites/european-institute/files/privacy_shield_brexit_and_the_future_of_transatlantic_data_flows_1.pdf

30 *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties.* (2020). Case C-311/18 Court of Justice of the European Union.

31 Solove, D. (2020). *Schrems II: Reflections on the Decision and Next Steps.* Retrieved from https://teachprivacy.com/schrems-ii-reflections-on-the-decision-and-next-steps/

32 Patel, O. (2020). The end of Privacy Shield spells trouble for Brexit Britain. *WIRED.* Retrieved from https://www.wired.co.uk/article/privacy-shield-future

33 techUK & Frontier Economics. (2017). *The UK Digital Sectors After Brexit*, p.10. Retrieved from https://www.techuk.org/images/programmes/DataCentres/techUK_Frontier_Economics_-_The_UK_Digital_Sectors_After_Brexit_January_2017.pdf

34 House of Commons Library. (2020). *Statistics on UK-EU trade.* Retrieved from https://commonslibrary.parliament.uk/research-briefings/cbp-7851/

35 UNCTAD (2020). *First draft of the UNCTAD Manual for the Production of Statistics on the Digital Economy.* Retrieved from https://unctad.org/system/files/official-document/dtlict4d2019-1203_Manual_en.pdf

36 Cambridge Econometrics. (2020). *Understanding and measuring cross border digital trade.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885174/Understanding-and-measuring-cross-border-digital-trade.pdf

37 UNCTAD. (2019). *Digital Economy Report 2019: Value creation and capture.* Retrieved from https://unctad.org/system/files/official-document/der2019_en.pdf

38 Bukht, R. & Heeks, R. (2017). *Defining, Conceptualising and Measuring the Digital Economy.* Development Informatics Working Paper No. 68. Retrieved from SSRN: https://ssrn.com/abstract=3431732 or http://dx.doi.org/10.2139/ssrn.3431732

39 Calvino, F. et al. (2018). *A taxonomy of digital intensive sectors.* OECD Science, Technology and Industry Working Papers No. 2018/14. Retrieved from https://doi.org/10.1787/f404736a-en

40 OECD. (2018). *Toolkit for measuring the digital economy.* Retrieved from https://www.oecd.org/g20/summits/buenos-aires/G20-Toolkit-for-measuring-digital-economy.pdf

41 UNCTAD. (2019). *Digital Economy Report 2019: Value creation and capture.* Retrieved from https://unctad.org/system/files/official-document/der2019_en.pdf

42 UCTAD. (2020). *Global e-commerce hits $25.6 trillion - latest UNCTAD estimates.* Retrieved from https://unctad.org/news/global-e-commerce-hits-256-trillion-latest-unctad-estimates

43 Zhang, L. & Chen, S. (2019). *China's Digital Economy: Opportunities and Risks.* International Monetary Fund Working Paper 19/16. Retrieved from https://www.imf.org/en/Publications/WP/Issues/2019/01/17/Chinas-Digital-Economy-Opportunities-and-Risks-46459

44 Cambridge Econometrics. (2020). *Understanding and measuring cross border digital trade.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885174/Understanding-and-measuring-cross-border-digital-trade.pdf

45 OECD, IMF, & WTO. (2017). *Handbook on Measuring Digital Trade.* Retrieved from https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade-Version-1.pdf

46 Meltzer, J. & Dollar, D. (2020). *The global competition to govern digital trade.* Dollar & Sense Podcast. Brookings Institute. Retrieved from https://www.brookings.edu/wp-content/uploads/2020/10/DollarAndSense_Transcript_Meltzer_CompetitionToGovernDigitalTrade.pdf

47 Cambridge Econometrics. (2020). *Understanding and measuring cross border digital trade.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885174/Understanding-and-measuring-cross-border-digital-trade.pdf

48 Nguyen, D. & Paczos, M. (2020). *Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective.* OECD Digital Economy Paper No. 297. Retrieved from https://www.ospi.es/export/sites/ospi/documents/documentos/Measuring_the_Economic_Value_of_Data.pdf

49 Nguyen, D. & Paczos, M. (2020). *Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective.* OECD Digital Economy Paper No. 297. Retrieved from https://www.ospi.es/export/sites/ospi/documents/documentos/Measuring_the_Economic_Value_of_Data.pdf

50 OECD. (2020). *A Roadmap toward a common framework for measuring the digital economy.* Report for the G20 Digital Economy Task Force. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/publications/OECDRoadmapDigitalEconomy2020.pdf

51 McKinsey Global Institute. (2016). *Digital Globalization: The new era of global flows.* Retrieved from https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx

52 Tharakan, A. & Patnaik, S. (2015). *Strong dollar hurts Akamai's profit forecast, shares fall.* Retrieved from https://www.reuters.com/article/us-akamai-tech-results-idUSKBN0NJ2IV20150428

53 Nguyen, D. & Paczos, M. (2020). *Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective.* OECD Digital Economy Paper No. 297. Retrieved from https://www.ospi.es/export/sites/ospi/documents/documentos/Measuring_the_Economic_Value_of_Data.pdf

54 Ferracane, M., Lee-Makiyama, H. & Van der Marel, E. (2015). *Digital Trade Restrictiveness Index.* European Centre for International Political Economy. Retrieved from https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf

55 Ferencz, J. (2019). *The OECD Digital Services Trade Restrictiveness Index.* OECD Trade Policy Papers, No. 221. OECD Publishing. https://doi.org/10.1787/16ed2d78-en

56 Ferracane, M., Kren, J. & Van der Marel, E. (2018). *The cost of data protectionism.* VoxEU. Retrieved from https://voxeu.org/article/cost-data-protectionism

57 OECD. (2019). *Data in the Digital Age*. Retrieved from https://www.oecd.org/going-digital/data-in-the-digital-age.pdf

58 US Department of Commerce. (2020). *U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows.* Retrieved from

https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and

59 European Commission. (2020). *Study on economic values of data flows.* Retrieved from https://ec.europa.eu/digital-single-market/en/news/study-economic-values-data-flows

60 Department for Culture Media and Sport. (2018). *DCMS Sectors Economic Estimates 2018 (provisional): Gross Value Added.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/863632/DCMS_Sectors_Economic_Estimates_GVA_2018.pdf

61 Department for Culture Media and Sport. (2018). *DCMS Sectors Economic Estimates 2018: Trade in Services.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/863862/DCMS_Sectors_Economic_Estimates_2018_Trade_In_Services.pdf

62 Patel, O. (2020). *Data adequacy, Brexit and the implications for professional and business services firms.* House of Lords EU Services Sub-Committee inquiry p.4. Retrieved from https://committees.parliament.uk/writtenevidence/7972/default/

63 FSB. (2019). *Destination Digital: How small firms can unlock the benefits of global e-commerce.* p.8. Retrieved from https://www.fsb.org.uk/resources-page/destination-digital-report-pdf.html

64 UK Government (2020). *Using personal data in your business or other organisation after the transition* period. Retrieved from https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation-after-the-transition-period

65 European Data Protection Board (2020). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.* Retrieved from: European Data Protection Board. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

66 Stolton, S. (2020). *Don't expect new EU-US data transfer deal anytime soon, Reynders says.* Euractiv. Retrieved from https://www.euractiv.com/section/data-protection/news/dont-expect-new-eu-us-data-transfer-deal-anytime-soon-reynders-says/

67 Duhs, E. (2020). *Complying with data protection law in the UK after the end of December 2020 – a game of three-dimensional chess?* FieldFisher. Retrieved from https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/complying-with-data-protection-law-in-the-uk-after

68 Patel, O. (2020). *Data adequacy, Brexit and the implications for professional and business services firms.* House of Lords EU Services Sub-Committee inquiry p.4. Retrieved from https://committees.parliament.uk/writtenevidence/7972/default/

69 Ibid.

70 European Commission. (2012). *Impact Assessment: Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Retrieved from https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf

71 GlobalScape. (2017). *The True Cost of Compliance with Data Protection Regulations.* Retrieved from https://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf

72 Clarke, O. (2007). Tyco Healthcare France suffers €30,000 data export fine. Retrieved from https://marketinglaw.osborneclarke.com/data-and-privacy/tyco-healthcarefrance-suffers-30000-data-export-fine/

Webster, R. (2016). *Germany - Fines for unlawful EU-US transfer issued by German DPA following invalidation of Safe Harbor* retrieved from https://www.dacbeachcroft.com/es/gb/articles/2016/june/germany-fines-for-unlawful-eu-us-transfer-issued-by-german-dpa-following-invalidation-of-safe-harbor/

73 Buchta, A. (2020). Speaking at European Policy Centre online webinar *The EU-US Privacy Shield: What future for transatlantic data transfers?* 17 September 2020.

74 Institute for Government. (2020). *Non-Tariff Barriers.* Retrieved from https://www.instituteforgovernment.org.uk/explainers/non-tariff-barriers

75 techUK. (2016). *Silver Linings: The Implications of BREXIT for the UK data Centre Sector.* Retrieved from http://www.techuk.org/images/programmes/DataCentres/Silver_Linings_The_implications_of_BREXITv2.pdf

76 EU Cloud COC. (2020). *Cloud Industry Unites to Create Global Standard for Transfer of Personal Data following 'Schrems II' ruling.* Retrieved from https://eucoc.cloud/fileadmin/cloud-coc/files/pressreleases/20200915_press_release_Global_Standard_for_Transfer_of_Personal_Data_following_SchremsII_ruling.pdf

77 ONS. (2018). *All data related to Modes of supply, UK experimental estimates: 2018.* Retrieved from https://www.ons.gov.uk/businessindustryandtrade/internationaltrade/articles/modesofsupplyukexperimentalestimates/2018/relateddata

78 Cambridge Econometrics. (2020). *Understanding and measuring cross border digital trade.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885174/Understanding-and-measuring-cross-border-digital-trade.pdf

79 Department for Digital, Culture, Media and Sport. (2020). *Explanatory framework for adequacy discussions: Section A.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872228/A_-_Cover_Note.pdf

80 ONS. (2019). *09 Geographical breakdown of the current account, The Pink Book.* Retrieved from https://www.ons.gov.uk/economy/nationalaccounts/balanceofpayments/datasets/9geographicalbreakdownofthecurrentaccountthepinkbook2016

81 Lowe, S. (2018). *Brexit and services: How deep can the UK-EU relationship go?* Centre for European Reform. Retrieved from https://www.cer.eu/sites/default/files/brexit_trade_sl_pbrief_6.12.18.pdf

82 Cambridge Econometrics. (2020). *Understanding and measuring cross border digital trade.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885174/Understanding-and-measuring-cross-border-digital-trade.pdf

83 European Commission. (2020). *DG Trade Statistical Guide.* Retrieved from https://trade.ec.europa.eu/doclib/docs/2013/may/tradoc_151348.pdf

84 Department for International Trade. (2020). *UK-US Free Trade Agreement.* Retrieved from https://assets.publishing.

service.gov.uk/government/uploads/system/uploads/attachment_data/file/869592/UK_US_FTA_negotiations.pdf

85 Douch, M., Du, J. & Vanino, E. (2020). *Defying Gravity? Policy Uncertainty, Trade Destruction and Diversion* Aston Business School. Retrieved from https://www.lbpresearch.ac.uk/wp-content/uploads/2020/05/P3-Defying-Gravity-Policy-Uncertainty-Trade-Destruction-and-Diversion-May.pdf

86 Deloitte. (2018). *GDPR Preparedness Survey Report.* Retrieved from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-riks-gdpr-preparedness-survey-report-noexp.pdf

87 Godel, M., Joshi, A., Bond, R., Cabello, J. & Fernandez, D. (2016). *Facilitating cross border data flow in the Digital Single Market.* European Commission DG Communications Networks, Content and Technology. Retrieved from https://ec.europa.eu/newsroom/document.cfm?doc_id=41185

88 CBRE. (2020). *Europe Data Centres Q4 2019.* Retrieved from https://www.cbre.com/research-and-reports/Europe-Data-Centres-Q4-2019

89 techUK. (2020). *The UK Data Centre Sector: The most important industry you've never heard of.* Retrieved from https://www.techuk.org/insights/reports/item/18557-uk-data-centre-sector-overview-2020

90 World Economic Forum. (2020). *A Roadmap for Cross- Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy.* Retrieved from http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf

91 Ward, M. (2019) *Foreign Direct Investment Statistics.* House of Commons Library. Retrieved from https://commonslibrary.parliament.uk/research-briefings/cbp-8534/

92 Dhingra, S., Ottaviano, G., Sampson, T. & Van Reenen, J. (2016). *The impact of Brexit on foreign investment in the UK.* Centre for Economic Performance LSE. Retrieved from https://cep.lse.ac.uk/pubs/download/brexit03.pdf

93 Bruno, R., Campos, N. & Estrin, S. (2020). *The Effect on Foreign Direct Investment of Membership in the European Union.* IZA Institute of Labor Economics. Retrieved from https://www.iza.org/publications/dp/13668/the-effect-on-foreign-direct-investment-of-membership-in-the-european-union

94 Ward, M. (2020). *Foreign investment in UK companies in 2018 and the effect of Brexit.* UK Parliament. Retrieved from https://commonslibrary.parliament.uk/foreign-investment-in-uk-companies-in-2018-and-the-effect-of-brexit/

95 EY. (2020). *How can Europe reset the investment agenda now to rebuild its future: EY attractiveness survey* Retrieved from https://www.ey.com/en_gl/attractiveness

96 Ibid.

97 Technation. (2020). *UK Tech for a Changing World.* Retrieved from https://technation.io/report2020/#10-investment

98 Patel, O. (2020). *Data adequacy, Brexit and the implications for professional and business services firms.* House of Lords EU Services Sub-Committee inquiry p.7. Retrieved from https://committees.parliament.uk/writtenevidence/7972/default/

99 Holmes, E. (2019). *Nearly a third of firms looking overseas due to Brexit.* Institute of Directors. Retrieved from https://www.iod.com/news-campaigns/press-office/details/Nearly-a-third-of-firms-looking-overseas-due-to-Brexit

100 Tomiura, E., Ito, B. & Kang, B. (2019). *Effects of Regulations on Cross-border Data Flows: Evidence from a Survey of Japanese Firms.* The Research Institute of Economy, Trade and Industry. Retrieved from https://www.rieti.go.jp/jp/publications/dp/19e088.pdf

101 Department for Digital, Culture, Media & Sport. (2020) *News story: Digital sector worth more than £400 million a day to UK economy.* Retrieved from: https://www.gov.uk/government/news/digital-sector-worth-more-than-400-million-a-day-to-uk-economy