# The Market Research Society – Written Evidence (DAT0016)

## MRS response to the House of Lords data adequacy inquiry

## 1. About the Market Research Society

1.1. The Market Research Society (MRS) is the UK professional body for market, opinion and social research, insight and analytics. MRS is the world's largest and oldest research association, representing 5,000 individual members and over 600 accredited Company Partners in over 50 countries and has a diverse membership of individual researchers within agencies, independent consultancies, client-side organisations, the public sector and the academic community.

1.2. MRS' expertise as the lead authority on market, opinion and social research is recognised around the globe. MRS provides the policy and standards expertise for the UK plus a number of global associations including EFAMRO the European Research Federation and EPHMRA the international healthcare research association. MRS also has close business ties with other research associations around the world via its participation in the Global Research Business Network (GRBN) plus formal agreements with associations in the US, Australia and Japan.

1.3. MRS promotes, develops, supports and regulates standards and innovation across market, opinion and social research and data analytics. MRS regulates research ethics and standards via its Code of Conduct. All individual MRS members and Company Partners agree to regulatory compliance of all their professional activities via the MRS Code of Conduct and its associated disciplinary and complaint mechanisms.

1.4. More information about MRS can be found on the MRS website: https://www.mrs.org.uk/https://www.mrs.org.uk/

## 2. About Market, Opinion and Social Research

2.1. Market, opinion and social research is the systematic gathering and interpretation of information about individuals or organisations using the statistical and analytical methods and techniques of the applied social sciences to gain insight or support decision making. It involves systematic study of different spheres of society, politics, and the economy. Research, insight and analytics stand at the heart of all well-informed commercial, social and political decisions. Insight into what makes a product, business initiative or government policy work is often the hidden – yet defining – factor between success and failure.

It is our sector that provides the deeper intelligence needed for our world today.

## 3. The UK Market, Opinion and Social Research Sector

3.1. There are circa 3,100 active registered businesses in the UK listing market research and opinion polling as their primary activity, and a further 1,700 listing market research and opinion polling as a subsidiary activity.

3.2. The UK research, insight and analytics sector is a great UK success story. The UK is an £9bn market for research and is the second largest research market in the world, second only to the US[1].

3.3. The UK research sector is recognised as leading the way in the development of creative and innovative research approaches including maximising the opportunities afforded by the development of new digital technologies. The methodological issues are explored and debated in the academic journal, the International Journal of Market Research (IJMR)[2].

## 4. Purpose of our Response

4.1. The MRS is responding to the House of Lords Data Adequacy Inquiry, which comes ahead of the upcoming renewal decision to continue allowing the free flow of personal data. Overall, the current data adequacy regime is highly valuable for UK businesses, especially those operating in the digital economy. The existing arrangement also enables congruency between EU and UK legislation and economic relations, which is critical to innovative and effective business across borders, particularly for SMEs.

4.2. However, we are concerned about the lack of clarity in the GDPR concerning the delineation and attribution of controller, joint controller and processor responsibilities. The determination of who is a controller, joint controller, data processor or third party is a question of fact rather than contractual stipulation. It is based on a determination of the purposes and means of the processing, and essentially the level of decision-making power exercised. Essentially, it is up to each party to determine to what extent they are involved, resulting in any of the classifications and subsequently designating themselves accordingly. However, for research activities GDPR is often interpreted in a broad manner which suggests that clients are always the controllers/joint

[1] [1] See Industry size and growth rates: https://www.mrs.org.uk/resources/industry-size

[2] For more information about IJMR: https://journals.sagepub.com/home/mre

controllers because they set any research questions to be answered or 'determine the purposes'. There should be more nuance to the delineation of roles, and it should be considered on a case-by-case assessment, which would be more accurate and reflective of the delineation of responsibility[3].

4.3. We also want to encourage a greater use and appreciation of existing sector and professional Codes of Conducts that are part of an association or a trade body's membership terms. These are an effective means to support and ensure compliance and greater awareness of rules from SME organisations. The MRS Code of Conduct is crucial in helping to protect and regulate first-rate research, insight, and data practice, and sector codes should be more effectively mobilised by the UK Government as a mechanism for compliance.

## 5. Our response

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

- **What is your assessment of the value of the EU's adequacy decisions to UK organisations?**
- **How are the General Data Protection Regulation and the Law Enforcement Directive working in practice? What extra costs do they impose on businesses?**
- **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?**

5.1. The EU's decision to grant the UK data adequacy status following Brexit was highly valuable for British companies, especially those operating in the digital economy. Many UK organisations had already invested significant resources to achieve compliance with GDPR prior to Brexit, making continued free flow of data from the EU crucial to avoid disruption to their operations. The EU remains by far the UK's largest export market, so the adequacy decision allowing the free flow of personal data is extremely important for sectors like market research that rely upon the ability to transfer data between suppliers and clients across international borders.

5.2. Without an adequacy decision, UK companies would face burdensome requirements to implement safeguards like Standard Contractual

[3] https://efamro.eu/wp-content/uploads/2024/05/gpdr5anniversary-edit-CG_KK.pdf

Clauses or Binding Corporate Rules when transferring EU personal data. Likewise, the UK's adequacy decision conferred on the EU meant that costly hurdles for UK businesses seeking to serve European markets and vice versa were minimised with the friction-less continued two-way transfer of data. This is especially important for SME's, which constitute circa 97% of the market research industry, many of which are microbusiness, which need to be able to conduct business without onerous requirements that could inflate their costs significantly. Similarly, as the UK is the second largest research market in the world, with an estimated one third of UK research activity based upon international activities, it is essential for the health of the sector that data movement can occur with minimum disruption.

5.3. The GDPR's key benefit was updating the original data protection directive and harmonising data protection regulation across EU/EEA countries. Being a risk and principles-based legislation, it allows for context in its interpretation and is technology neutral. Organisations have a large degree of autonomy on how they assess and quantify risk too. GDPR also removed the need for controllers to notify DPAs before any automated processing. Additionally, the legislation laid down new responsibilities for data processors and established the data protection authority one-stop-shop. Perhaps more significant was the large fines introduced under GDPR which meant that data protection became a board-level issue.

5.4. However, the GDPR, in solving a number of problems it also created some new ones. In some areas the language is ambiguous and in others the legislation has resulted in unintended consequences. Of course, due to the additional compliance and record keeping requirements it has resulted in additional costs for businesses.

5.5. For example, the GDPR sets out six lawful bases for processing data, where each basis is considered equally valid - yet organisations over-rely on consent as a legal basis. The GDPR's interaction with the e-Privacy directive, whose successor the e-privacy regulation remains in limbo, also creates further complications around the regulation of cookies and other similar technologies. Finally, complying with these requirements imposes significant expenditures on companies that relate to updating data management systems, training staff, hiring data protection officers, and implementing technical measures like consent management platforms.

5.6. Additionally, there is a lack of clarity with regard to the delineation of roles and proportional responsibilities concerning controllers, processors, and third parties. The determination and attribution of the controller, processor, or third-party role has practical implications for the parties involved in complex data processing activities, e.g., a research data chain. Through the attribution of the role, the liability and responsibility for safeguarding the processing of personal data changes as does the ability to exercise control over and determine further uses of the personal data. Under the GDPR, the attribution of this role is depending on the factual involvement of the parties in the processing activities which is then left to the appreciation of the parties involved. It is up to them to determine to what extent they are involved, resulting in any of the classifications and subsequently designating themselves accordingly and ensure that this designation is respected by the other parties in the data chain. However, for research activities GDPR is often interpreted in a broad manner which suggests that clients are always the controllers/joint controllers because they set any research questions to be answered or 'determine the purposes'. There should be more nuance to the delineation of roles, and it should be considered on a case-by-case assessment, which would be more accurate and reflective of the delineation of responsibility[4].

5.7. We have been largely supportive of the aims and objectives of the Data Protection & Digital Information (DPDI) Bill and regard it as a step in the right direction. This is because the DPDI Bill clarifies aspects of GDPR and aims to reduce unnecessary burdens on business without lowering the high standards of data protection that the UK currently enjoys. Additionally, it incorporates "scientific research carried out as a commercial activity" into the definition of scientific research, which is a welcome clarification of the scope of the definition. The new DPDI Bill also upholds necessary safeguards and reduces onerous requirements where market, social or opinion research is conducted for scientific, historical, or statistical purposes.

5.8. We are of the view that the ICO largely remains an effective independent data protection authority despite Brexit. That is not to say it has not been impacted by Brexit as the ICO is no longer a member of the European Data Protection Board. Additionally, the ICO was required to draft new guidance and standard contractual clauses for international data transfers specific to the UK.

5.9. However, we do harbour some concerns over the ICO's recent interpretations of the rules. Particularly when it comes to achieving

[4] https://efamro.eu/wp-content/uploads/2024/05/gpdr5anniversary-edit-CG_KK.pdf

the right balance between the right to privacy, which is not an absolute right, and the right to conduct business (Recital 4, GDPR). Additionally, the ICO's enforcement notice during the high-profile case against Experian was criticised by the First-tier tribunal and market participants alike. The ICO's strict interpretation of GDPR's transparency obligations would require companies to notify every individual on public registers before using their data. This would simply lead to confusion and huge costs. While the First-tier Tribunal overturned most of the ICO's enforcement notice against Experian, the ICO's appeal has reignited industry concerns and affects the use of public data sources such as the Electoral Register, Register of Companies, the Register of Judgements, Orders and Fines, the Land Register, and the Food Standards Agency Register among others.

5.10. Finally, given that the ICO has limited resources to pursue cross border enforcement action overseas (which has become more acute following Brexit) it has necessitated the need to join multilateral agreements such as the Global Cooperation Arrangement for Privacy Enforcement (Global CAPE)5. This is a welcome step as via the Global CAPE, the ICO can aid with investigations and share information with member countries without having to enter separate MoUs with each member nation.

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

- **What factors could influence the next European Commission when deciding whether to renew its data adequacy decisions for the UK in June 2025?**
- **What factors could the Court of Justice of the EU (CJEU) consider if the legality of the EU-UK adequacy decisions were challenged?**
- **How would you assess the possible impact of proposed UK rules on automated decision-making and the use of Artificial Intelligence on data adequacy?**

5.11. Whilst the actual data adequacy assessment process is unclear there are several key factors that are likely to influence the European Commission's decision on whether to renew its data adequacy decision for the UK in June 2025:

- Regulatory divergence - The Commission will assess if the UK's data protection laws and practices have remained essentially equivalent to the EU's GDPR standards since adequacy was

[5] https://cy.ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/04/ico-joins-global-data-protection-and-privacy-enforcement-programme/

granted. Any significant divergence or weakening of UK rules could jeopardise a renewal.

- UK court rulings - High-profile rulings by UK courts interpreting and applying data protection laws will likely be scrutinised to ensure they align with European standards and court precedents.
- UK-EU relationship – Any changes to the broader political relationship and any tensions between the UK and EU could affect the data adequacy decision.
- New EU laws - If the EU enacts major new digital/data regulations before 2025, it may re-evaluate whether the UK still qualifies as adequate under the updated rules.
- Surveillance concerns - Any revelations about expansive UK Government surveillance practices that infringe on privacy could raise concerns over adequate protections.

5.12. Enforcement record - The Commission will likely review the ICO's enforcement actions and examples of the UK adequately upholding data protection rights in practice.

5.13. Furthermore, it is worth highlighting that the Opinion of the European Data Protection Board (14/2021)6 regarding the European Commission draft adequacy decision for the UK. This Opinion cited the UK's international commitments and specifically welcomed (para 48) the UK's adherence to the European Convention on Human Rights (ECHR). This suggests that there would be potential implications for the EU-UK data adequacy decision should the UK, in the future, decide to withdraw from the ECHR. ECHR's relevance to the data adequacy debate stems from its relationship with the Charter of Fundamental Rights of the EU, which is central to GDPR (Recital 1). The Charter contains rights which correspond to rights guaranteed by the ECHR; hence the meaning and scope of those rights are the same as those laid down by ECHR.

5.14. The CJEU would likely consider factors like the ones described above if the legality of the EU-UK adequacy decisions were challenged. In trying to predict the CJEU's position on this, it is worth referring to the Schrems I & II cases which invalidated the EU's data adequacy decisions for the US in 2015 and 2020 and cast doubt on the Commission's Standard Contractual Clauses that were in use at the time. The key conclusion in both cases was the importance of the third country, receiving the data, having a level of data protection which is essentially equivalent to that required by EU law. From that

[6] https://www.edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf

perspective, if there was a risk of erosion or weakening of EU citizens' fundamental rights as the result of transferring their data to the UK then this would likely invalidate the EU-UK data adequacy decision.

5.15. Article 22 of the UK GDPR sets out the conditions under which solely automated decisions, including profiling, that produce legal or similarly significant effects on data subjects may be carried out. It restricts such activity to three conditions: (i) where necessary for entering into, or the performance of, a contract between a controller and a data subject; (ii) where such activity is required or authorised by law; or (iii) where a data subject has provided explicit consent. This article was largely designed to protect data subjects from being unfairly discriminated against or have legal effects on them via automated processing without a route to recourse. It is also taken that automated processing in this context is a broader term and would also encompass any processing performed by artificial intelligence.

5.16. Clause 14 of the DPDI Bill replaces Article 22 of the UK GDPR with new Articles 22A-D which effectively expands the use cases in which automated decision-making can be used. Article 22A(1)(a) defines a decision based on solely automated processing as one that involves no meaningful human involvement. Article 22A(1)(b)(i) and (ii) set out the definition of a significant decision as one that produces legal or similarly significant effects on a data subject.

5.17. Article 22A (2) requires controllers to consider, among other things, the extent to which a decision has been taken based on profiling when establishing whether human involvement has been meaningful.

5.18. Article 22D (1) and D(2) confer regulation making powers to the Secretary of State to provide directly, and/or, through secondary legislation to further clarify which cases under Article 22A(1)(a) that are, or are not, to be taken to have meaningful human involvement and to further describe under Article 22A(1)(b)(ii) what is, or is not, to be taken as a significant decision.

5.19. It is our opinion that the new Articles 22A-C would not have any material effect on the rights of individuals, however the secondary powers conferred in Article 22D does potentially allow for further divergence at a future point. Ultimately, we think the EU-UK data adequacy decision would be impacted only in the exercise of those powers and the level of divergence that is sought via those powers.

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

- **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?**
- **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?**
- **What would be the implications for the continued operation of Part III of the TCA (law enforcement and judicial cooperation on criminal matters)?**

5.20. Our understanding of the immediate changes being proposed via the DPDI Bill will not affect EU data adequacy. EU data adequacy does not require the same laws verbatim, but it does require essentially equivalent data protection outcomes. It is worth highlighting that the UK's starting point, from a legislative point of view, is GDPR and that the EU has granted Japan data adequacy status even though Japan has not implemented GDPR within its domestic data protection framework. It is worth adding that, even without the DPDI Bill, the UK would naturally diverge from the EU by virtue of no longer being subject to EU laws. In fact, the Commission and the European Parliament have been considering additional procedural rules related to the enforcement of GDPR[7] which would not apply to the UK. In any case, the risk of further divergence is very much dependent on how the secondary powers granted within the DPDI Bill are utilised.

5.21. It is also worth pointing out here that the DPDI Bill (New Article 45B) changes the concept of data adequacy and replaces it with a new "data protection test" and clarifies that the "transfers of personal data to a third country or international organisation if the standard of the protection provided for data subjects with regard to general processing of personal data in the country or by the organisation is not materially lower than the standard of the protection provided for data subjects" under the UK GDPR and Data Protection Act 2018. The key point is that "materially lower" appears to be different standard to that of "essential equivalence" and suggests there is a certain amount of flex assessing the standard of data protection of the third country.

5.22. At this moment in time, it is difficult to quantify the level of risk of the Commission withdrawing the UK data adequacy decision. It would be fair to say that this risk is higher than other data adequate

[7] https://commission.europa.eu/publications/proposal-regulation-laying-down-additional-procedural-rules-relating-enforcement-gdpr_en

countries because of the 4-year sunset clause built into the data adequacy decision, which is currently unique to the UK. Again, referring to the EDPB's Opinion offers some clues as to the general concerns of the EU.

(paras 52-54, pages 13-14)
*It is important to note that the possibility of the UK ministers and the UK Secretary of State to introduce secondary legislation following the end of the bridge period may lead to a significant divergence of the UK Data Protection Framework from the EU's in the future.*

*Indeed, the UK Government has indicated its intention to develop separate and independent policies in data protection, which may then lead to a divergence from EU data protection law. This intention encompasses the inclusion of personal data aspects in trade agreements, a practice that entails the risk of lowering the level of protection of personal data provided for by the UK.*

*Finally, not only since the end of the transition period, the UK is no longer bound by CJEU case-law but also, the already adopted judgments of the CJEU, considered as retained case law in the UK legal framework, might not bind the UK any more as, in particular, the UK has the possibility to modify retained EU law after the end of the bridge period and its Supreme Court is not bound by any retained EU case-law.*

5.23. Suffice to say that if the UK adopted policies that were seen to diverge significantly from the EU the risk of the EU withdrawing its decision would increase accordingly. The key sources of UK-EU divergence are likely to emerge from the UK's use of secondary powers and the inclusion of personal data aspects in trade agreements.

5.24. However, the EU would also need to balance these risks against the potential disruption that EU companies would equally face. If the EU withdrew its data adequacy decision for the UK, we think it could play out as two political scenarios: 1) the UK and EU quickly negotiating a resumption or continuation perhaps under different terms, or 2) the UK would accelerate its divergence with the EU on data protection. However, given the strong desire for businesses to maintain the free flow of data from both sides, the weighting of the two options lean more in favour of the first option.

5.25. The risk of significant disruption is high should the EU remove adequacy from the UK. The majority of British businesses are SMEs, and this is true for the research sector where 97% of businesses are

SMEs, and they have limited capacity or resources to adequately prepare for such a scenario, or the resources to adequately meet new and onerous requirements.

5.26. One possible mitigation against the potential interruption in dataflows is the underutilised sector Codes of Conduct pursuant to Article 40 of the GDPR. Associations, such as MRS 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 GDPR with regard to transfers of personal data to third countries. However, the process for gaining Code approval from the ICO is a complex and time consuming process, and as yet there are very few Codes approved.

5.27. Instead, MRS would welcome a greater appreciation and use of existing sector and professional Codes of Conducts that are part of an association or a trade body's membership terms and are an effective means to support and ensure compliance and greater awareness of rules from SME organisations. The MRS Code of Conduct is crucial in helping to protect and regulate first-rate research, insight, and data practice. For example, MRS regulates standards and innovation across market, opinion and social research and data analytics. MRS regulates research ethics and standards via its Code of Conduct and all individual MRS members and Company Partners agree to regulatory compliance of all their professional activities via the MRS Code of Conduct and its associated disciplinary and complaint mechanisms. MRS also provides guidance on EU-UK data flows and International Standard Contractual Clauses. MRS has a long and strong track record in providing excellent regulation to industry, and these existing mechanisms should be mobilised by the UK Government.

5.28. The UK Government could also consider mobilising sector specific Codes of Conduct, such as the MRS Codes of Conduct, which are crucial in helping to protect and regulate research, insight, and data practice. This could help with the proper application of legal obligations and considers the specific needs of micro, small and medium-sized enterprises better. Codes of Conducts are essential tools for industry, and are far easier to understand, apply and develop as opposed to legislation. The use of sector Codes, therefore, are essential to SME's and their ability to comply with GDPR and other legal requirements.

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

- **What conclusions do you draw from the European Commission's recent adequacy review of 11 countries and territories?**
- **Are there examples of best practice which the UK could learn from in the way other countries approach their data transfer arrangements with the EU?**
- **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?**
- **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?**

5.29. In the recent adequacy review[8] of the 11 countries/territories, the Commission concluded that after assessing developments in the legal frameworks and practices in each of the 11 countries/territories, they continued to provide an adequate level of protection for data transferred from the EU under the GDPR standards. However, the Commission recommended some countries enshrine certain protections developed at sub-legislative levels into legislation to enhance legal certainty (e.g., Argentina, Canada and Israel).

5.30. The report was notable from the perspective that is incorporated the clarifications from EU courts on the "essential equivalence" standard for adequacy, with specific references to the Schrems I and Schrems II cases. The report stated (page 5):

*Importantly, the adequacy referential also 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.*

5.31. In terms of best practice that the UK could draw from, the EU-Japan data adequacy decision[9] serves as a useful example of how countries with very different cultural and legal frameworks can establish mutually acceptable data transfer arrangements with the EU. The EU-Japan data adequacy decision is significant in that it was the first data adequacy decision to a non-EU country since the implementation of GDPR. It was also notable that the EU and Japan had different perspectives towards data privacy: the EU seeing it as a fundamental human right versus Japan's view which emphasised the economic

[8] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_161
[9] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421

importance of data flows. Despite the EU's and Japan's distinct concepts of privacy and enforcement mechanisms, the EU-Japan data adequacy decision ultimately managed to strike balance between convergence and preserving Japan's unique approach.

5.32. One highlight of this decision is the recognition of the "Supplementary rules" introduced by Japan's Personal Information Protection Commission (PPC). These rules, tailored to the specificities of the Japanese system, addressed potential gaps and enhanced protections to meet the EU's adequacy requirements.

5.33. Additionally, the cooperative data privacy model[10] at the heart of this adequacy decision allowed for a two-track system, where EU-to-Japan data flows are protected by the Japanese Act on the Protection of Personal Information ("APPI") in conjunction with the Supplementary Rules. However, the Supplementary Rules do not apply to Japan-to-EU data flows. Moreover, data handled and processed within Japan is protected at the standard of the APPI only. This collaborative approach facilitated convergence in key areas, such as ensuring robust safeguards for personal data transfers, while respecting Japan's cultural and legal particularities. It also demonstrates how countries can bridge differences through constructive engagement and a willingness to adapt existing frameworks.

5.34. In terms of 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, this largely depends on context and what concessions the UK can achieve in converging the data protection laws of the third country with that of the UK GDPR standard.

5.35. We can consider this question through two hypothetical scenarios whereby 1) the UK grants data adequacy to a country that the EU is also actively assessing for data adequacy, and 2) where the UK grants data adequacy to countries that the EU has deemed inadequate in terms of data protection standards.

5.36. For the former, any impact on the EU-UK data adequacy decision would depend on the type of concessions negotiated. This is where achieving a concession like Japan's Supplementary Rules, whereby UK data transfers to the third country is treated at a higher standard, would be helpful towards making the case that the UK, in granting the adequacy decision, is not eroding its standards. The downside is that if

[10] Yang, F (2020). Cooperative Data Privacy: The Japanese model of data privacy and the EU-Japan GDPR Adequacy Agreement. Harvard Journal of Law & Technology Vol 33, No 2 Spring 2020. Available from https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf

both the UK and EU are competing as rivals to complete a data adequacy decision for the same third country this may led to a less than optimal outcome and a possible breakdown in trust between both parties.

5.37. MRS believes the latter scenario would more likely jeopardise the EU-UK data adequacy agreement, as the EU may perceive the UK as lowering its standards, therefore putting EU citizens personal data at an elevated risk. In this situation, the UK would need to carefully balance the benefits of granting a data adequacy decision against potential trade-offs.

5.38. Similarly, the UK joining the Global Cross Border Privacy Rules (CBPRs) system would not necessarily lead to an adverse impact to the EU-UK data adequacy decision insofar as it would depend on the UK's ability to address the perceived deficiencies or gaps of the Global CBPRs and maintain the current standard of the UK GDPR.

5.39. Currently, the Global CBPRs:

a. Do not include a mandatory requirement for breach notifications, nor does it contain a standard definition of what a breach is.
b. Do not apply to data processors. Processor activities remain subject to enforcement through enforcement against data controllers.
c. Allow Members to adopt suitable exceptions based on national sovereignty, national security, public safety and public policy concerns.
d. They do not contain specific rules on the processing of data via wholly or partly by automated means.
e. They refer to the broad notion of harm but is not specific, as the GDPR is, about sensitive categories of data.

## 6. Conclusion

Maintaining the EU's data adequacy decision for the UK is crucial for businesses and the digital economy. While the DPDI Bill introduces some divergence from EU data protection rules, it appears the immediate changes would not significantly impact the adequacy decision. However, how the UK exercises its new regulatory powers going forward, as well as broader political factors, could influence the European Commission's review in 2025.

Both sides have strong incentives to preserve the free flow of data, but the UK will need to carefully balance unlocking potential opportunities through regulatory divergence against undermining trust with the EU and jeopardising the adequacy decision. Drawing lessons from other countries

like Japan that have bridged differences through collaborative approaches could help chart a path forward. It is of course essential that harmonisation between the EU and UK remain intact, this is not exclusive to data adequacy but business at a larger scale; in order to foster cross-border cohesiveness and effective relations that are mutually beneficial for the EU and UK.

Ultimately, maintaining a balance between an essentially equivalent level of data protection that respects EU standards, while adapting rules to UK interests, will be key for the UK retaining its EU data adequacy status long-term. Increased dialogue, legal certainty, and a spirit of cooperation from all parties will be vital for achieving this balance.

We welcome discussing these matters further, and we welcome the opportunity to discuss the MRS submission in response to the House of Lord's consultation: Data Adequacy Inquiry.

**Received 22 May 2024**