Oliver Patel, Research Associate and Manager, UCL European Institute – Written evidence (PBS0029)

Introduction

I am a Research Associate and Manager at the UCL European Institute, a non-partisan academic centre which serves as UCL's hub for research, collaboration, and engagement on Europe.

I have conducted academic and policy research on the Brexit negotiations since 2016. For the past two years, I have directed a research project on EU-UK data transfers post-Brexit. My written evidence focuses exclusively on the topic of EU data adequacy and the implications for professional and business services firms. It answers questions 11, 2, 3, and 9 (in that order, as 11 is the most relevant).

The evidence is derived from extensive research, including over eighty stakeholder interviews that I conducted.[1] I am currently conducting qualitative research which assesses the implications for business if the UK fails to attain an EU data adequacy decision.

Executive Summary

- **It is difficult to prove exactly how damaging disruption to EU-UK data transfers would be for services firms.** Empirical research in this domain is lacking and there is no precedent for disruption to previously unrestricted commercial data transfers between two jurisdictions.

- If the UK fails to attain an EU adequacy decision, it will affect services firms in five main ways:
  - **Increased cost of doing business** (due to new compliance requirements)
  - **Increased risk of General Data Protection Regulation (GDPR) fines**
  - **Reduction in EU-UK digital trade**
  - **Reduced investment** (both indigenous and international)
  - **Relocation of business functions, infrastructure, and personnel outside the UK**

- There is **minimal evidence of services firms, especially startups and SMEs, preparing for disruption to EU-UK data transfers**. Many are adopting a 'wait and see' approach, not least due to the upcoming European Court of Justice 'Schrems II' judgement on 16 July 2020.

- The **vast majority of services firms and business representatives want reciprocal data adequacy arrangements between the EU and the UK**. There is also no visible clamour for the UK to diverge from EU data protection standards.

[1] I have published two UCL European Institute policy reports on this topic with Dr Nathan Lea:
- EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows (May 2020)
- EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray? (August 2019)

- The EU-U.S. data transfers dispute is an instructive case study when assessing EU-UK data transfers post-Brexit. This tells us that **although the European Commission may act pragmatically and grant the UK an adequacy decision, it would likely face extensive legal challenges.**
- **There could be a 'grace period' if the UK fails to attain an adequacy decision before the end of the transition period,** if there is substantive evidence of progress.

Question 11. If there were no reciprocal data adequacy arrangements in place between the EU and UK by the end of the transition period, what would the implications be for professional and business services providers?

1. It is difficult to accurately answer this question

1.1. Brexit largely threatens EU to UK data transfers. UK to EU data transfers are not at risk, as the UK government has committed to recognising the EU as 'adequate'. However, it is uncertain whether the EU will grant the UK an adequacy decision. My response therefore primarily focuses on the implications for professional and business services providers of the EU not granting the UK data adequacy.

1.2. The implications for professional and business services providers – and the aggregate impact on the UK economy – of disruption to EU-UK data transfers, has received minimal attention in academic, policy, and political debates. There is very little robust economic data, or other empirical evidence, which highlights the extent to which disruption to EU-UK data transfers will impact businesses and the economy.

1.3. This is partly due to methodological challenges with measuring the value of data flows. This is a well-documented evidence gap in the literature.[2] Much of the evidence in this domain is qualitative, survey-based, or anecdotal.

2. The implications of no EU data adequacy decision for UK businesses

2.1. There are five main ways in which disruption to EU-UK data transfers will impact professional and business services providers (and the wider economy):

[2] Nigel Cory, 'Surveying the Damage: Why We Must Accurately Measure Cross-Border Data Flows and Digital Trade Barriers' (2020), ITIF.

- **Increased cost of doing business due to new compliance requirements**
- **Increased risk of GDPR fines**
- **Reduction in EU-UK digital trade due to new non-tariff barriers**
- **Reduced investment, i.e. both inward investment and domestic investment by UK firms**
- **Relocation of business functions, infrastructure, and personnel outside the UK**

2.2. My research does not prove the extent to which the above phenomena will be caused by disruption to EU-UK data flows alone. There are many aspects of Brexit, and the wider global economic situation and response to COVID-19, which will plausibly lead to similar negative economic consequences. Disentangling these variables is challenging.

3. Increased cost of doing business due to new compliance requirements

3.1. If the EU does not grant the UK an adequacy decision, this does not mean that EU-UK data transfers will stop. The EU cannot switch off the internet, and incredibly large volumes of personal data will continue to be systematically transferred by businesses, irrespective of the legal or political situation.

3.2. However, without an adequacy decision, EU-UK data transfers will need to be covered (i.e. 'papered') by ad hoc legal mechanisms, to be lawful under GDPR. This means that organisations currently transferring data from the EU to the UK, as well as organisations seeking to do so in future, will need to engage in hitherto unnecessary bureaucratic exercises to ensure compliance with EU data transfer rules. This will increase the cost of doing business for all impacted firms.

3.3. The vast majority of businesses would use Standard Contractual Clauses (SCCs).[3] These are template contracts, created by the European Commission, which both parties engaging in an EU-third country data transfer must sign, in order for that transfer to be

[3] European Commission, 'Standard Contractual Clauses (SCC)', accessed 24 June 2020.

lawful. SCCs are the primary mechanism for lawfully transferring personal data to third countries which have not been granted data adequacy status by the EU.

3.4. An SCC needs to be set up to cover each point-to-point data transfer. This will be a massive bureaucratic task for many services firms. Countless businesses engage with, and transfer data to, thousands of different organisations every day. It is commonplace to learn about large services firms needing to set up or update many thousands of contracts with clients and suppliers in the event of no adequacy decision. UCL, which is considerably smaller than some of the large, UK-based services firms, will need to amend up to 5,000 contracts in this scenario.[4]

3.5. When setting up SCCs, the first step is for companies to map their data transfers, which can be a major task in itself. This 'data flow mapping' is necessary because each SCC needs to describe the data which is being transferred, and each data transfer requires a separate SCC. During our interviews, one lawyer 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 was wasted.[5]

3.6. After the data mapping, the company transferring data from the EU to the UK will seek to sign new SCCs with the UK entity. This process is usually smooth. However, it can also be an opportunity for one party to negotiate other aspects of the commercial relationship, such as liability provisions, as SCCs can be inserted into broader contracts.

3.7. Once the SCC is in place, data can flow freely, as the entity in the third country has legally committed to a level of data protection which meets EU standards. However, by this stage, the damage to business has already been done, as the process of data mapping, and then implementing, negotiating, and signing SCCs, can be extremely costly and burdensome, due to the extensive legal fees and administrative labour involved.

3.8. This will negatively impact both UK and EU services firms. For example, many UK firms operate across the EU and transfer data back to subsidiaries and clients in the UK. These firms will need to spend lots of money setting up SCCs. Also, many UK services firms

[4] UCL 'Brexit Update', 11 October 2019.

[5] Research interview with data protection lawyer (June 2020).

buy or sell services to EU-based firms, which inevitably entails transferring data. They would also need to spend more money on compliance, i.e. through setting up and signing the necessary SCCs with the EU firms.

3.9. It is important to note that setting up SCCs could be a straightforward and cheap exercise for some firms, especially if they engage in a relatively small number of EU-UK data transfers. Also, the costs could probably be quite easily absorbed by most large and well-resourced multinational services firms.

3.10. Also, some large, multinational services firms will have already set up Binding Corporate Rules (BCRs), which are an alternative solution for EU-third country data transfers. BCRs are a legal mechanism, requiring approval from the relevant EU data protection authority (DPA), to facilitate data transfers within a company or group of companies. Once in place, they require the entire organisation or group to adhere to EU-approved data protection standards. They are almost exclusively used by large corporations operating in multiple jurisdictions.

3.11. Companies seeking to use BCRs to lawfully transfer data from the EU to the UK post-Brexit will have – or should have – already set up BCRs, as the prohibitively expensive process can take years.

4. Increased risk of GDPR fines

4.1. Businesses comply with data protection law to avoid being fined, because of both the financial and reputational damage which this entails. This is why many businesses will invest significant resources in ensuring that EU-UK data transfers are 'covered' by legal mechanisms like SCCs or BCRs in the event of no adequacy decision.

4.2. Before Brexit, firms transferring data from the EU to the UK did not have to worry about data protection enforcement action due to unlawful data transfers, whereas now they do. For example, if a UK-based firm which operates across the EU does not set up the necessary SCCs for a series of data transfers, they could be fined. This additional aspect of GDPR which many services firms may have to comply with increases the risk of GDPR fines.

4.3. Historically, there has been minimal DPA enforcement action targeting unlawful EU-third country data transfers. Due to this, it is plausible that many firms, especially startups and SMEs, will have a

higher appetite for risk, i.e. they would be willing to risk transferring data without implementing SCCs, because they view the prospects of enforcement action as low. One major fine on these grounds could be a game changer, as it would spur lots of companies into action, especially startups and SMEs who may have had a higher tolerance for risk.

4.4. Brexit also increases the risk of GDPR fines even if the UK does receive an adequacy decision, because the UK is leaving the one-stop-shop enforcement mechanism. This mechanism ensures that companies operating across the EU only have to deal with, and can be fined by, the DPA of their 'main establishment'.

4.5. After the transition period, services firms operating and transferring data across the EU will be at risk of regulatory double jeopardy, whereby they could be fined by both the ICO and the relevant EU DPA(s) for the same data protection wrongdoing. Receiving two or more fines for the same activity could significantly increase the level of GDPR fines. There will also be increased administrative work for UK-based firms, in terms of cooperating with multiple DPAs. In sum, many services companies will have to work with – and could be fined by – several EU DPAs post-Brexit, if their 'main establishment' is not in the EU.[6]

5. Reduction in EU-UK digital trade due to new non-tariff barriers

5.1. The factors which increase the cost of doing business, outlined above, would represent new non-tariff barriers to UK services exports and EU-UK digital trade.

5.2. For example, many UK firms, especially startups and SMEs, supply services to EU firms, including large multinationals. Those EU firms may no longer want to trade with the UK firm. 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. 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.[7]

5.3. Similarly, many UK services firms buy products and services from EU firms. Those EU firms may increase their costs in order to factor

[6] Travers Smith, 'Brexit, your business and data: processing European personal data' (March 2020).
[7] techUK, 'The implications of Brexit for the UK Data Centre Sector' (2016).

in the increased compliance cost and risk. This could be particularly problematic for startups and SMEs which rely upon critical SaaS and cloud computing services. It is plausible that the costs could increase and that UK firms have less choice in the market.

6. Reduced investment (both indigenous and international)

6.1. Disruption to EU-UK data transfers will also have a knock-on effect on levels of investment, both indigenous and international. The increased cost of doing business, the negative impact which this could have on EU-UK trade, and the risk of regulatory double jeopardy, will render the UK a less attractive investment destination and could restrict the investment capacity of UK-based firms. It is proven that restricting cross-border data flows has negative consequences for investment.[8]

7. Relocation of business functions, infrastructure, and personnel outside the UK

7.1. Another knock-on effect could be the relocation of functions, infrastructure, and personnel outside the UK. There is much anecdotal evidence that this has already happened, when services firms were preparing for no-deal Brexit in 2019.

7.2. For example, large multinational firms might move their data centre infrastructure out of the UK, so that data can keep being transferred across borders without additional compliance costs. Similarly, companies hosting data with cloud service providers, including services firms who rely on them to host their own customers' data, have been moving their data from UK instances to EU instances. This has a knock-on effect on revenue and jobs.

Question 2. What are the UK's different professional and business services sectors' key priorities for the future UK-EU relationship?

8. The services sector wants reciprocal adequacy decisions

8.1. There is widespread consensus among the business community regarding the importance of the UK attaining an adequacy decision from the EU and the importance of both EU-UK and UK-EU data transfers continuing to be unrestricted. Major business groups like

[8] World Economic Forum, 'A Roadmap for Cross Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy' (2020), p. 8.

the CBI[9] and techUK[10] have called for this.

8.2. I am unaware of any business or business organisation which does not want reciprocal EU and UK adequacy decisions and the continuation of the data transfers status quo.

9. There is no clamour from business for UK divergence from GDPR

9.1. Despite Prime Minister Boris Johnson stating that the UK will 'in future develop separate and independent policies in areas such as […] data protection',[11] there is no evidence of substantial business demand for policy change in this area. There are no notable campaigns or lobbying efforts whereby UK businesses are clamouring for divergence from EU data protection standards post-Brexit.

9.2. On the contrary, many firms want the UK to remain aligned with GDPR, so that they do not have to comply with two different regulatory systems and to increase the chances of the UK attaining and retaining an EU adequacy decision. Although this could change over time, especially as EU law evolves.

Question 3. What preparations (if any) have UK professional and business services providers made, or planned to make, ahead of the end of the transition period?

10. Many businesses are unaware of this issue or adopting a 'wait and see approach'

10.1. Data protection and Brexit is currently low down on the register of corporate risk priority, not least due to the impact of COVID-19. Preparation for disruption to EU-UK data transfers entails firms mapping data flows and setting up alternative transfer mechanisms, like SCCs and BCRs. There is minimal evidence that this is happening on the widespread scale that could be required after the transition period. However, it is fair to say that SCCs can be set up in a few months, so waiting is not always irrational.

10.2. Very few startups and SMEs have prepared for the different eventualities, preferring to wait and find out how the EU-UK

[9] Toby Helm, 'No-deal Brexit will 'instantly disrupt' UK's role as £174bn global data hub' (2019), The Guardian.
[10] techUK, 'No interruptions: Options for the future UK-EU data-sharing relationship' (2017), p. 10.
[11] Boris Johnson, 'UK / EU relations: Written statement' (February 2020).

negotiations unfold.[12] Large multinational firms and public companies, which are generally more risk averse and have legal and compliance teams, have undertaken much more preparatory work. Much of this was done before the previous Article 50 deadlines, in 2019.

10.3. Evidence indicates that levels of business awareness regarding this issue is relatively low. For example, in November 2019 the Federation of Small Businesses (FSB) found that small firms are generally not aware of SCCs.[13] Also, one regional Chamber of Commerce, which represents many digital startups and SMEs, said that the issue of data transfers post-Brexit has not once been raised by a member since 2016.[14]

11. The Schrems II case is key

11.1. On 16 July the European Court of Justice (CJEU) will deliver its judgement in the 'Schrems II' case.[15] This case concerns the validity of the EU's SCC system. Although it primarily concerns Max Schrems' complaint regarding Facebook Ireland's use of SCCs to transfer data from the EU to the U.S., the case has much wider relevance.

11.2. Businesses do not want to set up new data transfer mechanisms before this case is concluded, as there are several potential scenarios regarding SCCs which could emerge on 16 July:

Future of SCCs (potential scenarios)	**Implications for EU-UK data transfers**
SCCs are invalidated globally.	Existing SCCs would no longer be valid, and the European Commission would produce new model contracts, which firms would have to implement.
SCCs are upheld, but the CJEU requests amendments or annulments to specific provisions.	The European Commission would have to amend SCCs, meaning that firms would need to update existing SCCs or potentially implement new ones.
SCCs are upheld, but data protection authorities are instructed to	Firms would continue setting up SCCs as now, although these might be

[12] Research interviews with several businesses and trade associations.
[13] FSB, 'Destination Digital: How small firms can unlock the benefits of global e-commerce' (2019), p. 8.
[14] Research interview with a regional Chamber of Commerce CEO (June 2020).
[15] European Court of Justice, case C-311/18 - Facebook Ireland and Schrems.

investigate and suspend them on a case-by-case basis.	viewed as riskier, leading to enhanced corporate due diligence and scuppered deals.
SCCs are upheld with no further comment.	Firms would continue setting up SCCs as now, perhaps at greater scale with the legal uncertainty mitigated.

11.3. Irrespective of the outcome in this case, SCCs are vulnerable. Complaints, investigations, and potentially suspensions of SCCs used to transfer data from the EU to the UK post-transition are likely to increase in the coming years. This implicates UK businesses if there is no adequacy decision, especially 'telecommunications operators' most affected by Investigatory Powers Act notices (e.g. ISPs, social media websites, email, and cloud service providers).[16]

Question 9. What lessons, if any, can be learnt from the EU's existing trade agreements with other third countries including services, or negotiations on trade in services?

12. The long-standing dispute over EU-U.S. data transfers is an instructive case study for assessing EU-UK data transfers post Brexit

12.1. The EU-U.S. 'Privacy Shield' framework facilitates unrestricted commercial data flows across the Atlantic. Over 5300 firms use Privacy Shield and it underpins transatlantic digital trade. Privacy Shield's predecessor, the EU-U.S. 'Safe Harbour' framework, was agreed in 2000 and invalidated by the CJEU in 2015, following a complaint by Max Schrems, provoked by Edward Snowden's revelations of U.S. mass surveillance.[17]

12.2. Privacy Shield is currently at risk of invalidation due to unresolved concerns regarding U.S. government access to EU citizens' data, for law enforcement and national security purposes. Privacy Shield could be invalidated in the Schrems II judgement, or a future CJEU judgement. There is minimal scope for a political or legal resolution due to a clash between U.S. national security and surveillance laws

[16] Graham Smith, 'The UK Investigatory Powers Act 2016 – what it will mean for your business' (2016) Bird & Bird.
[17] Oliver Patel and Nathan Lea, 'EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows (2020), UCL European Institute, pp. 9-10.

and programmes, and EU data protection standards and fundamental rights.

13. The UK will face very similar problems to those of the U.S, but the European Commission could also act pragmatically

13.1. Despite the well-documented concerns with the UK's surveillance, data protection, and human rights system, it is highly plausible that the European Commission will grant the UK an adequacy decision. The history of EU-U.S. data transfers demonstrates that the Commission acts in a flexible and pragmatic way to preserve unrestricted data transfers with important economic partners. Indeed, the U.S. does not even have comprehensive, federal privacy legislation, but received a partial adequacy decision (i.e. Privacy Shield).

13.2. However, this analysis must be heavily caveated. Data adequacy is at the whim of the wider EU-UK future relationship negotiations. Also, the judgement in the Schrems II case could render it virtually impossible for the Commission to grant the UK an adequacy decision. Furthermore, a Privacy Shield type arrangement would be a severe downgrade from the EU-UK data transfers status quo.

13.3. If the European Commission does not grant the UK an adequacy decision before the end of the transition period, but there are indications that it may yet be forthcoming, EU DPAs could declare an unofficial 'grace period', whereby EU-UK data transfers can continue without any risk of enforcement action. This is what happened after Safe Harbour was invalidated in 2015, as U.S. and EU companies scrambled to implement alternative transfer mechanisms.

13.4. Both Safe Harbour and Privacy Shield have been challenged on multiple legal fronts. If the UK attains an adequacy decision from the Commission, it will also be very likely to face extensive legal challenges. There are several organisations which pursue strategic litigation to uphold data protection standards, including None of Your Business (led by Max Schrems), La Quadrature du Net, and Privacy International. These organisations will view any UK adequacy decision as a weakening of EU fundamental rights standards and will immediately seek to invalidate it. Any legal challenge could take many years to conclude, potentially shrouding EU-UK data transfers in clouds of legal uncertainty.

13.5. Because of this potential legal uncertainty, a UK adequacy decision will be viewed by many businesses as an unstable arrangement. These businesses may invest in setting up SCCs or BCRs as a backup option, even if they are not legally necessary. Some large organisations which engage in EU-U.S. data transfers do not actually use Privacy Shield as it is viewed as too unstable.

13.6. If the UK does not attain an adequacy decision, and the global system of SCCs is invalidated in the Schrems II case, or critical SCCs used to transfer data from the EU to the UK post-transition are suspended by DPAs due to concerns with UK surveillance law, EU-UK data transfers could become severely restricted.

14. There is minimal precedent for disruption to EU-third country data transfers

14.1. There is virtually no precedent for major disruption to previously unrestricted commercial data transfers between two jurisdictions. No one knows exactly what it would entail if the UK failed to attain an adequacy decision, and there is minimal empirical research on this topic.

14.2. The invalidation of EU-U.S. Safe Harbour is perhaps the only similar example, but Privacy Shield was implemented only a few months later. In the intervening period, data transfers did not stop, and although companies directed significant resources towards data protection compliance (i.e. setting up data transfer mechanisms), there were no major economic implications nor any enforcement action.

14.3. It is important not to exaggerate the economic effects of the UK not attaining an EU adequacy decision. It would be very damaging for some services firms, especially those conducting significant volumes of digital trade with the EU (i.e. if a firm has thousands of clients, they may need to update thousands of contracts). Specific sectors like cloud computing, software, and data centres will be particularly affected. However, although the main effects on business of increased compliance costs and reduced investment would be damaging, this issue alone is not going to cripple the economy or lead to a halt in EU-UK digital trade, as many firms will be able to absorb these costs.

June 2020