DMA's evidence to the House of Lords European Affairs Committee inquiry Into data adequacy and its implications for the UK-EU relationship

21 May 2024

1. The Data & Marketing Association (DMA) represents around 700 companies across the UK that are involved with marketing activities, including commercial and non-commercial businesses like charities.

2. International data flows are essential to the UK's trade and economic growth. A report published by the Government in July 2023 stated that in 2021, 93% of the UK's service exports were data-enabled[1]. This means that the trusted flow of cross-border data, especially with the EU – the UK's biggest trading partner - is extremely important.

3. The DMA has long believed that it is in the interest of businesses as well as consumers to have high standards in place regarding customer data. Responsible data management is essential to customer trust and business growth.

4. The DMA's leadership has encouraged high standards on data ethics across the business community. Its Code, developed in 2014, sets out principles which underpin GDPR and PECR and is therefore a useful tool to help ensure high levels of compliance. This is useful in the debate around the renewal of the Commission's data adequacy agreement with the UK next year.

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

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

5. The adequacy arrangement between the UK and the European Commission is very important to the UK and the data and marketing industry, as it provides certainty and frictionless trade as regards the cross-border flow of data with the EU which is fundamental to everyday business practice. Without it, companies would face new levels of bureaucracy as they would need to complete Standard Contractual Clauses (SCCs) or Binding Corporate Rules with all the partners in the EU with whom they do business. This would have a direct impact on the UK's trade with the EU bloc which is our biggest trading partner. In 2020, it accounted for 42% of UK exports of goods and services and 50% of the UK's imports[2].

6. The UK has implemented GDPR rigorously and organisations have spent considerable time and investment changing their systems and processes to achieve compliance. The uncertainty created by Brexit and the year-long process involved in the European Commission granting adequacy status to the UK were therefore frustrating and concerning to businesses. The DMA therefore regards it as a high priority to retain the UK's data adequacy agreement.

[1] https://www.gov.uk/government/news/uk-gets-new-status-in-global-data-privacy-certification-programme

[2] https://commonslibrary.parliament.uk/research-briefings/cbp-7593/

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

7. Once companies had put in place the systems they needed to comply with GDPR, the benefits of harmonisation of laws with other countries across the EU, with frictionless access, were apparent.

8. However, the cost to businesses, particularly SMEs, in implementing GDPR when it first came into force were significant. The Secretary of State described this as causing business losses of 8% and costing the UK £23 billion. Others have calculated the losses as being about 2%[3]. The added cost was incurred because the Regulation raised standards of data protection for companies, requiring new administrative processes and business costs. For example, GDPR requires companies to appoint a DPO (Data Protection Officer) and to conduct DPIAs (Data Protection Impact Assessments). It is helpful that the DPDI Bill will lighten the regulatory burden for smaller companies which do not conduct high-risk processing by making them exempt from the duty to keep records and to have a Senior Responsible Individual (previously a DPO).

9. Implementation of GDPR in the UK has misunderstood the legislation. Across the country and across industry sectors, it has become believed that GDPR requires consent to process the data. This is not the case. There are six lawful basis for processing data, including legitimate interests. Recital 4 of GDPR makes it very clear that privacy is not an absolute right but a fundamental right which must be balanced with other fundamental rights, including the right to conduct a business. The new DPDI legislation going through Parliament brings essential clarification to GDPR without risking adequacy.

10. GDPR harmonises rules across the EU and is risk and principles-based. This means that organisations must assess their own processes and strategies with regards to data and take a proportionate approach balancing their legitimate interests with their customer's right to privacy, though the fines, if the ICO gets involved, are very high (up to 10 million euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher). This has led to a great deal of caution as company lawyers often advise a risk-averse approach requiring consent for the data they are processing. This is time-consuming and costly It is also, in many cases, unnecessary as GDPR allows that "Legitimate Interest" can be used, in many cases, as the lawful basis for consent[4].

[3] https://www.gov.uk/government/news/uk-gets-new-status-in-global-data-privacy-certification-programme

[4] Under the "Legitimate Interest" test, the organisation needs to show that it has conducted a "balancing test" to identify the legitimate interest, show the processing is necessary to meet it, and that it is balanced against the rights and freedoms of the data subject.

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?

11. Data adequacy has been important for the ICO as well as for other parties in the UK because it has provided a formal basis for post-Brexit relationships with other data protection authorities.

12. The ICO's standing was impacted by Brexit, as it was no longer able to be part of the European Data Protection Board in which it had played a leadership role, being widely listened to by other data protection regulators. The ICO has had to find new ways of engaging with other DP authorities, with the UK outside the EU.

13. On the whole, businesses find that the ICO is an engaged, constructive and evidence-based data protection authority. However, sometimes it gets it wrong. For example, in February 2020, it took an enforcement decision against Experian requiring them, on grounds of transparency, to write to data subjects whose personal data was on the Open Electoral Register to seek their consent. In our view, this was unnecessary, as it has been the case for many years that legislation (the Electoral Representation of the People Act 2013) permits companies to use personal data on the OER for direct marketing purposes because they have already given their consent.

14. This case has since been going through the legal process which has created years of unnecessary market uncertainty for any organisation using the OER or other public registers. The First Tier Tribunal ruled against parts of the ICO's enforcement notice and recently the Upper Tribunal has conclusively ruled against the ICO, stating that the ICO "exaggerated the harms and ignored the benefits of the processing" contrary to the required principles of proportionality in Recital 4.

15. Although the UTT has now ruled against the ICO, we advocate that the DPDI Bill needs to be amended so as to restore legal and business certainty.

What are the possible challenges to the 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?

16. There are good indicators of what will influence the European Commission from its reports and press releases about adequacy arrangements with other countries.

17. It is clear they will look at a range of factors as part of evaluating whether the UK has continued to be in alignment with GDPR and whether the ICO has taken decisions that demonstrably uphold the principles of GDPR. If the EU updates GDPR, it will expect the UK to bring its own laws in line, so as to retain data adequacy arrangements.

18. The Commission is also likely to consider the impact of any political decisions the Government takes, for example, adherence to the European Convention on Human Rights because data protection is regarded by the EU as a fundamental human right.

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

19. The Court of Justice will have regard to any legal cases that demonstrate that the UK has weakened data protection below the level of GDPR and thereby reduced the fundamental human rights of EU citizens. This needs to be avoided at all costs, as the consequences – as demonstrated by the Schrems I & II cases which invalidated the EU's data adequacy decisions with the US in 2015 and 2020 – can be catastrophic.

c. How would you assess the possible impact of proposed UK rules on automated decision-making and the use of Artificial Intelligence on data adequacy?

20. Clause 14 of the DPDI Bill amends Article 22 of UK GDPR with new Articles 22A-D expanding the use cases in which automated decision-making can be used. In our view, these have no material impact on the rights of individuals. However, the Secretary of State has powers to clarify which cases are to be taken to have "meaningful human involvement" and therefore be contrary to GDPR, and what is or is not to be taken as a significant decision under Article 22A(1)(b((i) and (ii). Whilst this is useful to allow for further developments in AI, there is a potential risk to data adequacy if the resulting decisions create regulatory divergence between the EU and the UK.

What implications, if any, would a no or disrupted UK-EU data adequacy scenario have?

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?

21. The DMA does not believe that the changes proposed in the DPDI Bill affect data adequacy. On the contrary, the amendments made by the Bill to UK GDPR provide some helpful clarifications and interpretations, for example, regarding Legitimate Interest.

22. Obviously, the powers of the Secretary of State to introduce secondary legislation provides the opportunity to update the law in light of market developments, but it also provides a potential risk to adequacy, should the Government decide to reduce data protections at any future time. We are reassured currently that not only the Government but all political Parties understand the importance of not compromising the data adequacy agreement and so we are of the view that this would remain a high priority in the future.

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?

23. There is always a risk in any negotiation and wider political issues or negotiations can get in the way of concluding the deal. However, the DMA is confident that the UK's legal and regulatory framework is sufficiently aligned to the EU's that the risk of the Commission withdrawing its data adequacy decision is low. Whatever minor divergence UK makes in the future, we will be closer to EU standards than any other country who has achieved adequacy After all, as set out in response to question 4(a) below, the Commission's own adequacy review confirms that data protection needs to be comparable but that point-to-point replication of GDPR is not required.

24. Obviously the impact on businesses and the public sector of a withdrawal of Adequacy would be significant. However, in principle, the UK should be well prepared and the Government, with business associations, should raise awareness about the need for organisations to make fallback arrangements, including Standard Contractual Clauses.

25. In addition, in GDPR Article 40, the data protection authorities must encourage trade associations to draw up industry Codes of Conduct. Furthermore, it is accepted in 40.2 that industry associations are best placed to interpret the legislation for their sector "Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation".[5]

26. The DMA has been working on a Direct Marketing Code of Conduct for the UK which is consistent with other Direct Marketing Codes of Conduct approved or in development in Austria, Germany, Italy, Poland and elsewhere. It is intended that these Codes of Conduct will contribute to a harmonized interpretation of GDPR within the EU, and help to demonstrate that the UK's interpretation is consistent with the EU.

27. It is helpful that the DPDI Bill now confirms that a single code of conduct can cover both UK GDPR and PECR considerations.

c. What would be the implications for the continued operation of Part III of the TFCA (law enforcement and judicial cooperation on criminal matters)?

28. Not applicable.

[5] https://gdpr-info.eu/art-40-gdpr/

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

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

29. The adequacy review conducted by the Commission in January 2024 acknowledges that the standard of 'essential equivalence' does not involve a point-to-point replication ('photocopy') of EU rules, given that the means of ensuring a comparable level of protection may vary between different privacy systems, often reflecting different legal traditions." This is important to note as, whatever minor divergences UK makes in the future, we will be closer to EU standards than any other country who has achieved adequacy. Even after the implementation of the DPDI Bill, the UK will remain close to EU in the fundamental principles of GDPR and PECR with both laws remaining in place.

30. Countries such as Argentina and Japan which have achieved Adequacy with the EU have data protection laws that are quite different to the EU's GDPR. This demonstrates that the principle of "essential equivalence" is in place and there is no reason UK should be treated differently, especially because its starting point was the same laws as in the EU.

b. Are there examples of best practice where the UK could learn from in the way other countries approach their data transfer arrangements with the EU?

31. In April 2023, the EU and Japan recently agreed the continuation of their 2019 agreement on data flows following the first review.[6] The Commission's very positive report about the steps taken by Japan to bring its laws closer to the EU's demonstrates that maintaining a close relationship, being open and transparent about changes made in domestic law and why, and the fact Japan has developed Supplementary Rules, give strong pointers about an effective approach. On the basis of the improvements Japan has made, the EU now plans to review the agreement every four years instead of every two[7].

c. 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?

32. If the UK does this, it would be advisable to ensure that the countries to which we grant adequacy status are sufficiently aligned with our own laws and with GDPR that we do not put at risk EU citizens' data collected and processed in the UK.

d. 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?

33. In July 2023, the Government announced that the UK was the first country in the world to get associate status in the Global Cross-Border Privacy Rules Forum. It stated that this would "unlock opportunities for closer collaboration on international

[6] https://commission.europa.eu/news/joint-press-statement-conclusion-first-review-japan-eu-mutual-adequacy-arrangement-2023-04-04_en

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0275

data flows with key global partners" and position the UK "to help shape practical solutions in building a global data transfers system".

34. There are undeniable advantages of this to trade, growth and to the UK's leadership in the world. Many countries involved already have their own adequacy deals with the Commission. However, the UK needs to be alert to countries coming into the forum that do not have adequacy status as this might be of concern to the European Commission.

Conclusion

35. Adequacy is important. Adequacy is not based on having identical legislation but "essential equivalence". The EU should apply the same approach to UK as it has done for all other countries that have achieved adequacy. The UK should not be treated differently just because its starting point was EU data protection laws.