Dr Karen Mc McCullagh, Lecturer in Law, University of East Anglia – Written Evidence (DAT0008)

House of Lords European Affairs Committee

Evidence on Inquiry into data adequacy and its implications for the UK-EU relationship

Dr Karen Mc McCullagh, Lecturer in Law, University of East Anglia

I am a Lecturer in Law at the University of East Anglia. My research specialism is information rights, including data protection. This evidence is based on an analysis of all adopted adequacy decisions and available commentary on failed applications under Directive 95/46/ec (Directive) and the General Data Protection Regulation (GDPR) in the forthcoming journal article "A critical evaluation of the evolution of EU data protection adequacy assessments and their effectiveness as a mechanism for promoting EU data protection standards as the global norm," *Common Market Law Review*. It also draws upon these publications: Mc Cullagh, K., Post-Brexit UK Data Protection: Staying the Course or Charting a New Direction? In *Data Protection and Digital Sovereignty Post-Brexit.* Celeste, E., Costello, R. Á., Harbinja, E. & Xanthoulis, N. (eds.), (Bloomsbury, 2023) and Mc Cullagh, K., Post-Brexit data protection in the UK – leaving the EU but not EU data protection law behind, in Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics. González Fuster, G., Van Brakel, R. & de Hert, P. (eds.), (Edward Elgar Publishing, 2022)

I would be happy to provide the Committee with a copy of the listed publications.

Responses to Questions

1.What is your assessment of the existing adequacy arrangement underpinning data flows between the UK and the European Union?

a. What is your assessment of the value of the EU's adequacy decisions to UK organisations?

The EU-UK adequacy decision is valuable to UK organisations in three respects:

(a) the *necessity* of and *economic value of personal data transfers* – by way of example, in 2022, the UK exported £146 billion of services to the EU and imported £121 billion, resulting in a trade surplus of £25 billion. Financial services and other business services (which includes legal, accounting, advertising, research and development, architectural, engineering, and other professional and technical services) and made up 54% of all UK service exports to the EU.[1] These services generate and rely upon huge volumes of personal data in their operations (e.g., in the form of customer records, behavioural, profile, and transactional data). Also, the European Commission has strategically sought to encourage key trading partners to engage with the adequacy process in the hope of creating a club or network effect by fostering stronger trading relations with each other. This strategy worked as "countries with EU adequacy decisions exhibit an increase in digital trade [of] between 6-14 percent," primarily because they "exhibit greater digital trade among each other.[2]

(b) *minimisation of compliance burden* – an adequacy decision is the least administratively burdensome mechanism for facilitating transfers. If the GDPR adequacy decision was not renewed UK-based entities would be forced to rely on other transfer mechanisms e.g., consent, standard contractual clauses or binding corporate rules, all of which would be expensive and administratively burdensome (estimated £1-1.6billion).[3] For many of the UK's Small and Medium-Sized enterprises, it would be a cost they could not bear.

(c) *Brussels effect & reputational value* - multi-national companies operating in both the EU and UK are likely to advocate for continued compliance with the GDPR and related adequacy decision because of the Brussels effect, that is, the regulatory 'race to the top' whereby the most stringent standard (GDPR) has an appeal to companies operating across multiple regulatory environments because it minimise their compliance costs. Given the relative (small) size of the UK market compared to the EU market, businesses will advocate for continued compliance with the GDPR standard. Customers and individuals in the UK increasingly value high levels of data protection and are unlikely to call for a lower standard of protection.[4]

---

[1] House of Commons Library, Statistics on UK-EU Trade, (11 May 2023) https://researchbriefings.files.parliament.uk/documents/CBP-7851/CBP-7851.pdf

[2] Ferracane, M, B Hoekman, E van der Marel and F Santi (2023), "Digital Trade, Data Protection and EU Adequacy Decisions", EUI RSC Working Paper 2023/37.

[3] New Economics Foundation & UCL, "The Cost of Data Inadequacy The Economic Impacts of the UK Failing To Secure An Eu Data Adequacy Decision," <https://www.ucl.ac.uk/european-institute/sites/european-institute/files/ucl_nef_data-inadequacy.pdf>

[4] Mc Cullagh, K., Post-Brexit UK Data Protection: Staying the Course or Charting a New Direction? In *Data Protection and Digital Sovereignty Post-Brexit.* Celeste, E., Costello, R. Á., Harbinja, E. & Xanthoulis, N. (eds.), (Bloomsbury, 2023) and Mc Cullagh, K., Post-Brexit data protection in the UK – leaving the EU but not EU data protection law behind, in Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics. González Fuster, G., Van Brakel, R. & de Hert, P. (eds.), (Edward Elgar Publishing, 2022)

b. How are the General Data Protection Regulation and the Law Enforcement Directive working in practice? What extra costs do they impose on businesses?

One report estimated that implementing the GDPR adversely affected companies through increased compliance costs and reduced demand – asserting that it caused an 8.1% drop in profits and 2.2% dip in sales for affected businesses.[5] At best, the report finding should be viewed as a snapshot of a particular period. The methodology and findings could also be questioned on the basis that in the run-up to the GDPR coming into force some data controllers and processors many have needed to seek legal advice and change their practices to ensure compliance (but for those who already complied with predecessor legislation the changes were not vast), and such costs were 'one-off' not ongoing. Also, the research did seek to measure the positive impacts of GDPR compliance e.g., whether the reputational benefit and customer trust and satisfaction outweighed the compliance costs.

c. How would you assess the overall performance and effectiveness of the Information Commissioner's Office (ICO) as the UK's independent data regulator? Has its work been impacted by decisions on data adequacy?

The ICO is well resourced in terms of funding and staff, and it processes a large volume of complaints. In the past it was weak on enforcement. If, over time, the ICO remained weak on enforcement, such that data subjects lacked enforceable rights and remedies it could become an issue for consideration in future adequacy reviews. Likewise, if proposals in the DPDI Bill had the effect of negating the independence of the ICO, it could become an issue for consideration in future adequacy reviews. Neither are an immediate concern.

2. What are the possible challenges to UK-EU data adequacy regime?

a. **What factors could influence the next European Commission when deciding whether to renew its data adequacy decisions for the UK in June 2025**?

The Commission is required to have regard to the criteria in Art 45 GDPR, EDPB guidance, and CJEU jurisprudence. It will also take account of a latent, non-legal consideration, namely the extensive trade relationship it has with the UK. It will not want to jeopardise that given the economic value of bidirectional personal data flows between the EU and UK. The forthcoming review is therefore likely to highlight the extent to which the UK mirrors the GDPR before outlining known

[5] Chen et al, "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally," The Oxford Martin Working Paper Series on Technological and Economic Change, Working Paper No. 2022-1, <https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf>

deficiencies and calling upon to encourage remediation by the date of the next periodic review.

b. What factors could the Court of Justice of the EU (CJEU) consider if the legality of the EU-UK adequacy decisions were challenged?

The aspect of UK law and practice that is of greatest concern is the powers in the Investigatory Powers Act 2016. Whilst there has been some convergence in ECtHR and CJEU jurisprudence on laws permitting surveillance measures in recent years (In *Big Brother Watch*[6] and *Centrum för Rättvisa v. Sweden*[7] the ECtHR held that "bulk interception is of vital importance to Contracting States in identifying threats to their national security"[8] and "no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power",[9] and in *La Quadrature du Net* the CJEU ruled that the EU law does not preclude indiscriminate data retention measures when Member States can prove legitimate and serious threats to national security, the Court also established a hierarchy of legitimate public interest objectives for which surveillance measures are permissible, if carried out under certain criteria and subject to applicable safeguards.[10] The Commission arguably erred in not explicitly benchmarking UK law and practice against the requirements stipulated in La Quadrature du Net.

Nevertheless, there is an important difference between theoretical risk and actual risk of legal challenge and revocation of the EU-UK adequacy decision. The *theoretical risk* of the adequacy decision being challenged e.g., by Maximilian Schrems, noyb.eu or similar entities is *high* because the adopted decision is deficient, particularly in relation to surveillance and data retention powers. However, complainants are, in my view, more likely to focus their attention on the US Data Privacy Framework on the basis that if the US were required/persuaded through repeated legal challenges to introduce significant changes to its surveillance practice and attendant oversight and redress mechanisms, five eyes' partners such as the UK would be incentivised to introduce similar reforms. As resources are more likely to be invested in pursuing complaints in respect of the EU-US partial adequacy decision than the EU-UK adequacy decision, the *actual risk* of the UK adequacy decision being challenged and invalidated should be regarded as **low**.

In the unlikely event that the EU-UK adequacy decision is the subject of a legal challenge and withdrawn, the Commission would prioritise the scheduling of talks to develop a successor adequacy decision (as it has repeatedly done in respect of the US) because of the economic value of the data flows.

---

[6] Big Brother Watch and Others v The United Kingdom *(Applications Nos. 58170/13, 62322/14 And 24960/15)*
[7] Centrum För Fättvisa V. Sweden *(Application No. 35252/08)*
[8] BBW, para 166
[9] CFR, para 365
[10] C-511/18 - La Quadrature du Net and Others, ECLI:EU:C:2020:791

3. a. **Do you have any concerns about the direction of travel of the UK Government's data policies as set out in the Data Protection and Digital Information Bill, and about the potential for greater divergence from EU data standards?**

My concerns about the DPDI Bill have lessened over time as the most radical proposals have either been removed or significantly watered down. This is a positive development as radical divergence would not only increase the risk of the EU-UK adequacy decision not being renewed in due course, but it could also have the unintended consequence of making the UK a less desirable place to establish a business. The UK has a strong record of attracting tech unicorns (defined as a privately held start-up company with a value of over $1 billion). It is a good 'test bed' for start-ups because of its highly skilled workforce, data centres, and the size of its market. However, any initial competitive advantage of lax data protection rules and less onerous compliance burdens would be quickly lost when a start-up decided to enter the EU market, as it would have to comply with the higher standards in the GDPR when processing data of individuals in EEA Countries. Care must be taken to ensure that the final latest version of the DPDI Bill represents an appropriate attempt by the UK to use the 'white space' in the UK GDPR to 'fine tune' it to the needs of the UK economy and does not do so in a way that jeopardises adequacy.

b. How high is the risk of the European Commission withdrawing its UK data adequacy decisions? What impact would that have and how prepared are businesses or the public sector for such a scenario?

The risk of the Commission withdrawing its UK GDPR data adequacy decision is **low**. It uses the periodic review process to identify shortcomings and set a timeframe for review of progress, e.g., Privacy Shield was reviewed annually when it was in force.

Israel, like the UK, has extensive surveillance and data retention measures. During the review of adopted adequacy decision. The Commission recommended that Israel enshrine in legislation "the protections that have been developed at sub-legislative level and by case law" and observed that Amendment 14 to the Privacy Protection Law, which was being deliberated by the Israeli Knesset, offers an opportunity to implement this recommendation. It did not, however, seek to impose a timeframe for requiring Israel to implement those legislative reforms, or stipulate that it would conduct a future periodic review of Israel's laws within a shorter timeframe to ensure that it passed the proposed legislative measures – perhaps understandable given the Israel-Palestine conflict occurring at the time the review was conducted, but an approach that suggests the Commission is willing to renew adequacy decisions on the strength of proposed

reforms. The approach is appropriate given that all adopted adequacy decisions are now subject to periodic review.[11]

4. **What can be learned from other countries' experience with the adequacy system and engagement with the European Commission's process?**

In theory, adequacy assessments involve the Commission assessing (with input from other EU Institutions e.g., the EDPB and Parliament) whether an applicant third country meets the *legal* criteria in Art 45, EDPB guidance and CJEU jurisprudence. However, the Commission takes account of a latent consideration, namely the actual or potential trading relationship between the EU and applicant third country and gives such considerations equal if not greater weight when deciding whether to make a finding of adequacy. As a result, the Commission often ignores or requires only minimal remediation of identified deficiencies ahead of adoption of an adequacy decision.

My analysis of all adopted adequacy decisions and commentary on failed applications found that the legal criteria are applied most rigorously during the initial assessment. That is when the Commission is most likely to decide not to adopt an adequacy decision. Moreover, the Commission is more likely to adopt a facilitative approach when it already has or is seeking to deepen an existing trading relationship or forge a new trading relationship with the third country, as typified by the experiences of Argentina, Burkina Faso, Morocco and Tunisia. The Commission adopted an adequacy decision in respect of Argentina[12] despite the Art29WP Opinion noting that as the head of the supervisory authority was a political appointment, their independence was not guaranteed and the Data Protection Authority had issued no significant guidance, pursued no enforcement, and issued no sanctions, so its effectiveness could not be fully assessed. By contrast, an adequacy decision was not adopted by the Commission in respect of Burkina Faso, Mauritius, Morocco and Tunisia – the newness of their data protection frameworks and the consequent dearth of case law or decisions through which the operational effectiveness of the national data protection authorities could be assessed were cited as reasons why adequacy decisions could not be adopted in respect of these countries. Normatively, the applicant countries should have been treated in uniform manner, with no finding of adequacy adopted/a conditional finding of adequacy made in respect of all. Yet, the Commission adopted a finding of adequacy in respect of only one of the countries, Argentina - a country it already had a deep trade relationship with.

---

[11] Mc Cullagh, K. "A critical evaluation of the evolution of EU data protection adequacy assessments and their effectiveness as a mechanism for promoting EU data protection standards as the global norm," *Common Market Law Review (forthcoming)*.

[12] European Commission, Commission Decision 2003/490/EC of 30 June 2003 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data in Argentina, *Official Journal L 168, 05/07/2003 P. 0019 – 0022.*

The Commission also adopted an adequacy decision in respect of New Zealand but not in respect of Australia, despite New Zealand law containing deficiencies. Arguably, the Commission did so for strategic reasons – it wanted to harness the club or network effect to extend the global reach of adequacy decisions. By adopting an adequacy decision in respect of New Zealand rather than Australia it limited the risk to its own data protection standards – if New Zealand did not rectify the deficiencies the volume of personal data flows was at that time insignificant compared to the much larger neighbouring economy of Australia.

a. What conclusions do you draw from the European Commission's recent adequacy review of 11 countries and territories?

The Commission engaged in a light-touch review of adopted adequacy decisions. It renewed all adopted adequacy decisions despite many containing identified deficiencies. Although some of the GDPR criteria are more stringent than those in the Directive, the Commission did not seek to impose conditions on renewal and did not seek to impose time frames by which remediation would be complete. For instance, it accepted assurances by Canada and Israel that reforms were in progress, even though the proposed reforms might not come to fruition. The approach is appropriate given that all adopted adequacy decisions are now subject to periodic review.

b. What are the implications for the UK's EU adequacy status if the UK grants its own adequacy decisions to other third countries currently not subject to EU adequacy?

The UK must ensure that the adequacy decisions it adopts cannot be used as a 'back door' to circumvent GDPR adequacy requirements, particularly in respect of onward transfers. Doing so would jeopardise the EU-UK adequacy decision.

Received 3 May 2024