Advertising Association – Written Evidence (DAT0010)

Advertising Association's response to the House of Lords' Inquiry into data adequacy and its implications for the UK-EU relationship

Summary

1. Data is fundamental to the advertising and marketing industry and is critical for tasks such as consumer trend analysis, behavioural insights, market segmentation, targeted advertising, and AI.

2. The EU's decision to grant the UK data adequacy status post-Brexit was highly valuable to the industry, avoiding potential burdensome requirements for data transfers. While the GDPR ushered in a new era of harmonised data protection and enhanced rights and protections, it also created some ambiguities and imposed additional compliance costs.

3. The introduction of the Data Protection and Digital Information (DPDI) Bill has been broadly welcomed by industry especially where it aims to clarify those aspects of GDPR while maintaining high data protection standards.

4. Key factors that could influence the European Commission's decision to renew the UK's data adequacy status include regulatory divergence, UK court rulings, the broader UK-EU relationship, new EU laws, surveillance concerns, and the ICO's enforcement record. The CJEU would likely consider similar factors and whether the UK's regulatory framework remains essentially equivalent if the EU-UK's data adequacy decision was challenged.

5. Potential implications of the UK granting its own adequacy decisions to third countries depend on whether those decisions lower or maintain the UK's current standards. Joining the Global Cross Border Privacy Rules system would only impact adequacy if identified gaps are not addressed and the UK GDPR's level of protection is not maintained.

6. Maintaining EU data adequacy is crucial for businesses. Whilst it is important for the UK to seek new opportunities, it must balance those against undermining trust with the EU. Increased dialogue and cooperation will be vital for the UK to retain adequacy long-term while adapting rules to its own interests.

About the Advertising Association

7. The Advertising Association promotes the role and rights of responsible advertising and its value to people, society, businesses,

and the economy. We bring together companies that advertise, their agencies, the media and relevant trade associations to seek consensus on the issues that affect them. We develop and communicate industry positions for politicians and opinion-formers, and publish industry research through advertising's think-tank, Credos, including the Advertising Pays series which has quantified the advertising industry's contribution to the economy, culture, jobs, and society.

8. The membership of the Advertising Association is very broad and includes the associations representing industry sectors, such as the advertisers (through the Incorporated Society of British Advertisers), the agencies and advertising production houses (through the Institute of Practitioners in Advertising and the Advertiser Producers Association), all the media (from broadcasters and publishers, cinema, radio, outdoor and digital), advertising intermediaries and technology providers (which include platforms and the IAB UK), market research (through the Market Research Society) and marketing services such as direct marketing (through the Data & Marketing Association).

Context

9. Advertising and marketing are important. They play a crucial role in brand competition, drive product innovation and fuel economic growth. Many industries such as the arts, sport and culture depend on it for their revenues and it also funds a diverse and pluralistic media, including a free and open internet, enjoyed by consumers of all ages, including children and young people.

10. Advertising is also a driver of economic growth and competition. We have previously estimated that every pound spent on advertising returns up to £6 to GDP through direct, indirect, induced, and catalytic economic effects. According to the latest the latest Advertising Association/WARC Expenditure Report the UK's ad spend rose 6.1% during 2023, to a total of £36.6 billion. This would mean a contribution of approximately £220bn to the economy supporting over 1 million jobs across the UK.

11. According to Deloitte research carried out on behalf of the Advertising Association, the one million jobs supported by advertising can be broken down as follows:
    a) 350,000 jobs in advertising and the in-house (brands) production of advertising.
    b) 76,000 jobs in the media sectors supported by revenue from advertising.
    c) 560,000 jobs supported by the advertising industry across the wider economy.

12. Data is fundamental to the advertising and marketing industry:
    a. It can improve the analysis of consumer trends, market segmentation and help deliver more relevant ads.
    b. Specific consumer and behavioural insights can be derived through surveys and opinion polls.
    c. It helps with the matching of buyers and sellers of online advertising inventory.
    d. It is important to the development and advances in AI, which the advertising and marketing industry are at the forefront of as responsible developers, deployers and end users of AI.

13. Finally, advertising's importance to the free and open internet should not be understated. Advertising funds free content online and it is indispensable to content creators and publishers to monetise their work. Online advertising allows companies to increase their digital reach through attract new consumers and increase awareness of their products and services.

14. For further information regarding the points made in this submission, please contact konrad.shek@adassoc.org.uk

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?**

15. 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 advertising and marketing that rely heavily on data. Without an adequacy decision, UK companies would face burdensome requirements to implement safeguards like Standard Contractual 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.

16. The GDPR's key benefit, of course, 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 also have a large degree of autonomy on how they assess and quantify risk. The 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.

17. However, the GDPR, in solving several 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.

18. 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 used for online advertising. 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.

19. It is for these reasons 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 addresses the overreliance on consumers' consent to their data being used as a legal basis and clarifies that "legitimate interests" – an equally valid legal basis under GDPR – can apply to processing that is necessary for the purposes of direct marketing. It also extends the "soft opt-in" for email to the charity and voluntary sector. Moreover, it incorporates "scientific research carried out as a commercial activity" into the definition of scientific research which is of benefit to the market research community.

- **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?

20. 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.

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

22. Instead of remaining technology or market neutral, the ICO has at times waded into market issues by expressing preferences for certain technologies, for example preferring contextual advertising over behavioural advertising - with reasoning that has been viewed by others in the industry as misplaced. While the ICO remains a respected regulator overall, there are fears that certain decisions or approaches risk overreaching into policy areas that exceed its current remit and it does not have the competency over.

23. 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)[1]. 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?

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

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

24. Whilst the actual data adequacy assessment process is opaque we think there are several key factors that could 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 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 potentially spill over, with the data adequacy decision being impacted.
    - 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.
    - Enforcement record - The Commission will likely review the ICO's enforcement actions and examples of the UK adequately upholding data protection rights in practice.

25. Furthermore, it is worth highlighting the Opinion of the European Data Protection Board (14/2021)[2] 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.

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

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

26. 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 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.

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

27. 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 AI.

28. 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.

29. 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.

30. 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.

31. 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?**

32. 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[3] 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.

33. 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.

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

34. 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 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.

35. Suffice to say that if the UK adopted policies that were seen to diverge significantly from the EU then 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.

36. 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 one.

- **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?**

37. Having experienced Brexit, we believe that companies are probably better prepared (compared to pre-Brexit) in the event of the Commission withdrawing the UK data adequacy decision due to the greater awareness of standard contractual clauses. In many cases large multinationals have also implemented binding corporate rules to facilitate international data transfers. However, the risk of disruption among SMEs have largely remained same. Often SMEs have limited knowledge of the rules or do not have the resources to adequately prepare for that scenario.

38. One possible mitigation against the potential interruption in dataflows is the underutilised codes of conduct pursuant to Article 40 of the GDPR: 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 GDPR with regard to transfers of personal data to third countries. Using codes of conduct that are part of an association or a trade body's membership terms would be an effective way to reach out those SME organisations and increase compliance and awareness of the rules.

39. 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. The Data & Marketing Association (DMA), for example, represents around 700 companies, both large and small, in the data and marketing sector and its members must comply with the DMA Code which sets out standards in data ethics. The DMA is well-known to the ICO, and it has been in discussions for some years about developing a Code of Conduct under Article 40 and 41 of UK GDPR.

40. It is worth highlighting that the DPDI Bill establishes Codes of Conduct for the Privacy & Electronic Communications Regulations (PECR) that can be contained in the same document as a GDPR Code of Conduct. Given the interaction between GDPR and PECR, a Code of Conduct for Advertising or Marketing must cover both GDPR and PECR aspects.

41. Additionally, our members have expressed a desire for a greater appreciation and use of existing sector and professional Codes of Conducts. Sector Codes that are part of an association or a trade body's membership terms are an effective means to support and ensure compliance and greater awareness of rules from SME organisations.

42. For example, the Market Research Society (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 its individual 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 could be mobilised by the UK Government.

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?**

43. In the recent adequacy review[4] 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).

44. The report was notable from the perspective that 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.

- **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?**

[4] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_161

45. In terms of best practice that the UK could draw from, the EU-Japan data adequacy decision[5] 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 remarkable in 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 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.

46. 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.

47. Additionally, the cooperative data privacy model[6] 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.

- **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?**

48. 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] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421

[6] 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

49. 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.

50. 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 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.

51. 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.

- **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?**

52. For similar reasons, we argue that 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.

53. 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.

Conclusion

54. 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.

55. 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.

56. 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.

Received 3 May 2024