Open Rights Group - Written Evidence (DAT0021)

Open Rights Group response to the House of Lords European Affairs Committee inquiry into data adequacy and its implications for the UK-EU relationship.

Author: Mariano delli Santi
Date: 24 May 2024

0. Open Rights Group welcomes the opportunity to answer to the House of Lords European Affairs Committee inquiry into data adequacy and its implications for the UK-EU relationship. Due to the recent announcement concerning the General Election, and the need to submit this response before its deadline, we will not be able to fully reference the evidence we include in this submission. We therefore remain available, and indeed we encourage to reach out, for any follow up questions you may have.

Question 3a: 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?

1. We find the proposals enshrined of the DPDI Bill regarding international data transfers rather concerning, for the following reasons.

2. The right to data protection is a fundamental right, it allows individuals to retain control over how data pertaining to them is shared and used to take decisions that affect their lives in almost every aspect—from employment to commercial offers to their relationship with the State and local authorities. As digital technologies keep developing and are embedded into every aspect of our lives, the right to data protection becomes a necessary means to assert and protect human rights, individuals' aspirations and societal expectations.

3. The global nature of the Internet means that digital data, including personal data, can be easily moved across geographical boundaries and jurisdictions. If the right to data protection were dependent on where personal data were stored, individuals' rights could be easily circumvented just by transferring this information to a country with lower data protection standards. As such, the International Data Transfers Regime of the UK GDPR constitutes a cornerstone of UK data protection rights, as it ensures that rights and responsibilities established under the law apply regardless of where personal data may be stored.

4. Retaining the high standards the UK has inherited from the GDPR is important from the perspective of EU adequacy: if the UK were to become a country with lower data protection standards than the European Union, this would expose European citizens to the threat of their data being transferred to the UK and then abused by public or

private actors alike. Such a state of affairs is unlikely to remain sustainable in the long term, and would inevitably lead to a reassessment of the adequacy status the UK currently enjoys under EU law.

5. The debate around UK adequacy is underpinned by a broader issue. Low data protection standards, and in particular disproportionate or undemocratic access to personal data by state authorities of third countries, constitute the single and most relevant driver of uncertainty for International Data Transfers and digital trade at large. Abusive practices by US intelligence services has already led to the invalidation of two adequacy decisions between the EU and the US. The United States have recently asserted, in the context of WTO negotiations regarding digital trade, the need to retain regulatory space in data protection matters, and the Biden administration has issued an Executive Order to ban the bulk transfer of personal data to countries of concerns. Several countries have been discussing legislation to ban TikTok from their own country due to the risk that personal data collected by the social media platform could be accessed by Chinese authorities. Several countries have enacted data localisation measures to protect their sovereignty and economic interests.

6. Thus, the barriers to the free flow of data do not originate, as some private interest groups have tried to argue, from regulation, but from the need to protect individuals' data regardless of where they're stored, from national security considerations, and from broader issues related to international relations and the policies and aspirations that different countries may have. Indeed, the regulatory regime of the GDPR may not be perfect, but currently constitutes the framework that best guarantees legal certainty for organisations and individuals alike.

7. Both the UK and the EU GDPR are rights-based regimes. They prioritise the protection of personal data and other relevant rights, and allow such rights to be interfered with insofar this is done proportionately and in the pursuit of another, legitimate aim, in line with the broader system established by the European Convention of Human Rights. However, the DPDI Bill was proposing to politicise these determinations, i.e. making data transfers dependant on the discretionary assessment of the Secretary of State rather than on the existence of effective protections and enforceable remedies against violations to the right of data protection. Such a system would introduce significant uncertainty, as international data transfers could be declared legal or illegal overnight and on the basis of politically-driven decisions, rather than the adherence of the country of destination to required legal and human rights standards. Likewise, the DPDI Bill would have politicised the functioning of the Information Commission, thus allowing the government to interfere with how the law is applied and enforced domestically. This would adversely affect individuals' right to data

protection, legal certainty, and ultimately endanger the UK adequacy decision; thus, it is a policy option that ought not to be considered again.

8. The need to ensure a high level of data protection and proportionate access to data by State authorities has also been recognised by OECD declaration on government access to personal data held by private-sector organisations. In that declaration, OECD countries have agreed in principle to limit public access to personal data according to criteria which are directly drawn from the GDPR. Ultimately, this declaration also stems from the underpinning assumption that legal certainty and the rule of law are essential drivers for commerce and economic growth. Thus, a future government should consider how to build upon existing GDPR standards to reduce political influence and achieve a higher degree of certainty, and should consider the role the UK could play to influence other countries in implementing the standards they have agreed in principle within the OECD declaration.

9. It may be argued that such an endeavour would not only require domestic legislation, but also to exercise external influence and promote alignment in a highly contested policy area. In other words, it is a difficult task at hand. However, the UK has always expressed its aspiration to become a world leader in digital regulation, but they cannot achieve this aim by ignoring the tough questions and sacrifice the rights of its residents for the private, and dubiously legitimate, interests of large technology companies.

Question 1c: 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?

10. The performance of the ICO is notoriously poor and unsatisfactory. In our report concerning the enforcement of data protection during the pandemic, the ICO has demonstrated a lack of independence and willingness to enforce the law, leaving UK residents exposed to several abuses of their personal data. ORG is also going to publish a second report that analyses the performance of the ICO under the tenure of John Edwards: in particular, we found that the new ICO strategy, which prioritises non-legal enforcement means such as reprimands, is failing to provide effective enforcement to individuals who are victims of egregious violations of their rights. We also found that the ICO is failing to enforce the law in critical areas such as online advertisement and artificial intelligence. By doing so, the ICO is not only failing the public, but are diminishing the regulatory influence of the UK internationally.

11. The dysfunctional nature of the ICO constitutes an obvious threat to the protracted existence of the UK adequacy decision. In a hearing before the Civil Liberties Committee of the European Parliament, the

Information Commissioner was vehemently criticised by Members of the European Parliament for his attempt to defend the UK government and their proposed data protection reform, as well as for his attempt to defend his "record" of data protection enforcement. The independence of the ICO and its track record on regulatory enforcement have consistently been identified by EU stakeholders as a major adequacy concerns. The report on the implementation of the EU – UK Trade and Cooperation Agreement also identifies the ICO as an issue.

12. In order to benefit both UK residents' rights and the UK adequacy status, the next government should consider reforming the ICO to make it a Parliamentary appointment, increase its arms-length from the government, and establish a clear legal duty to enforce the law and strong legal redress for individuals who are dissatisfied with how the authority has dealt with their case.

Question 2a: What factors could influence the next European Commission when deciding whether to renew its data adequacy decisions for the UK in June 2025?

13. The European Commission has answered to several questions raised by Members of the European Parliament, either individually or as the Civil Liberties Committee as a whole. These questions concerned the assessment of the Commission regarding the DPDI Bill and its compatibility with EU data protection standards; thus, the answers they gave provide us useful hints as to what the Commission has been looking at.

14. In particular, the Commission has been particularly concerned about the independence of the ICO and its effective enforcement of data protection laws. The Commission has also raised concerns around the impact that delegated legislative powers, and in particular Henry VIII clauses, could have on legal standards for data protection. Finally, the Commission has raised concerns around the threshold individuals need to meet in order to exercise their rights under the GDPR, and the importance for these to remain unconditional and free of charge.

Question 2b: What factors could the Court of Justice of the EU (CJEU) consider if the legality of the EU-UK adequacy decisions were challenged?

15. Existing case-law revolves around government access to personal data held by private sector entities and the independence of EU data protection authorities. However, the CJEU can assess any factor they consider relevant in establishing that the level of protection provided by the UK is "essentially equivalent" to the EU one.

16. Under this government, the main policy concern around personal data seems to have been about making it as easy as possible to access or reuse personal data for whatever reason, and as difficult as possible to challenge such determinations. However, accountability requires clarity as to what are the boundaries that separates a data use from a data abuse. Thus, the policy approach pursued so far by the UK government is incompatible with EU adequacy standards and democratic standards at large.

Question 3b: 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?

17. The risk of the European Commission withdrawing an adequacy decision cannot be quantified, insofar this depends on the degree of divergence the UK may implement with domestic legislative reform. On the other hand, the withdrawal is not the only possible outcome of a review of the UK adequacy decision. For instance, the UK could be asked to separate personal data processing of EU data from the UK counterparts, in a similar manner to the adequacy arrangement between the EU and Japan. This would introduce significant administrative requirements and burdens for UK businesses who want to process EU personal data.

Question 3c: What would be the implications for the continued operation of Part III of the TCA (law enforcement and judicial cooperation on criminal matters)?

18. ORG has heard from several EU stakeholders and officials that divergence from EU data protection standards would endanger the TCA and possibly lead to a "digital Brexit". Data sharing constitutes a necessary mean for the practical functioning of most of the post-Brexit agreements between the EU and the UK, and these were underpinned by the UK alignment with EU data protection standards. In case of regulatory divergence of the UK, there would be the need to renegotiate them.

Question 4a: What conclusions do you draw from the European Commission's recent adequacy review of 11 countries and territories?

19. The UK adequacy status cannot be compared with that enjoyed by other "adequate" countries under the EU GDPR. The UK has deep economic and political ties with the European Union. There is significant cross-border trade in between the two blocks, and several cooperation agreements in matters related to defence, law enforcement, immigration control and defence, among others. The UK also shares an open border with Ireland and is part of the Windsor Framework. These mechanisms

all require data sharing and were negotiated with the understanding that EU and UK data protection standards were aligned. This would amplify the significance and the impact of UK divergence when compared to other countries, making a comparison between the UK and other "adequate" countries a hollow and useless exercise.

Question 4d. If the UK joined the Global Cross Border Privacy Rules system, what impact if any could that have on the UK's EU adequacy status?

20. The Global Cross Border Privacy Rules system establishes legal and due diligence standards that can be enforced against private entities only, and cannot be relied upon to challenge government access or use of personal data. As such, compliance with the CBPR framework will never meet European data protection standards, nor will address any of the issues related to International Data Transfers as explained in our answer to Q3a.

About Open Rights Group

21. Founded in 2005, Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect individuals' rights to privacy and free speech online. ORG has been following the UK government's proposed reforms to data protection since their inception. In June 2022, we organised an open letter signed by a coalition of over 30 organisations that highlighted the failure of the DCMS to properly engage with civil society groups about the proposed reforms, and in March 2023, we delivered a letter signed by 25 CSOs to Michelle Donelan, highlighting our serious concerns with the Government's draft legislation.

22. Open Rights Group remains available for further comments or clarifications at the contact below

Received 24 May 2024