Reset – Written Evidence (DAT0006)

House of Lords European Affairs Committee

UK/EU Data Adequacy Call for Evidence

Response from Reset

Reset (https://www.reset.tech/) seeks to improve the way in which digital information markets are governed to serve the public. We do this through supporting new public policies across a variety of areas–– including data privacy, competition, elections, online safety, security, taxation, and education. Reset has analysed and consulted extensively on the Data Protection and Digital Information Bill (the 'DPDI Bill'), including giving evidence to the House of Commons Public Bill Committee[1] and the Joint Committee on Human Rights[2].

Question (2) in this call for evidence asks[3]:

> *"What are the possible challenges to UK-EU data adequacy regime?*
> *a. What factors could influence the next European Commission when deciding whether to renew its data adequacy decisions for the UK in June 2025?*
> *b. What factors could the Court of Justice of the EU (CJEU) consider if the legality of the EU-UK adequacy decisions were challenged?*
> *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?"*

We are concerned that the DPDI Bill undercuts multiple aspects of the UK's data protection regime. As well as creating risks for ordinary people in the

[1] https://bills.parliament.uk/publications/51216/documents/3445
[2] https://committees.parliament.uk/writtenevidence/121482/pdf/
[3] The annexed opinion also speaks to questions 3(b), 4(a) and 4(c).

UK, this could threaten the UK's adequacy decision from the EU. The possibility of losing of adequacy will cast a long shadow if this bill is passed without amendment that may deter investment in UK markets due to uncertainty for business operations.

We have worked with data rights law firm AWO to seek an opinion from leading counsel Alastair Sutton on whether the DPDI Bill poses a risk to the EU's adequacy decision in favour of the UK. Mr Sutton has worked on European and international trade law for 57 years, including advising the UK Government during the UK's accession to the (then) European Community (1970-73), and other clients on the UK's process of withdrawal from the EU and the EU-UK Trade and Cooperation Agreement. He worked on the opinion with Aarushi Sahore of Brick Court Chambers, a leading junior in the fields of public and data protection law.

Counsel's opinion is annexed and states that the DPDI Bill:

> *"Represent[s] the weakening of foundational principles of data protection and privacy rights derived from EU law [and poses] specific risks to the continuation of the adequacy assessment by the EU and we do consider that these – taken together – could undermine the UK's hard-won assessment of data adequacy."*

Counsels' opinion identifies the following areas of particular concern in the DPDI Bill:

- **The role and independence of the ICO;**
- **The addition of lawful bases for processing which provide blanket authorisation without protection for data subject rights;**
- **The prospect of onward transfers from the UK to jurisdictions with lower standards of data protection as a form of 'data laundering';**
- **Greater freedom for risky processing by political parties, public bodies and businesses; and**
- **An undermining the practical utility of data rights.**

The opinion also finds:

> *"There is of course an entirely independent risk of the European Court of Justice striking down any adequacy assessment as well. Given [the Court's] approach to privacy rights in recent years, we consider that it is possible that one or more of the above changes could fall foul of a strict judicial assessment of adequacy."*

This echoes concerns raised by European Parliamentarians about the impact of the DPDI Bill on the standard of data protection in the UK, and whether it will continue to be adequate[4].

That is, the DPDI Bill poses a risk to the UK's adequacy decision both:

(i) **In 2025** when the European Commission formally reviews and decides to renew it; **and**

(ii) **On an ongoing basis** due to the European Commission's ongoing monitoring and – most importantly – the risk of a successful challenge to the Commission's decision before the European Court of Justice. That challenge could come from anywhere in the EU at any time and is difficult to predict. Past challenges to adequacy decisions in favour of the United States have been successful.

The DPDI Bill, if passed in its current form, therefore leaves a 'sword of Damocles' hanging over the UK's adequacy decision for the foreseeable future. Even if the decision is formally renewed in 2025, there will be significant long-term uncertainty about whether and when the decision might be successfully challenged, leading to an abrupt end to data transfers which would be very harmful to businesses on both sides of the Channel. We are concerned that this uncertainty may act as a disincentive to data-driven businesses to invest in the UK in the coming years.

Other respondents to this Call for Evidence will be better placed to comment on the likely costs of the loss of the UK's adequacy decision. But in our view

[4] See for example https://www.forbes.com/sites/emmawoollacott/2024/03/13/meps-say-uks-dpdi-bill-could-jeopardize-uk-eu-data-transfers/ and https://www.europarl.europa.eu/doceo/document/E-9-2024-000591_EN.html

the speculative benefits from the DPDI Bill are far outweighed by the uncertainty which it will introduce regarding future data transfers from the EU to the UK which are crucial to so many British businesses. This is in addition to the damage the DPDI Bill will do to data rights, user protection, and the Age-Appropriate Design Code among other aspects of the UK's data protection regime. Ultimately, investment is driven by business confidence and the risks and uncertainties introduced by this Bill are surely too high.

2 May 2024

Annex: Legal Opinion

THE DATA PROTECTION AND DIGITAL INFORMATION BILL:

RISKS TO THE EU'S ADEQUACY DECISION

OPINION

A. Introduction and Summary

1. We are asked to advise on whether the proposed Data Protection and Digital Information Bill (the "**DPDI Bill**") poses a risk to the EU's Adequacy Decision in favour of the UK.

2. The Adequacy Decision, issued by the European Commission on 28 June 2021, concluded that the UK provided an adequate level of legal protection for personal data, and thereby enabled the free flow of data from the EU into the UK after Brexit.[1] Since that time, EU and UK laws on data protection have diverged in various respects. Most recently, following a consultation on the liberalisation of the UK's data protection regime,[2] the DPDI Bill has passed through the House of Commons and is in the Committee Stage in the House of Lords.[3]

3. For the reasons outlined below, we consider that there are a number of areas where the DPDI Bill makes material changes to the UK's approach to data protection. The DPDI Bill is already being scrutinised by EU institutions and the detailed changes are likely to be the subject of

---

[1] Commission Implementing Decision of 28 June 2021 (the "**Adequacy Decision**").

[2] Data: a new direction, launched by the Department for Digital, Culture, Media & Sport ("**DCMS**") on 10 September 2021. DCMS published its response to the consultation on 17 June 2022.

[3] The DPDI Bill is set out on the UK Parliament website. It was originally introduced in the 2022-23 parliamentary session and has been carried over to the 2023-24 session. The changes to the Bill following the Report Stage in the House of Commons are summarised online.

careful analysis by the European Commission when the Adequacy Decision is reconsidered for renewal prior to its expiry on 27 June 2025.[4] In the event that the Commission cannot be satisfied that the UK's legal framework provides an adequate level of protection, it will not be in a position to renew the decision and may either refuse to renew it or require further commitments from the UK to bridge any gaps.

4. In particular, we have identified the following areas of the DPDI Bill as posing specific risks to the continuation of the adequacy assessment by the EU and we do consider that these – taken together – could undermine the UK's hard-won assessment of data adequacy:

   (1) **The role of the ICO.** The ICO's role has become more directly interlinked with Government priorities and policies. There is also legal uncertainty as to how this can be expanded further by secondary legislation.

   (2) **Lawful bases.** The list of lawful bases for data processing has been widened to include a number of "recognised legitimate interests", which would provide blanket authorisation for processing on a range of new grounds. Again, there is legal uncertainty and unpredictability about how much further this can be widened by secondary legislation.

   (3) **Third country transfers**. The basis on which data can be transferred from the UK to other third countries has been liberalised. This will be a cause for concern insofar as it

[4] Adequacy Decision, Recitals 289-290, Article 4. In addition, we note that the Commission is required to review the position and reconsider it every four years: EU GDPR Article 45(4) and Recital 106. It is also empowered to suspend, repeal or amend the decision: EU GDPR Articles 45(5), 93(2)-93(3). From the UK's perspective, we understand that the European Affairs Committee is undertaking an inquiry into the Adequacy Decision and whether there is a risk that it may not be renewed when it is reconsidered by the EU next year: Call for evidence in 'Data adequacy and its implications for the UK-EU relationship examined'.

undermines the continuity of protection afforded to data transfers from the EU to the UK and then onwards to other third countries.

(4) **Processing by political parties, public bodies and businesses**. Specific provisions have been added to permit greater data processing by political parties in respect of democratic engagement, public bodies such as the Department for Work and Pensions, and businesses engaged in (broadly defined) research activities.

(5) **Undermining the practical utility of data rights.** Proposals intended to reduce the compliance burden on businesses are likely to have the effect of undermining the practical enforceability of data subject rights.

5. When the EU Commission comes to reconsider its adequacy assessment, the UK is likely to be treated in the same way as any other third country. In other words, the UK will be subject to the usual scrutiny as to whether "essentially equivalent" protection is given to personal data under its laws and practices. In that regard, we acknowledge that the Commission has not revoked or failed to renew an earlier adequacy decision to date and indeed has recently renewed a number of adequacy decisions in favour of a range of third countries.[5] However, each adequacy decision is unique and, as far as the UK is concerned, because the UK was previously a Member State of the EU, its laws are fundamentally familiar to the EU and any divergences are capable of being examined in minute detail. In addition, the Commission will be aware of the legal risk of any adequacy decision being challenged

[5] Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC (15 January 2024) ("**Review Report**"). The Review Report makes clear that the Commission reviewed the changes over time in collaboration with the relevant jurisdictions (p. 5).

in the more exacting forum in the CJEU and will therefore need to be assured that the proposed reforms do not give rise to an unacceptable level of risk.

6. The position is also naturally affected by the evolving political relationship and dialogue between EU and UK institutions. For example, certain Members of European Parliament Members have been vocal in their criticisms of the DPDI Bill,[6] but we are aware that the EU Commission and UK Government officials are in communications about the DPDI Bill in order to promote the renewal of the Adequacy Decision.[7] We focus below on the legal risk of the Adequacy Decision being revoked (or suspended following judicial intervention) in response to changes in UK law. We are less able to opine on broader political factors which may influence EU decision-making.

7. We begin by setting out the nature of the existing Adequacy Decision and the EU's likely approach to renewing it in **Section B** below. We then turn to examine the key legal changes made by the DPDI Bill and our assessment of their impact on the EU's adequacy assessment in **Section C** below.

B. The Adequacy Decision

8. The UK is now a "third country" under the General Data Protection Regulation ("**EU GDPR**"). This means that, under EU law, personal data transfers from the EU to the UK are permitted only under certain conditions,[8] most importantly an adequacy decision of the EU

---

[6] See for instance "MEPs Say UK's DPDI Bill Could Jeopardize UK-EU Data Transfers" by Emma Woollacott (13 March 2024) published in Forbes Magazine and the Question posed by Dutch MEP Paul Tang on 22 February 2024 to European Parliament.

[7] The Secretary of State was reported as saying that the UK was in "constant contact" with the European Commission in creating the proposal: see "UK data reform bill revived after lengthy legislative delay" available online. See further oral evidence given by the Director of Research and Insights at the International Association of Privacy Professionals to the European Affairs Committee on 26 March 2024 (in particular in response to Q6 on p. 14).

Commission concluding that the UK ensures an adequate level of protection for personal data.[9] The effect of the Adequacy Decision is that it acts as a 'shield' permitting all such personal data transfers without the need for case-by-case authorisation.[10] We understand that the Adequacy Decision is of critical importance to businesses operating both in the EU and the UK.[11]

(i) The EU's approach to adequacy decisions generally

9. The test for adequacy under the EU GDPR is whether the particular third country ensures an adequate level of protection for privacy rights, essentially equivalent to that guaranteed within the EU.[12] This does not require a "point by point" mirroring of EU legislation but the Commission will look for equivalence in substance based on core requirements in the third country legislation and in practice.[13]

10. The Commission bases its decision on a wide-ranging assessment of the third country's legislation (both general and sectoral), rules and international commitments, together with the powers and functioning of the independent supervisory authorities which have responsibility for enforcing the rights of data subjects.[14] In order to make an adequacy

---

8 EU GDPR Article 44 provides that any transfer of personal data to a third country can only take place if the conditions in Chapter V are complied with by the controller and processor, including for onward transfers to other third countries. The purpose of these restrictions is ensuring that a continuous level of protection is not undermined by international data flows, see EU GDPR Recital 101.

9 EU GDPR Article 45(1) and (3).

10 EU GDPR Article 45(1) and Recital 103. The other lawful routes for third country transfers include the specific derogations in Article 49 or the inclusion of sufficient safeguards such as corporate rules or contractual provisions in Articles 46-47. Those apply on a case-by-case basis.

11 The UCL European Institute published a study in November 2020 suggesting that businesses would need to spend £1bn to £1.6bn in compliance costs in the absence of an adequacy decision: "The Cost of Data Inadequacy". We cannot verify that figure but it appears to be well-established in the UK and the EU that the disruption to business would be significant if the Adequacy Decision is not renewed.

12 EU GDPR Article 45(1) and Recital 103-104.

13 EDPB Adequacy Referential p. 3; Case C-362/14 *Schrems I* (ECLI:EU:C:2015:650) [73] and Case C-311/18 *Schrems II* (ECLI:EU:C:2020:559) [94] ("requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter").

14 EU GDPR Article 45(2). Specific subjects identified for attention are laws governing the access of public authorities to personal data and rules for the onward transfer of personal data to another country or international organisation.

decision, the Commission will have regard to the relevant EU case law as well as the guidance of the European Data Protection Board ("**EDPB**").[15] Any adequacy decision will be subject to review by the EU courts, as the *Schrems I* and *Schrems II* litigation (discussed below) demonstrates.[16]

11. At present, the EU has adequacy decisions in place in respect of a small number of countries such as Argentina, Canada, Israel, Japan, New Zealand, Switzerland, the United States and Uruguay.[17] Each country's adequacy decision is bespoke rather than formulaic, as it depends on the particular legal system and the degree of exposure that EU citizens' data may face there. In some cases, such as the United States and Japan, the assessment is based on the existence of certain additional commitments as to the treatment of EU persons' personal data.

12. The intensity of scrutiny has also varied over time and in respect of different issues. For instance, the decision in respect of Israel, which was made under the earlier Data Protection Directive and renewed recently, is in brief terms. It appears to take as sufficient the fact that Israeli privacy laws were modelled on the EU's data protection laws at the time.[18] In its review decision, the Commission welcomed the further legislative developments in Israel which contributed to an "increased level of protection".[19] On the other hand, the decision in respect of Japan is very detailed, and involves supplementary rules to bridge the differences between the two systems, as well as assurances from the

---

[15] The EDPB was set up under the GDPR: Recital 139. It has issued relevant guidance in the Adequacy Referential noted above and the Recommendations on the European Essential Guarantees for Surveillance Measures.

[16] Case C-362/14 *Schrems I* (ECLI:EU:C:2015:650) and Case C-311/18 *Schrems II* (ECLI:EU:C:2020:559).

[17] See the list of the Commission's current adequacy decisions.

[18] See the Adequacy Decision in respect of Israel, which was informed by the Article 29 Working Party's Opinion (the predecessor to the EDPB). The decision notes that Israel largely adopted the Data Protection Directive (the predecessor to the GDPR) in its Privacy Protection Act 5741-1981 and that there were Basic Laws included a right to privacy: Recitals 5-6.

[19] See Review Report [4.71].

Japanese Government in respect of law enforcement and national security.[20]

13. The most recent illustration of the EU's approach to adequacy is the decision in favour of the United States.[21] This is the third attempt of the Commission to establish an adequacy arrangement with the United States, after the EU-US Safe Harbour Agreement was struck down by the CJEU in *Schrems I* and the EU-US Privacy Shield was struck down by the CJEU in *Schrems II*.[22] In particular, in *Schrems II*, the CJEU had examined the EU-US Privacy Shield in extensive detail and did not accept the Commission's overall assessment of adequacy. The CJEU found that, among other things, the Privacy Shield did not give data subjects sufficient protection from bulk surveillance by US intelligence authorities (including because such surveillance on the grounds of national security did not meet the requirements of proportionality) and that there was no adequate administrative and judicial redress (in the sense of an independent judicial process) for data subjects whose data was being transferred to the US.[23]

14. The most recent EU adequacy decision in favour of the US is based on a new arrangement between the EU and US known as the Data Protection Framework, which seeks to address the specific criticisms made by the CJEU in *Schrems II*.[24] The new framework imposes more onerous obligations on US entities and establishes new mechanisms of enforcement and quasi-judicial redress for EU data subjects. It is

---

20 See the Adequacy Decision in respect of Japan as well as the further review decision.

21 US Adequacy Decision dated 10 July 2023.

22 Case C-362/14 *Schrems I* (ECLI:EU:C:2015:650) and Case C-311/18 *Schrems II* (ECLI:EU:C:2020:559).

23 Case C-311/18 *Schrems II* (ECLI:EU:C:2020:559) [168]-[201].

24 The DPF is an arrangement between the EU and the US under which US companies can self-certify as committed to data protection principles or DPF Principles. See the US Department of Commerce website.

possible that this arrangement will nonetheless be challenged in the CJEU.[25]

(ii) The reasoning underpinning the Adequacy Decision in favour of the UK

15. As noted above, each Adequacy Decision is unique. In the case of the UK, it is highly likely that the Commission will begin by reflecting on the previous Adequacy Decision, including the areas of concern previously identified and any further divergences between EU and UK law. The overall question will be whether the UK continues to provide – in law and in practice – an essentially equivalent protection to fundamental privacy rights to that achieved in the EU.

16. Reading the existing Adequacy Decision as a whole, we can identify the following as the building blocks for the conclusion that the UK provided "essentially equivalent" protection:[26]

    (1) First, it was of fundamental importance that the UK's legal framework was very similar to that in the EU.[27] The analysis was straightforward because the GDPR was retained in domestic law after Brexit ("**UK GDPR**") and had been given effect in various ways under the Data Protection Act 2018 ("**DPA**").[28] The Commission was not concerned about minor or technical amendments, and was clear that there was strong alignment in all

[25] An interim relief application was refused in Case T-553/23 *Latombe v Commission* but it appears the proceedings have not yet concluded.

[26] The Adequacy Decision takes the form of short operative provisions preceded by lengthy recitals. Adequacy Decision Recitals 273-275, 277 and 281 are helpful summaries of the Commission's assessment "in the round".

[27] Adequacy Decision, Recital 19.

[28] After the end of the implementation period on 31 December 2020, the EU GDPR was converted into a new form of domestic legislation known as "direct EU legislation", which is a category of retained EU law under s. 3 of the European Union (Withdrawal) Act 2018 ("**EUWA**").

the core concepts, such as personal data, data processing, data controllers, grounds for processing and consent.[29]

(2) Second, any material differences were scrutinised by the EU Commission more closely, but in each case the Commission was satisfied at the time that there were adequate safeguards in place based on the surrounding legal framework:

(a) Restrictions in relation to **defence and national security** were considered to be sufficiently controlled by necessity and proportionality principles.[30]

(b) The exemptions for **journalistic, artistic and literary purposes** were also considered sufficiently limited including because they required a "reasonable belief" that the publication was in the public interest.[31]

(c) The exemptions for **scientific or historical research purposes**, or other purposes in the public interest, would be kept under review.[32] In the UK, the exemption for research purposes allows data controllers not to inform data subjects about the safeguards applicable to international transfers.[33]

(3) Third, the Commission placed reliance on the role and powers of **the Information Commissioner's Office ("ICO")** in ensuring that adequate protection was guaranteed in practice through monitoring and enforcement.[34] The decision emphasised the

---

29 Adequacy Decision, Recitals 15-16, 19-20, 23-26, 43-53, 68, 83-84; EDPB Opinion, [8], [58].

30 Adequacy Decision, Recitals 56-67.

31 Adequacy Decision, Recitals 68-73.

32 Adequacy Decision, Recitals 71-73.

33 Compare Articles 15(2) and 89 of the EU GDPR with paras. 27(2) and 28(2) of Part 6 of Schedule 2 to the DPA 2018. In fact, the acceptance of this difference was criticised at the time by commentators, see Douwe Korff "The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK" at p. 14.

independence of the Information Commissioner,[35] and the interpretive weight of their guidance.[36]

(4) Fourth, the Commission took comfort from the general protections in UK laws for privacy rights under **international and domestic human rights** laws including the European Convention on Human Rights ("**ECHR**").[37] It approved the protection of individual data rights, such as the right of access, both in terms of substance and procedure.[38]

17. We note that the Commission expressed caution in relation to the following matters and we consider it highly likely that these issues will be addressed further in any renewal decision:

(1) The Commission noted the risks of UK government access to personal data,[39] in particular **law enforcement authorities and intelligence services**.[40] The need for necessity and proportionality,[41] independent oversight,[42] and the continued application of the ECHR,[43] was emphasised.

---

[34] Adequacy Decision, Recitals 85-98.

[35] Adequacy Decision, Recitals 87-90. The independence of oversight was also an important consideration as regards the lawfulness of any restrictions on the right to privacy under the ECHR, see Recitals 117-118.

[36] Adequacy Decision, Recital 18.

[37] Adequacy Decision, Recitals 9-11, 19, 120, 277 ("Continued adherence to [international human rights laws] is therefore a particularly important element of the assessment on which this Decision is based").

[38] Adequacy Decision, Recitals 51-73, 104-111, 274 ("taken as a whole, the oversight mechanisms and redress avenues in United Kingdom law enable infringements to be identified and punished in practice and offer legal remedies to the data subject to obtain access to personal data").

[39] This occupied the majority of the decision: Adequacy Decision, Recitals 112-272. It was also the primary point considered by the EDPB: EDPB Opinion, [24]-[34], [117]-[215].

[40] Adequacy Decision, Recitals 122-141, 175-243. Addressed with particular care was the use of "bulk" interception powers by intelligence agencies under Part 6 of the Investigatory Powers Act 2016 ("**IPA 2016**"). See Recitals 216-240, 250-260, 263-272. The IPA 2016 introduced transparency and new safeguards, including the requirement that warrants be approved by a Judicial Commissioner, and replaced piecemeal oversight mechanisms with the Investigatory Powers Commissioner's Office.

[41] Adequacy Decision, Recitals 220, 224-225, 226-230, 234-235, 238-240, 275.

[42] Adequacy Decision, Recitals 157, 174, 244-272, 274-275.

[43] Adequacy Decision, Recitals 116-120, 270.

(2) The Commission also noted the **sharing of data between UK agencies and agencies in third countries**.[44] The Commission was on balance satisfied that there were sufficient safeguards in place to protect EU persons' data from being transmitted overseas.[45] The Commission however acknowledged the sensitivity of international transfers of data from the UK more generally.[46]

(3) The Commission reserved its position as to the **immigration exception** (at that time in paragraph 4(1) of Schedule 2 to the DPA). At the time, there was a Court of Appeal decision which considered the exception to be incompatible with EU law and the Commission noted that the position would be reviewed at a later date.[47] Since then, the Government has introduced legislation seeking to address the position and the ICO has indicated that the legislation would suffice in meeting the requirements of the Court of Appeal decision.[48]

18. The tone of the Adequacy Decision was generally supportive of the UK system. This reflected both the UK's continued close adherence to the GDPR at the time of the decision and the pragmatic inclination of the Commission – backed on the whole by business and law enforcement on both sides of the EU-UK divide – to maintain a blanket authorisation for EU-UK data flows.

---

44 Adequacy Decision, Recitals, 142-156, 242-243.

45 Adequacy Decision, Recitals 153-156. The EDPB however had "strong concerns" in relation to this agreement: EDPB Opinion [88]. Similarly, the European Parliament noted in its Resolution dated 11 May 2021 ("**Resolution**") that it was "deeply concerned that this will allow undue access to the personal data of EU citizens and residents by US authorities": [25].

46 Adequacy Decision, Recitals 74-81.

47 Adequacy Decision, Article 1(2) and Recital 6. The relevant Court of Appeal decisions are *Open Rights Group v SSHD* [2021] EWCA Civ 800 and [2021] EWCA Civ 1573. There was a further decision in *the3million v SSHD* [2023] EWCA Civ 1474.

48 See "ICO responds to Home Office's draft regulations to the immigration exception".

(iii) Factors likely to influence the renewal of the Adequacy Decision

19. When it comes to reconsider the Adequacy Decision, the EU Commission is likely to be well aware of the continuing commercial importance of data flows between the EU and UK,[49] as well as the importance of retaining adequacy for the operability of provisions in the Withdrawal Agreement and the Trade and Cooperation Agreement.[50]

20. However, there are a range of legal factors which will constrain the Commission's ability to grant an adequacy decision simply based on pragmatic factors:

    (1) First, recent history suggests that there is a real risk of a successful legal challenge to an adequacy decision, whether at the suit of an EU-based individual, an NGO or the European Parliament. The Commission will no doubt be mindful of the way in which the CJEU criticised its approach in *Schrems II* in particular, including by delving into various points of detail to which the Commission had given the green light. More generally, the CJEU has in recent years consistently taken a more absolute line than the Commission (and most of the Member States) in defence of fundamental privacy rights, striking down previous EU-third country agreements[51] and even EU legislative measures.[52] The

[49] For example, the Commission has stated in its Communication dated 10 January 2017 that when it pursues dialogues in respect of adequacy it will take into account the extent of commercial relations with the country, geographical ties, cultural ties, and the overall political relationship. The Communication indicates the Commission's awareness that free data flows facilitate trade. In addition, the EU might also be mindful of retaining the UK's determination of EU adequacy: paragraphs 4 and 5 of Schedule 21 to the DPA.

[50] EU data protection obligations and the significance of the adequacy decision is apparent from Article 71 of the Withdrawal Agreement as well as Articles 201-202, 525, and 769 of the Trade and Cooperation Agreement. For a detailed discussion of the Trade and Cooperation Agreement see David Erdos, 'The UK and the EU personal Data framework after Brexit: A new trade and cooperation partnership grounded in Council of Europe Convention 108+', (2022) 44 *Computer Law & Security Review* 105639.

[51] As noted above, the CJEU struck down the EU-US Safe Harbour Agreement in *Schrems I* and the EU-US Privacy Shield in *Schrems II*. After *Schrems I*, the European Parliament also successfully challenged an EU-Canada agreement for the sharing of Passenger Name Records ("**PNR**") on the grounds that it was incompatible with fundamental rights: Case C-1/15 Opinion of the Court (Grand Chamber) (ECLI:EU:C:2016:656).

CJEU has proved more interventionist in this area than the European Court of Human Rights ("**ECtHR**") in Strasbourg.[53] It therefore remains a distinct possibility that an Adequacy Decision could be challenged in EU courts.[54] The Commission understands this well and will not wish to expose its decision to what it considers to be unacceptable legal risk. The prospect of a successful legal challenge in the EU courts also constitutes an independent risk of which the UK must be mindful as well.

(2) Second, the Commission will pay regard to the views of other EU institutions and Member States (in the comitology process and through representatives on the EDPB Board) which may take a more stringent approach. As was the case for the original Adequacy Decision, we consider it likely that the Commission will take into account the views of the EDPB,[55] and any concerns identified by resolutions in European Parliament. We note, for instance, that the European Parliament's powerful LIBE Committee recently wrote directly to the UK House of Lords Committee about its concerns about the DPDI Bill;[56] it is clear that those concerns will continue to be shared with the Commission.

---

52 The CJEU invalidated the EU Data Retention Directive in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications* (ECLI:EU:C:2014:238) ("***Digital Rights Ireland***") as being incompatible with EU fundamental rights and freedoms, in particular Article 7 (right to privacy) and Article 8 (protection of personal data) under the Charter of Fundamental Rights: [69]. Challenges were then brought to related domestic laws in the UK and in Sweden, and then referred by domestic courts to the CJEU. The CJEU confirmed that the domestic laws on data retention were inconsistent with EU laws and principles: Joined Cases C-203/15 *Tele2 v Post-och telestyrelsen* and C-698/15 *Secretary of State for the Home Department v Watson* (ECLI:EU:C:2016:970) ("***Watson***") [112], [125].

53 Judges Pandaros and Eicke of the ECtHR noted in *Big Brother Watch v UK* (First Section judgment of 13 September 2018; Joint Opinion at [22]; see now Grand Chamber judgment of 25 May 2021) that the approach of the ECtHR was in "clear contrast" to that of the CJEU, which they described as having adopted (in cases such as *Digital Rights Ireland* and *Watson*) "a more prescriptive approach as regards the safeguards it considers necessary".

54 See for example in respect of the original Adequacy Decision: Oscal Stephen Kelly, "The UK Adequacy Decision and the Looming Possibility of a Schrems III" on the King's Law School EU Law Blog. There has indeed been a challenge to the latest US adequacy decision as well: Case T-553/23 *Latombe v Commission* (where interim relief was refused but it appears the case has not yet concluded).

55 The original Adequacy Decision was heavily informed by the EDPB Opinion of 13 April 2021. Wherever the EDPB Board expressed reservations about aspects of the draft decision, those were addressed in more detail in the final decision.

56 Letter dated 22 April 2024 from the LIBE Committee Chair to the House of Lords Adequacy Decision Committee. The letter identifies a range of issues including the independence of the ICO, third country transfers, and the definition of personal data. The letter also makes overarching observations that it is "concerned about the overall direction of the data policies of the UK

(3) Third, the Commission must – in accordance with ordinary EU principles of effectiveness, legal certainty, and transparency – give detailed reasons explaining the basis for its view that divergences in the UK contain sufficient safeguards to ensure an adequate level of protection for personal data originating in the EU. The starting point will be the wording of the UK legislation and the operation of data protection in practice. This will include examining carefully the material changes proposed by the DPDI Bill and the overall trajectory of UK data protection laws from its EU origins. As with the original Adequacy Decision the EU will need to derive comfort that there are sufficient safeguards in place for fundamental privacy rights notwithstanding divergences in different areas. If there is a real difficulty identified in the DPDI Bill, then the Commission could potentially seek further commitments or other bespoke arrangements from the UK, as it has done with countries such as Japan.

(4) Fourth, the Commission is likely to take into account the wider legal landscape in both the UK and the EU. As far as the EU is concerned, it has introduced ambitious new rules under the Digital Services Act and Digital Markets Act which among other things reinforce the EU's commitment to data protection.[57] The Commission has also looked favourably upon third countries whose data protection laws have – over time – converged towards the high standards imposed by the EU.[58] Going forward, the EU will also be looking to update and refine the EU GDPR in coming

---

Government" and "observes a switch towards using executive legislative powers in these policies with limited oversight from the UK Parliament".

[57] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) and

[58] See the Review Report dated 15 January 2024 noted above.

years.[59] As regards the UK, the EU will be mindful of the reforms in the Retained EU Law (Revocation and Reform) Act 2023 ("**REULA**") which have been introduced specifically to promote divergence between the EU and UK and to give powers to the Executive to amend and restate retained EU law. This includes the abolition of supremacy of EU law.[60] The Commission will also be aware that the UK no longer applies the EU Charter of Fundamental Rights (the "**Charter**") which provides a specific right of data protection in Article 8.[61] Finally, the Commission will be paying close attention to any mooted reforms of the Human Rights Act 1998 or the UK's continued adherence to the ECHR.[62]

21. As for timing, we note that the Adequacy Decision expires on 27 June 2025. It appears likely that a draft decision will be available in early 2025 which will then be subject to commentary from the EDPB Board, the European Parliament, and further revision in the comitology process. We assume, for the purposes of this Opinion, that the DPDI Bill will have received Royal Assent in the UK by that time and will be taken into consideration by the EU institutions.

---

[59] See the Commission's Report on the application of the GDPR which is due to be adopted later this year following a call for evidence between 11 January 2024 and 8 February 2024.

[60] Section 3 of REULA.

[61] We note, however, that the UK has introduced legislation making clear that references to "fundamental rights" in the UK GDPR should be understood by reference to the privacy rights in Article 8 of the European Convention on Human Rights. See The Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023.

[62] While the Bill of Rights Bill, which was a proposal to pare back the influence of the ECHR, has been abandoned, certain political issues such as immigration (e.g. the interim relief decision in the Rwanda litigation in the European Court of Human Rights (*N.S.K. v. the United Kingdom* (application no. 28774/2)) have led to suggestions by Members of Parliament that the UK should withdraw from the ECHR. From the EU perspective, that would be a radical change to the legal landscape which may require wholesale reconsideration of adequacy.

C. Assessing the DPDI Bill

22. Against that background, we turn to consider the legal consequences of the DPDI Bill and whether it poses any genuine risk to the renewal of the Adequacy Decision.

(i) Introduction to the Bill

23. As a starting point, we note that the DPDI Bill is a very complex piece of legislation. It takes the form of a large number of amendments to existing legislation, in particular the UK GDPR and DPA. While it does not fundamentally alter the architecture of those pieces of legislation, it makes a number of encroachments upon the data protection framework that was retained immediately after Brexit. Many of the changes appear technical in nature but are, in our view, more substantive than is immediately apparent. In this regard it is worth recalling that the clear intention of the DPDI Bill is to give effect to the perceived advantages of Brexit.[63] It is therefore necessary to consider the changes in detail to determine how far they represent a shift to the existing framework.

24. We have considered the DPDI Bill and the Explanatory Memorandum in detail and identified a number of changes to the UK GDPR and DPA which are likely to merit close scrutiny by the EU institutions. We discuss each of these further below:

    (1) **The role of the ICO.** The ICO will be required to pay regard to the Secretary of State's strategic and policy objectives and will have broader powers to refuse to action a complaint. This is likely to be a point of concern for EU institutions, in particular because

[63] Paragraph 2 of the Explanatory Notes to this Act makes clear that the new legislation expressly gives effect to policies set out in the Benefits of Brexit Report published by the Government. In addition we note the Press Release dated 23 November 2023 where it is suggested that common sense changes in the DPDI Bill will help to "safeguard the public, prevent fraud and unlock post-Brexit opportunities".

the strategic objectives are subject to uncertainty because of the prospect of further amendment by secondary legislation.

(2) **Lawful bases.** The list of lawful bases for data processing will be expanded, in particular by adding a new lawful basis of "recognised legitimate interests" where no balancing exercise is required. The amendments also enable the Secretary of State to add further legitimate interests to the list. These are fundamental amendments to core concepts in the UK GDPR, some of which are delegated to secondary legislation.

(3) **Third country transfers**. The basis on which data can be transferred from the UK to other third countries has been liberalised. This is likely to be carefully examined by the Commission because third country transfers are an express requirement of the adequacy assessment under the EU GDPR. The underlying policy concern would be the risk of "data laundering" through the UK.

(4) **Processing by political parties, public bodies and businesses.** There are many ways in which data processing has been expanded into new categories and we consider three of these in particular as potentially significant for the EU Commission.

(5) **Undermining the practical utility of data rights.** The DPDI Bill contains proposals which are intended to reduce the burden on businesses in complying with the GDPR but in our view also undermine the practical enforceability of data subject rights.

25. In addition to the subject-matters identified above, throughout the DPDI Bill significant powers are given to the Secretary of State to make

further amendments to fundamental data rights concepts by way of **secondary legislation**. We discuss those below as appropriate and we note the criticisms made by the Delegated Powers and Regulatory Reform Committee in this regard.[64] As far as the EU institutions are concerned, delegating significant powers to the Secretary of State under the DPDI Bill could have the effect of reducing legal certainty, predictability and transparency, and therefore impair confidence in an overall guarantee of adequacy.

(ii)The role of the ICO

26. The independence of the ICO is of crucial importance in any decision by the EU Commission to renew the adequacy decision. Indeed, it is an express requirement in the EU GDPR when determining adequacy.[65] It is also part of the EU Commission's overall assessment of certainty and enforceability of the rules in practice. Thus, in the existing Adequacy Decision, the Commission noted that independent supervision ensures that any interference with privacy rights under human rights legislation had the necessary quality of law.[66] At the time, the European Parliament had gone further than the Commission and recommended that the ICO should be made entirely independent from the Government.[67] We therefore consider it likely that any changes to the position of the ICO will attract significant scrutiny.

---

64 See the 10th Report of the Delegated Powers and Regulatory Reform Committee Session 2023-24.

65 Article 45(2)(b) of the EU GDPR.

66 Adequacy Decision Recital 117. See also Adequacy Decision Recital 85, 87 ("The authority should act with complete independence and impartiality in performing its duties and exercising its powers"). See further Recital 281 ("Amongst other elements, case law developments and oversight by the ICO and other independent bodies will inform the Commission's monitoring"). The GDPR also emphasises independence of the supervisory body whether in Member States or in third countries: Articles 45(2)(b), 52 and Recitals 104, 117, 121. For example, Recital 104 states "the third country should ensure effective independent data protection supervision".

67 Resolution dated 21 May 2021 [8]. See also Resolution [6] ("expresses its concern about the lack and often non-existent enforcement of the GDPR by the UK when it was still a member of the EU; points, in particular, to the lack of proper enforcement by the [ICO] in the past").

27. As regards the ICO's role, the DPDI Bill includes new provisions in the DPA to update the approach to the ICO's strategic priorities and its response to complaints. We note the following in particular:

(1) **Strategic priorities.** Under proposed section 120B, the ICO is required to have regard, as far as relevant in the circumstances, to matters such as "*the desirability of promoting innovation*" and the "*importance of the prevention, investigation, detection and prosecution of criminal offences*" as well as the "*need to safeguard public security and national security*". These objectives are in addition to its primary objective which is to secure an appropriate level of data protection and promote public trust and confidence in data protection: proposed section 120A.

(2) **Additional strategic priorities.** Under proposed section 120E, the Secretary of State may issue a statement of "*strategic priorities*" which sets out the priorities of the Government with respect to data protection.[68] Under proposed section 120F, the ICO is under a duty to have regard to that statement of strategic priorities when carrying out their functions, and to "*explain in writing*" how the ICO will do so. This obligation does not apply to individual investigations.[69]

(3) **Actioning complaints.** Under proposed section 165A, the ICO is given additional powers to refuse to act on complaints, including if there is any pending complaint with the controller or the complaint is "*vexatious*" or "*excessive*" by reference to criteria such as the nature of the request and the relationship between the sender and

[68] That statement is to be laid before Parliament under proposed section 120H of the DPA.

[69] Proposed section 120F(2) of the DPA.

recipient.[70] The ability of individuals to complain was of course taken into account in the EU's assessment in the Adequacy Decision.[71]

28. We consider the first two changes to be significant. In particular, even though the incorporation of broader objectives for the ICO might not be objectionable *per se* to the EU institutions, these changes do reflect a material shift in the independence of the ICO insofar as the ICO is required to account for various Government policy objectives rather than have a single-minded focus on the protection of data rights. The EU Commission is likely to be highly sceptical of any political interference with the ICO's role given that the effectiveness of the ICO was an important facet of the existing Adequacy Decision.[72] We therefore consider it likely that the EU Commission will seek to understand further how this will impact the day-to-day effectiveness of the ICO and is likely to be concerned about any further alignment between the ICO and the Government.

29. More generally, we consider that the Commission will be fundamentally focused on the practical enforcement of data rights. This is important because adequacy requires infringements to be "identified and punished in practice".[73] The risks of reducing the ICO's independence is also significant because the weakness of the UK's existing regime was already identified as a problem by the European Parliament before the Adequacy Decision was formally adopted.[74]

---

[70] Proposed section 204A of the DPA. In this regard we note that, even prior to the proposed changes, the UK system for complaints to the ICO did not guarantee a substantive resolution. This is because the Commissioner need only investigate complaints "*to the extent appropriate*": Section 165(4)-(5) of the DPA. The right to apply to the First Tier Tribunal under s. 166 of the DPA is also limited to procedural rather than substantive failures on the part of the ICO: *Leighton v The Information Commissioner (No. 2)* [2020] UKUT 23 (AAC) [31].

[71] Adequacy Decision Recitals 96, 105-106. The right to lodge a complaint is set out in Article 57(1)(f) and Article 77 of the GDPR and the UK GDPR.

[72] Adequacy Decision, Recitals 85-98.

[73] Adequacy Decision Recital 274, drawing on the EDPB Adequacy Referential p. 8.

(iii) Lawful bases for processing

30. Article 6 of the UK GDPR (deriving from Article 6 of the EU GDPR) establishes one of the cornerstones of data protection law, which is that there must be a "lawful basis" for any processing of personal data. There is a closed list of conditions, such as "consent", "necessity" or "legitimate interest", one of which must be satisfied for the data processing to be lawful.

31. The DPDI Bill introduces substantive amendments to Article 6 through the inclusion of new lawful bases known as "**recognised legitimate interests**" or "**RLIs**". By way of context, the existing GDPR provisions treat "legitimate interests" as a lawful basis but that is subject to a balancing test to account for individual privacy rights. Article 6(1)(f) of the UK GDPR currently provides that the processing will be lawful if it is "*necessary for the purposes of the legitimate interests*" pursued by the controller "*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*." In other words, where the controller relies on a legitimate interest, there is a balancing exercise undertaken between the legitimate interest and the countervailing rights of the data subject (the "**balancing test**").

32. The balancing test has been regarded as a fundamental protection of individual privacy and data rights,[75] and has been in place for many years in both the EU and the UK.[76] The continuation of these key

---

[74] See Resolution, [6] ("expresses its concern about the lack and often non-existent enforcement of the GDPR by the UK when it was still a member of the EU; points, in particular, to the lack of proper enforcement by the [ICO] in the past").

[75] Under Article 6(1)(f) of the GDPR and the UK GDPR. Recital 47 of the GDPR explains that the balancing test requires considering the reasonable expectations of data subjects based on their relationship with the controller. The interests of the individual could in particular override the interest of the data controller "where personal data are processed in circumstances where data subjects do not reasonably expect further processing".

concepts was presumed by the Commission in the Adequacy Decision.[77] However, that balancing test has been removed in respect of "recognised" legitimate interests in the DPDI Bill. In particular, proposed Article 6(1)(ea) will provide that processing will be lawful where it is "*necessary for a recognised legitimate interest*" and the balancing test is removed for RLIs. The enumerated RLIs are set out in Annex I of the DPDI Bill (see proposed Article 6(5)) and include matters such as "*detecting, investigating or preventing crime", "national security*", "*public security*", "*defence*", "*safeguarding vulnerable individuals*" and "*democratic engagement*".[78] These categories are, on their face, potentially extremely wide, and provide a blanket lawful basis so long as the processing can come within the definition. We consider that the EU may be particularly conscious of provisions as to defence and national security, given its existing concerns about access by law enforcement agencies and security services noted above. Finally, as discussed further below, the Secretary of State is empowered to add or delete provisions in Annex I, and thus to update and amend the lawful grounds of processing even further by delegated legislation.

33. We note that, as a matter of presentation, the introduction of "recognised legitimate interests" does not change the structure of Article 6. However, despite the label, RLIs are essentially entirely new lawful bases added to the previously closed list in Article 6 of the UK GDPR. There is no balancing test so there is no fact-sensitive, case-by-case assessment of whether the legitimate interest is being pursued in a proportionate way vis-à-vis individual privacy rights. Rather, these RLIs provide for blanket authorisation for the enumerated interests. The

---

[76] Article 7(f) of the Data Protection Directive and s. 4 and para. 6 of Schedule 2 of the Data Protection Act 1998.

[77] Adequacy Decision Recital 25.

[78] The breadth of the concept of democratic engagement is discussed further below.

wholesale removal of the balancing test is highly significant given that, at least until now, the concept has been embedded in UK case law.[79] It is also the foundation for important protections such as "the right to be forgotten" which was developed in the well-known *Google Spain* decision.[80] The jettisoning of this test in favour of potentially wide-ranging RLIs is a material shift in approach.

34. Finally, we consider that the ability of the Secretary of State to add new RLIs to Article 6[81] is notable because it gives the executive significant power to update and amend lawful bases of processing without having to introduce primary legislation.[82] We note that this particular use of secondary legislation powers has been criticised by the Delegated Powers and Regulatory Reform Committee in the House of Lords as follows:

> The grounds for lawful processing of personal data go to the heart of the data protection legislation, and therefore in our view should not be capable of being changed by subordinate legislation. This on its own in our view makes the power inappropriate. But we are also not convinced that the Department has provided strong reasons for needing the power. Those reasons are based on the possibility that new difficulties might emerge with the application of the balancing test in Article 6(1)(f) of the UK GDPR. We do not find that convincing given that the relevant test has been present in the legislation since the UK GDPR first had effect.

---

79 See for instance *R (M) v Chief Constable of Sussex Police* [2021] EWCA Civ 42 [25]: "Article 6(i)(f) of the GDPR expressly provides that processing of personal data for a legitimate interest may be overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. That is an operative provision which creates substantive rights."

80 Case C-131/12 *Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD)* (ECLI:EU:C:2014:317) [80]-[81] ("In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing.")

81 New Article 6(7) and (8) provide that, before laying regulations, the Secretary of State must have regard to the effects of any changes on the interests and fundamental rights and freedoms of data subjects, particularly children. The regulations must be made by statutory instrument and are subject to the affirmative procedure.

82 This was a point identified by the Select Committee on the Constitution in its report on the DPDI Bill at [6] ("The House may wish to examine further the breadth of the Secretary of State's powers in clauses 5 and 6 and consider whether such changes to the regulation of personal data should be the subject of primary rather than secondary legislation").

35. We note also that while the Secretary of State must "have regard" to data subject rights when introducing new RLIs,[83] this is much less strict than the case-by-case balancing test that is mandated by the existing provisions of Article 6 of the UK GDPR. In general, the expansion of regulation-making powers is likely to be a point of concern for the Commission,[84] in part because it affects the Commission's ability to assess the adequacy of the legislative framework because that framework is uncertain and unpredictable going forward.

(iv) Third country transfers

36. In its consultation, the Government made clear its intention to reduce barriers to data flows into third countries from the UK.[85] At present, Article 45 of the UK GDPR reproduces the approach to adequacy in the EU GDPR. In other words, the Secretary of State is required to issue a decision as to whether to permit data flows to a third country on the basis of the third country's adequate protection of data.[86]

37. The DPDI Bill amends these provisions as follows:

    (1) **Adequacy regulations.** Article 45 of the UK GDPR is repealed. The Secretary of State is still required to make regulations approving transfers of personal data to third countries under the proposed Article 45A of the GDPR. However:

        (a) The adequacy test is replaced with a "*data protection test*" set out in Article 45B. Under the data protection test, the

[83] Proposed Article 6(7) of the UK GDPR.

[84] For example including the broad powers in the proposed in sections 150-151 of the DPDI Bill.

[85] Consultation, Chapter 3 [229]-[270].

[86] Article 45 of the UK GDPR and section 17A of the DPA.

third country must not provide "*materially lower*" data protection.[87]

(b) As regards the factors to be taken into account, the Secretary of State may take into account the "*desirability of facilitating transfers*" of personal data to and from the UK in addition to the third country's respect for rule of law, human rights and redress.[88] The requirement for an "independent" supervisory authority has been removed.[89] The requirement for "judicial redress" has also been removed.[90] This latter point is potentially significant under EU law as it is inherently tied up with the EU conception of the right to a fair trial and judicial determination.[91]

(c) There is an ongoing obligation to monitor but the mandatory four-year review has been removed under Article 45C.[92]

(2) **Alternative transfer mechanisms**. The DPDI Bill also contains changes to increase reliance on the alternative transfer mechanisms for third country data flows aside from adequacy decisions. At present, alternative transfer mechanisms involve shifting the burden onto the controller or processor (usually in the UK) to impose appropriate safeguards, such as standard contractual clauses, to achieve an adequate level of protection.

---

87 Proposed Article 45A(2) of the UK GDPR.

88 Proposed Article 45B(2) of the UK GDPR.

89 Compare Article 45(2)(b) of the EU GDPR ("one or more independent supervisory authorities") with the proposed Article 45B(2)(b) of the UK GDPR ("an authority responsible for enforcing the protection of data subjects.").

90 Compare Article 45(2)(a) of the EU GDPR ("effective administrative and judicial redress") with the proposed Article 45B(2)(c) ("arrangements for judicial or non-judicial redress").

91 The link is drawn in Recital 141 and Articles 77 and 78 of the EU GDPR. Note also that the CJEU fixated heavily on a lacuna for "judicial redress" when striking down the EU-US arrangements for data adequacy. See *Schrems I* at [95]. In *Schrems II*, the CJEU was clear that an Ombudsman was not a mechanism for providing judicial redress as guaranteed by Article 47 of the EU Charter of Fundamental Rights, which is the EU equivalent of a right to a fair trial, as well as the rights inherent in the rule of law: [187]-[197].

92 Proposed Article 45C of the UK GDPR.

The DPDI Bill proposes to reduce the burden on organisations by requiring them to consider what is proportionate with respect to specified safeguards,[93] and permitting the Secretary of State to make regulations for further safeguards by reference to the "*data protection test*" noted above.[94] The amendments also permit the use of blanket derogations, again to be introduced in secondary legislation by the Secretary of State.[95]

38. These changes would be of significance to the Commission and in particular the CJEU because "*onward transfers*" are a mandatory consideration in the EU GDPR when assessing adequacy: Article 44 and Article 45(2)(a). In other words, the EU is expressly required to consider whether an adequacy decision would permit onward transfers to further third countries with lower levels of protection. Under EU law, the logic for this requirement is that the level of protection should not be compromised despite the transfers across borders; there should be a continuity of protection.[96]

39. We consider that the current proposal in the UK DPDI Bill waters down the test for adequacy from the UK. Instead of "*essential equivalence*", the third country need only ensure that its level of protection is not "*materially lower*" than that in the UK. This is, on its face, a minor amendment. However, the language used ("*materially*") is more permissive than that in the EU GDPR and is open to interpretation by a court. It is entirely possible that this would give the Commission and the CJEU pause for thought. The concern would be that the Adequacy

---

93 Proposed Article 46(1A)(a)(ii) and 46(6)-(7) of the UK GDPR.

94 Proposed Article 47A(4)-(7) of the UK GDPR.

95 Proposed Article 49(4A) of the UK GDPR. This is rather different from the narrow and "one-off" derogations in Article 49 of the EU GDPR. See EU GDPR Recitals 112-113, EDPB Opinion [97]-[98], Resolution dated 21 May 2021 [39].

96 GDPR Recital 101.

Decision could permit the UK to become a conduit for data transfers from the EU to third countries with lesser protections. By way of context, we note that the Government had indicated that the purpose for these reforms was to have a more flexible approach to assessing adequacy. The "priority destinations" for adequacy include at present Australia, the Dubai International Financial Centre, India, Colombia, Singapore and Brazil.[97]

40. In addition, the increased emphasis on alternative transfer mechanisms is likely to be examined closely by the Commission. As with other areas of the DPDI Bill, the detail is left to be worked out in secondary legislation and may lead to significant increases in third country transfers over time.[98] It is likely to be difficult for the EU institutions to forecast the extent of these divergences but it will certainly have regard to the usual EU principles of transparency, certainty, and lawfulness in assessing the risks to data subjects from the expanded role of secondary legislation in this context.

(v) Liberalisation of data use by political parties, public bodies and businesses

41. The DPDI Bill makes a number of seemingly minor amendments which broaden out the scenarios in which data can be lawfully processed by businesses and political parties. For example:

(1) **Political activities.** Proposed section 21A in the DPA widens the circumstances in which data reflecting a person's political opinion (which is sensitive data)[99] can be processed by political parties.

---

97 See "International data transfers: building trust, delivering growth and firing up innovation" available online.

98 See for a comprehensive overview of delegated powers the 10th Report of the Delegated Powers and Regulatory Reform Committee. See also the four Delegated Powers Memoranda available online.

99 UK GDPR Article 9 and Recital 51 ("Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedom merit specific protection as the context of their processing could create significant risks to the fundamental

The processing can now be done by registered political parties, candidates for election, permitted participants in referendums, or accredited campaigners in connection with "*democratic engagement*" which is very broadly defined and appears to extend to fundraising activities.[100] Such processing is not permitted if it is likely to cause "*substantial damage or substantial distress*" to an individual or if the individual gives express "*notice in writing*" requiring the controller to cease processing.[101] This will work in conjunction with provisions enabling direct marketing for the purposes of democratic engagement.[102] These appear to be significant amendments which legitimise widespread data-processing in connection with any electoral or campaigning process. Such provisions are unknown to EU laws and are likely to be examined closely by the Commission.

(2) **DWP access to benefits data.** One major change which was introduced in the report stage in the House of Commons was to permit the Department for Work and Pensions to require banks and financial organisations to provide it with data about accounts held by benefits claimants.[103] The purpose of this is to detect benefits fraud,[104] but the power is available in respect of anyone

---

rights and freedoms.")

[100] Proposed section 21A(5) defines democratic engagement as "engagement by the public, a section of the public or a particular person with, or with an aspect of, an electoral system or other democratic process in the United Kingdom, either generally or in connection with a particular matter, whether by participating in the system or process or engaging with it in another way" and includes fundraising activities (see proposed section 21A(5)(c)(vi)). There was already a limited provision for processing for democratic engagement in the public interest under section 8(e) of the DPA but this has been broadened in the proposed amendments.

[101] Proposed section 21A(3) and (4) of the DPA.

[102] The Secretary of State is empowered to make exceptions from direct marketing provisions in the Privacy and Electronic Communications Regulations (known as "**PECR**") in section 114 of the DPDI Bill. Again, a broad definition of democratic engagement is set out in section 115 of the DPDI Bill. The Consultation had made this proposal clear: Consultation [222]-[223]; ICO Response to Consultation [105], [107].

[103] Schedule 11 in the DPDI Bill introduces new powers in the Social Security Administration Act 1992.

[104] The Secretary of State for Work and Pensions has commented in the DPDI Bill Press Release that the new powers will be aimed at "rooting out fraudsters at the earliest possible opportunity".

on benefits even they are not means-tested.[105] This widespread access appears to be permitted without any particular grounds for suspicion and is likely to be a cause for concern when the EU considers the Adequacy Decision,[106] including in particular if the powers impact EU individuals (e.g. those who have bank accounts in the UK).

(3) **Expansion of scientific research.** The proposed Article 4(3) of the UK GDPR will broaden out the definition of data processing for scientific research to cover "*processing for the purposes of any research that can reasonably be described as scientific*" including "*privately funded*" research that is carried out as a "*commercial activity*". The word "scientific" is not explicitly defined but it would appear likely to cover commercial enterprise that is connected with research that is directed towards technological advancement,[107] or even market research. This has knock-on consequences because scientific research provides a basis for further processing (proposed Article 8A), extends the time limit for retention (Article 5(1)(e) of the UK GDPR), provides a justification for processing sensitive data (Article 9(2)(j)) and provides exemptions from the right to erasure and right to object (Article 17(3)(d) and 21(6) of the UK GDPR). Given that this was identified in the Adequacy Decision as an area to monitor,[108] we consider it will be examined carefully by the Commission in its renewal decision.

---

[105] See the definition of "relevant benefits" in proposed section 121DA of the Social Security Administration Act 1992.

[106] The ICO has explained its concerns about these provisions in its updated response to the DPDI Bill. The Select Committee on the Constitution has also been critical of the scope of the powers, see its Report at [15]-[18]. The new powers have been criticised by organisations such as JUSTICE as well ("JUSTICE considers Clause 128 and Schedule 11 of the Bill to be unlawful, lacking in evidence, and to undermine the rule of law", JUSTICE Report at [3]).

[107] See proposed Article 4(4)(a).

[108] Adequacy Decision, Recitals 71-73.

42. The above are three discrete illustrations which widen access to personal data for political, governmental and commercial use. We are not able to comment on every single such amendment of this kind but have identified the above as examples. It is not possible to predict how these powers would be used in practice and who they would affect. But we do consider that the EU institutions will look carefully at these changes, in the round, when assessing adequacy. Each of these represents shifts from the EU origins of the UK rules and represent a concerted attempt to be more permissive – and therefore strike a slightly different balance than the EU – in the use of personal data to achieve other policy and commercial objectives.

(vi) Weakening data subject rights

43. The DPDI Bill aims to give effect to the objective of reducing burdens on businesses in numerous ways. This includes various amendments that favour the convenience of controllers over data subject rights, such as:

(1) **Exercise of data subject rights.** Proposed Article 12A UK GDPR enables data controllers to more readily refuse (or charge a fee for) data subjects' exercise of their rights in Chapter III UK GDPR. This covers data access requests as well as lesser-known but important rights such as the right to rectification, erasure, and to object to processing. Proposed Article 12B UK GDPR also extends the time for compliance. Previously, refusing or charging a fee for data requests was permitted only if the request was "*manifestly unfounded or excessive*" whereas now the test is "*vexatious*" or "*excessive*". The factors to be considered in deciding whether a request is vexatious include "*the resources available to the controller*" and the "*nature of the request*". Examples of vexatious

requests include requests which are "*not made in good faith*".[109] These changes are perhaps intended to reflect concepts from Freedom of Information legislation,[110] but Chapter III data rights are concerned with individuals accessing their own data and controlling how it is processed. For example, the case law suggests that it is not open to data controllers to ask why a data subject is requesting their data; the request has to be answered even if the subject has a collateral purpose in making that request.[111] It is unclear how this can be reconciled with a requirement of good faith. In its original Adequacy Decision, the Commission had noted that data subject rights were included in the UK GDPR and were practically enforceable,[112] and we consider that it is likely to scrutinise these changes closely.[113]

(2) **Re-use of data for new purposes.** The UK GDPR currently includes a purpose limitation principle, i.e. if a data controller collects data for a particular purpose, they cannot then process it further for an incompatible purpose.[114] This has a provenance going back decades in the EU Data Protection Directive 1995 and the UK Data Protection Act 1998.[115] The rationale is that the data subject should know at the time of collection why their data is being collected and what will be done with it.[116] The DPDI Bill

---

[109] Proposed Article 12A(4).

[110] See section 14 of the Freedom of Information Act 2000.

[111] *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74 [107] ("We have been shown nothing in the DPA or the Directive which limits the purpose for which a data subject may request his data, or provides data controllers with the option of not providing data based solely on the requester's purpose").

[112] Adequacy Decision Recital 51, 53, 104, 124-125, 170 fn 251; Article 15 of the UK GDPR and the EU GDPR. Note also Recital 104 of the EU GDPR which states in respect of adequacy that "data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress".

[113] The CJEU has been strengthening data access rights in recent cases, see e.g. Case C-579/21 *JM v Pankki S* (ECLI:EU:C:2023:501).

[114] Article 5(1)(b) of the UK GDPR.

[115] Article 6(1)(b) of the Data Protection Directive and s. 4 and para. 2 of Part 1 of Schedule 1 of the Data Protection Act 1998. As the ICO noted in its Response to the Consultation, "these are fundamental principles" so "it is important to address them fully in order to maintain public confidence": [6].

provides for a new Article 8A in the UK GDPR which would permit further processing in certain circumstances when it is done for research purposes[117] or for other purposes listed in Annex 2. These include "*public security*", "*emergencies*", "*detecting crime*", and "*safeguarding vulnerable individuals*".[118] Again, the Secretary of State is empowered to update the further purposes listed in Annex 2.[119] These are potentially significant changes given that the Adequacy Decision was premised on the assumption that the purpose limitation would be kept in place after Brexit.[120] In addition, the expansion of processing by law enforcement agencies and security services was specifically noted as a point of concern in the original Adequacy Decision.[121] Finally, we note the criticisms made by the House of Lords' Delegated Powers and Regulatory Reform Committee in giving these powers to the Secretary of State by way of secondary legislation.[122] Taken together, we consider that these changes could allow data to be used in ways that a subject can neither foresee nor control.

(3) **Automated decision-making**. The UK GDPR currently provides a right not to be subject to a decision based solely on automated processing.[123] This right was contained in the earlier legislation,[124]

---

[116] "When we share personal data with others, we usually have an expectation about the purposes for which the data will be used. There is a value in honouring these expectations and preserving trust and legal certainty, which is why purpose limitation is such an important safeguard, a cornerstone of data protection": Article 29 Working Party Opinion on Purpose Limitation p. 4 (the Article 29 Working Party is the predecessor to the EDPB).

[117] Proposed Article 8A(3)(b) of the UK GDPR. This, in turn, is affected by the broadening out of the definition of scientific research in the proposed Article 4(3) of the UK GDPR discussed above.

[118] Proposed Annex 2, paragraphs 3, 4, 5 and 8.

[119] Proposed Article 8A(5)-(8) of the UK GDPR.

[120] Recital 44.

[121] As noted above, these issues occupied the majority of the decision: Adequacy Decision, Recitals 112-272. It was also the primary point considered by the EDPB: EDPB Opinion, [24]-[34], [117]-[215].

[122] "The Department acknowledges in the memorandum that the rules governing further processing "relate to a fundamental principle in the UK GDPR that processing in a manner incompatible with the original purpose is not permitted". Given the fundamental nature of this principle, we do not consider it is appropriate to use subordinate legislation to make changes to the matters which are automatically to be treated as being compatible with the original purpose. The Department rely on unforeseen consequences arising from changes to legislation as the primary reason for the power. Again, we do not find this convincing": Report of the Delegated Powers and Regulatory Reform Committee at [10].

and the continuation of that right was taken into account by the Commission in its Adequacy Decision.[125] The DPDI Bill includes amendments in the form of a new Article 22A which provides that the protection only applies if there is "*no meaningful human involvement*" in the taking of the decision. This is in broad terms a restatement of the existing provisions but one notable change is that the Secretary of State is empowered to make regulations which would: (i) deem decisions as falling outside the scope of the provisions (by specifying whether a particular type of decision is taken to have meaningful human involvement or have significant effects on the data subject); or (ii) add or delete enumerated safeguards.[126] As noted above, it is significant that these sorts of changes can be introduced by secondary rather than primary legislation,[127] in particular where there is such uncertainty about the extent and prevalence of automated decision-making by governments and private bodies. By way of contrast, the EU approach to the use of AI has been to promote innovation whilst seeking to maintain data protection standards.[128]

44. We acknowledge that one of the primary aims of the Consultation was to reduce the perceived technicality and complexity of the law and to encourage the free flow of data.[129] However, in our opinion, proposals such as these might operate cumulatively to dilute the protection of

---

123 Article 22 of the UK GDPR and sections 49-50 of the DPA.

124 Article 15 of the Data Protection Directive and s. 12 of the Data Protection Act 1998.

125 Adequacy Decision Recitals 54-55, 124, 125 fn 156.

126 Proposed Article 22D, in particular Article 22D.

127 10th Report of the Delegated Powers and Regulatory Reform Committee at [14]-[15].

128 Proposal for an Artificial Intelligence Act dated 21 April 2021. It includes specific rules about data and data governance in particular for high-risk AI systems. It is expected to be adopted later this year.

129 The Consultation describes data as a "*strategic asset*" and expresses the view that the current rules are either "*too vague or overly prescriptive*". The Government's position is that being outside the EU permits the UK to "*operate a pro-growth and innovation-friendly regime*" that continues to maintain high standards of protection. See Consultation, [1]-[3].

individual data rights vis-à-vis controllers and may be viewed critically by EU institutions when considering the renewal of the Adequacy Decision.

D. Conclusion

45. The purpose of the DPDI Bill is to amend further the GDPR and DPA since the UK has left the EU, including to achieve a range of Government policy objectives post-Brexit. We consider that the substance of certain fundamental divergences identified above will constrain the ability of the Commission to approve an adequacy decision on purely pragmatic grounds. In particular, each of these divergences (and the uncertainty associated with their further amendment by secondary legislation) will individually and cumulatively increase the legal risks to which the Commission exposes itself when seeking to evaluate overall adequacy under the principles of the EU GDPR and applicable EU case law.

46. More generally, the changing trajectory of UK data protection rules from their EU origins will continue to be examined closely by EU institutions as the Adequacy Decision is considered for renewal in coming months. The EU will of course be influenced by the practical and commercial importance of maintaining data flows between the EU and UK. However, we consider that the cumulative effect of the legal changes described above – which may appear technical and insignificant at first glance – represent the weakening of foundational principles of data protection and privacy rights derived from EU law. There is of course an entirely independent risk of the CJEU striking down any adequacy assessment as well. Given the CJEU's approach to privacy rights in recent years, we

consider that it is possible that one or more of the above changes could fall foul of a strict judicial assessment of adequacy.

ALASTAIR SUTTON

AARUSHI SAHORE

Brick Court Chambers
7-8 Essex Street
London WC2R 3LD
29 April 2024

AWO

Received 2 May 2024