PROPOSED CHANGES TO UK DATA PROTECTION LAWS:
RISKS TO THE EU'S ADEQUACY DECISION

OPINION

A. Introduction and Summary

1. We are asked to advise on whether recently proposed changes to data protection laws could imperil the European Commission's Adequacy Decision in favour of the UK.

2. The Adequacy Decision concluded that the UK provided an adequate level of legal protection to personal data, and thereby enabled the free flow of data from the EU into the UK after Brexit.[1] The Government has launched a consultation on proposals to liberalise the UK's data protection regime to encourage innovation and economic growth (the "**Consultation**").[2] There is a concern that these changes could undermine the basis for the Adequacy Decision and lead to its revocation or suspension by the Commission and/or its invalidation by the Court of Justice of the EU ("**CJEU**").

3. For the reasons outlined below, we conclude that a number of the proposed changes represent significant divergences from the UK's existing laws on data protection. As such, they risk undermining some of the fundamental principles of EU data protection and therefore the foundation of the Adequacy Decision. In particular:

   (1) Proposals to ***reduce the regulatory burden on organisations*** are accompanied by consequent inroads on fundamental and long-standing data protection rights, such as the purpose limitation and the legitimate interests balancing test.

---

[1] Commission Implementing Decision of 28 June 2021. This is the Adequacy Decision made under the GDPR (defined below). There is also a further Implementing Decision under the EU Law Enforcement Directive which is not discussed here, though it may raise similar issues.

[2] Data: a new direction, launched by the Department for Digital, Culture, Media & Sport ("**DCMS**") on 10 September 2021. The Consultation is part of the National Data Strategy launched in September 2020. Parts of the Consultation also give effect to the Ten Tech Priorities, which were published in March 2021. See the direction of change summarised in Consultation [1]-[10].

(2) ***Liberalising the basis on which transfers can take place to foreign countries*** will be an obvious source of concern to the EU because it has the potential to reduce the minimum standards of data protection applicable to personal data (including the personal data of EU citizens and residents) which is transferred to third countries from the UK.

(3) Any ***reduction in the protections governing access to data by UK authorities*** is likely to be viewed with scepticism, given existing reservations about the indiscriminate collection of data for the purposes of preventing crime and protecting national security.

(4) ***Reducing the independence of the ICO*** is highly relevant to the EU's assessment of whether the UK provides adequate protection of data rights.

4. We consider it significant that each of these proposals raises issues which EU institutions have already identified as troubling, even on the basis of existing UK law and practice. The proposals, if adopted, will also operate cumulatively, in complex ways. The precise degree of future risk to the Adequacy Decision depends on currently unquantifiable factors, including the exact nature of decisions that are taken pursuant to the Consultation and the degree of political animosity or tension between the EU and the UK that exists at the time. In summary, however, we are of the view that if the proposals are adopted, the UK's hard-won assessment of data adequacy will be placed in jeopardy.

B. The Adequacy Decision

5. We begin by explaining in brief terms the legal relevance of adequacy, before turning to the detail of the Adequacy Decision in favour of the UK.

(i) What is an adequacy decision?

6. The UK is now a third country under the General Data Protection Regulation ("**GDPR**"),[3] which means that data transfers from the EU to the UK are permitted only under certain conditions.[4] There are broadly three options for lawfully transferring data outside the EU:

   (1) The first option is an ***adequacy decision***. This is a decision of the EU that a particular third country ensures "an adequate level of protection" for personal data.[5] The effect is that transfers of personal data can occur without the need for any specific authorisation.[6]

   (2) The second option is the use of ***appropriate safeguards***, also known as alternative transfer mechanisms. This option shifts the responsibility to the data controller or processor to protect data when it is transmitted overseas. There is a closed list of appropriate safeguards, such as binding corporate rules, standard contractual terms, a code of conduct or an approved certification mechanism.[7]

   (3) The third option consists of ***derogations*** for specific situations, such as where explicit consent has been given, or it is necessary for important reasons of public interest. These are usually understood as narrow exceptions which are "not repetitive" in their use.[8]

7. The first mechanism, an adequacy decision, is the most straightforward channel for permitting data transfers overseas because it acts as a blanket "shield" for the data transfers between the EU and the other country. The second and third mechanisms provide less certainty because they rely on the terms of particular contracts or the individual circumstances of each transfer.

---

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[4] 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 Recital 101.

[5] Article 45(1) and (3). Such a decision can also apply to territories, specific sectors of a country or an international organisation.

[6] Article 45(1) and Recital 103.

[7] Article 46. Binding corporate rules are elaborated in Article 47.

[8] Article 49(1) and Recitals 112-113.

8. An adequacy decision has to be made by the European Commission (the "**Commission**"). The test is whether the third country ensures an adequate level of protection, essentially equivalent to that guaranteed within the EU.[9] The Commission bases its decision on a wide-ranging assessment of the third country's relevant legislation (both general and sectoral), rules and international commitments, together with the powers and functioning of those independent supervisory authorities which have responsibility for enforcing the rights of data subjects.[10] Among the 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.[11]

9. In order to make an adequacy decision, the Commission will have regard to the relevant EU case law as well as the guidance of the European Data Protection Board ("**EDPB**").[12] The decision will be subject to review by the EU courts. This is why, for example, the adequacy decision concerning the US was invalidated by the CJEU in the *Schrems II* case in 2020.[13] The Commission must in addition monitor the functioning of adequacy decisions, and review them at least every four years.[14]

10. 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 and Uruguay.[15] 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. 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 in

---

[9] Recital 104; Case C-362/14 *Schrems v Data Protection Commissioner* (ECLI:EU:C:2015:650) ("***Schrems I***") [73].

[10] Article 45(2). See also the EDPB Adequacy Referential p. 3 ("the objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation").

[11] Article 45(2)(a).

[12] 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.

[13] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Schrems* (ECLI:EU:C:2020:559) ("***Schrems II***") [198]-[201]. The US is in a slightly different position to the UK because the EU's assessment of the US was based on: (i) US laws and practices, as well as (ii) commitments given by the US under an agreement known as the EU-US Privacy Shield: [163]. There is no such bilateral arrangement on data privacy between the UK and EU, so the Adequacy Decision is based on the EU's unilateral assessment of the UK's laws and practices alone.

[14] Recital 106, Article 45(3)(4).

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

2011 under the earlier Data Protection Directive, 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.[16] On the other hand, the more recent decision (2019) 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 Japanese Government in respect of law enforcement and national security.[17] Part of this may be explained by the CJEU's more stringent approach to data protection in recent years (as to which see further below).

(ii) The Adequacy Decision in favour of the UK

11. The Adequacy Decision in favour of the UK was adopted by the Commission on 28 June 2021. It consists of a brief operative section that concludes that the UK ensures an adequate level of protection for personal data,[18] preceded by numerous recitals which analyse UK legal principles and practices in detail. The recitals do not on the whole identify whether certain features were more important than others,[19] but more guidance on this can be drawn from the EDPB's Opinion which informed the Commission's approach.[20]

12. Reading the Adequacy Decision as a whole, we can identify the following as the central building blocks for the Commission's conclusion that the UK provided "essentially equivalent" protection:

    (1) It was of fundamental importance that the UK's legal framework was "very similar to the one applying in the European Union".[21] This followed from the fact that the GDPR was retained in domestic law after Brexit (as the "**UK GDPR**") and had

---

[16] 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 the Basic Laws included a right to privacy: Recitals 5-6.

[17] See the Adequacy Decision in respect of Japan as well as the associated Press Release.

[18] Adequacy Decision, Article 1(1). The decision excludes personal data transferred for the purpose of immigration control under Article 1(2).

[19] Although Adequacy Decision, Recitals 273-275, 277 and 281 are helpful summaries of the Commission's assessment "in the round".

[20] The EDPB Opinion responds to a draft version of the Adequacy Decision published in February 2021. The Commission relied on the EDPB Opinion in its final Adequacy Decision: see Adequacy Decision Recital 291 and the Commission Press Release dated 28 June 2021.

[21] Adequacy Decision, Recital 19.

also been given effect in various ways under the Data Protection Act 2018 ("**DPA**").[22] Accordingly, there was strong alignment in core concepts, such as personal data, data processing, data controllers, grounds for processing and consent.[23]

(2) The Commission observed that although the UK GDPR had been amended since Brexit, the substance of the legal protections remained sufficiently similar on many issues.[24] Where minimal or technical changes were made, they did not affect the assessment.[25] However, the Commission noted that the position would be kept under review including as to any further developments.[26]

(3) Wherever there were material differences between the EU and the UK positions, such that individual rights were affected, the Commission scrutinised the position in more detail:

(a) The restrictions on rights in the DPA, for example in relation to defence and national security, were considered to be sufficiently controlled by necessity and proportionality principles.[27] The Commission relied in particular on the decisions of UK courts, human rights legislation, and the guidance of the UK Information Commissioner's Office ("**ICO**") as safeguards against an expansion of the restrictions.[28]

(b) The exemptions for journalistic, artistic and literary purposes were also considered sufficiently limited because they required a "reasonable belief" that the publication was in the public interest, and that the GDPR would be incompatible with the journalistic, artistic or literary purpose. Again, the

---

[22] 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**").

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

[24] The UK GDPR has been amended by secondary legislation, pursuant to powers given to Ministers under the EUWA. The amendments are reflected in the consolidated UK GDPR in a "Keeling Schedule" published by the DCMS.

[25] Adequacy Decision, Recitals 14, 17.

[26] Adequacy Decision, Recitals 73, 82, 156, 272, 281-282, 288. The EDPB referred specifically to the UK's National Data Strategy as a point which would require further consideration: EDPB Opinion, [52]-[55].

[27] Adequacy Decision, Recitals 56-67.

[28] Adequacy Decision, Recitals 57, 62, 64-67.

Commission relied on the guidance of the UK Courts and the ICO as clarifying the appropriate boundaries of the exemptions.[29]

(c) The exemptions for scientific or historical research purposes, or other purposes in the public interest, would be kept under review.[30] In the UK, the exemption for research purposes allows data controllers not to inform data subjects about the safeguards applicable to international transfers of their data.[31]

(4) The Commission placed reliance on the role and powers of the ICO in ensuring that adequate protection was guaranteed in practice through monitoring and enforcement.[32] The decision emphasised the independence of the Information Commissioner,[33] and the interpretive weight of her guidance.[34]

(5) The Commission took comfort from the general protections in UK laws for privacy rights under international and domestic human rights laws.[35] It approved the protection of individual data rights, such as the right of access, both in terms of substance and procedure.[36]

13. The Commission however expressed itself with caution in relation to the following matters:

---

[29] Adequacy Decision, Recitals 68-70.

[30] Adequacy Decision, Recitals 71-73. Research exemptions are dealt with under Article 89 of the GDPR and the UK GDPR, as well as various provisions in the DPA.

[31] Compare Articles 15(2) and 89 of the 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 has been criticised by commentators, see Douwe Korff "The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK" at p. 14.

[32] Adequacy Decision, Recitals 85-98.

[33] 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 European Convention on Human Rights, see Recitals 117-118.

[34] Adequacy Decision, Recital 18.

[35] 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").

[36] 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").

(1) ***The risk of UK government access to personal data once it was transmitted to private entities in the UK***.[37] The issue has been brought into sharp focus because of *Schrems II*, in which the CJEU applied strictly the principles of lawfulness and proportionality to interferences with privacy rights, and on that basis invalidated the Commission's adequacy decision in respect of the US.[38] The Commission considered in particular:

(a) ***Access to, and use of, personal data by UK law enforcement authorities and intelligence services*** under the DPA and other legislation.[39] 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**").[40] On this point, the Commission concluded that there were sufficient safeguards in place, particularly as compared with the earlier legislation.[41] However, the Commission emphasised the critical importance of necessity and proportionality tests,[42] independent oversight mechanisms,[43] and the continued application of European human rights law.[44]

(b) ***Sharing of data between agencies, both within the UK and between agencies in the UK and third countries***.[45] The Commission looked carefully at the UK-US CLOUD Act Agreement, under which UK data controllers could be required to provide data to US agencies.[46] The

---

[37] 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].

[38] *Schrems II* [174]-[175], [180]. In that case, the CJEU was also concerned as to the lack of any individual redress mechanism in respect of the broad surveillance powers in place: [181]-[197].

[39] Adequacy Decision, Recitals 122-141, 175-243

[40] Adequacy Decision, Recitals 216-240, 250-260, 263-272.

[41] The IPA 2016 introduced transparency and new safeguards, including the requirement that warrants be approved by a Judicial Commissioner, and replaced piecemeal oversight mechanisms by a new Investigatory Powers Commissioner's Office ("**IPCO**").

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

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

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

[45] Adequacy Decision, Recitals, 142-156, 242-243.

[46] The Clarifying Lawful Overseas Use of Data Act is a US federal law. It permits the US to enter into bilateral arrangements with other countries so that communication service providers located in either country can share information with the other country's government agencies. The UK entered into such an agreement with the US in October 2019.

Commission was ultimately satisfied however that there were sufficient safeguards in place to protect EU persons' data from being transmitted overseas.[47]

(2) The Commission also acknowledged the sensitivity of ***international transfers of data from the UK more generally***.[48] This was because of the risk of data flowing out of the UK into countries that the EU has not recognised as providing adequate protection.[49] At the time of the Adequacy Decision, the UK had simply duplicated the EU approach to international transfers (i.e. requiring either adequacy regulations, appropriate safeguards or derogations as described above in [6]).[50] It had also adopted adequacy regulations in respect of transfers of data from the UK into EU countries.[51] The Commission found this to be sufficient for the time being, but noted that any further divergences would be kept under review.[52]

14. The tone of the adequacy decision is generally supportive of the UK system. This reflects 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. However, as hinted by the Commission's circumspection on certain issues, its assessment of adequacy was controversial even at the time. In particular:

(1) The ***EDPB*** Opinion of 13 April 2021 expressed reservations about aspects of the draft decision, identifying a need for further clarification, assessment and

---

[47] 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 that it was "deeply concerned that this will allow undue access to the personal data of EU citizens and residents by US authorities": [25].

[48] Adequacy Decision, Recitals 74-81.

[49] The "onward" flow of data from one third country to another has to be taken into account when assessing adequacy: GDPR Article 45(2)(a), (c) and Recital 101.

[50] UK GDPR, Articles 44-50 and DPA, s. 17A, 17B, 17C and 18. The changes to these provisions as compared with the GDPR are generally technical and limited, except that Article 48 (concerning the status of foreign judgments which require the transfer of data overseas) has been removed from the UK legislation. That point is discussed in the EDPB Opinion, [99]-[106]. The procedural details of how the UK will assess adequacy under these provisions are set out in a Memorandum of Understanding between DCMS and the ICO.

[51] Consultation, [237]. The Government has adopted regulations in respect of EU and EEA states, EU institutions, and the countries the EU had already assessed as adequate. It has also made regulations in relation to Gibraltar which the EU had not assessed as adequate.

[52] Adequacy Decision, Recital 82: "the Commission will closely monitor the situation, assess whether the different transfer mechanisms are used in a way that ensures the continuity of protection, and, if necessary, take appropriate measures to address possible adverse effects for such continuity."

reassurances in particular on the immigration exception, UK-third country transfers and bulk interception.[53] It also noted, significantly in view of the subject-matter of the Consultation, that future UK divergence from EU data protection law "might create risks for the maintenance of the level of protection provided to personal data transferred from the EU".[54]

(2) Following a critical report from its influential LIBE Committee on 11 May 2021, the ***European Parliament*** passed a resolution on 21 May expressing the view that the adequacy decision was not consistent with EU law and asking for it to be amended.[55] Among other matters, the resolution:

(a) expressed concern about "the lack and often non-existent enforcement of the GDPR by the UK when it was still a member of the EU", with particular reference to the "lack of proper enforcement" by the ICO;[56]

(b) characterised the treatment of "mass surveillance" in the draft adequacy decision as "unacceptable", alleging defects in oversight and insufficient protections for metadata and registering "deep concern" over the insufficiency of safeguards concerning the onward transfer of the data of EU citizens and residents to the US National Security Agency ("**NSA**");[57] and

(c) objected that grants of adequacy by the UK would lead to the bypassing of EU rules, with particular reference to the UK's Digital Economy Act 2017 and possible future UK trade deals, including its planned participation in the Comprehensive and Progressive Trans-Pacific Partnership ("**CPTPP**").[58]

(3) The ***CJEU*** has in recent years consistently taken a more absolute line than the Commission and most of the Member States in defence of individual data rights,

---

53 EDPB Opinion, [12]-[37].

54 EDPB Opinion, [11].

55 Resolution, [35]-[36].

56 Resolution, [6]-[8].

57 Resolution, [12]-[17]. See also "Data protection and digital competition" by Ian Brown and Douwe Korff, 17 June 2021, which commented that "the Commission failed to look seriously and critically at UK surveillance in particular".

58 Resolution, [18]-[23].

striking down previous EU-third country agreements[59] and even EU legislative measures.[60] It has indeed proved notably more activist in this area than the Council of Europe's European Court of Human Rights ("**ECtHR**").[61] It therefore remains entirely possible that the Adequacy Decision in its current form will be challenged in EU courts.[62]

15. As this context demonstrates, the Commission is significantly constrained in its ability to retain and renew the Adequacy Decision, particularly in the event of a change in the UK data protection climate. Recent history suggests that the possibility of a successful legal challenge, whether at the suit of an individual, an NGO or the European Parliament, can by no means be discounted. The Commission understands this well and whatever its inclinations towards the unimpeded flow of data, will not expose itself to what it considers to be unacceptable legal risk.

16. A further consideration is that the direction of travel, in terms of the EU's approach to data protection, is towards increasing data protection. Most recently, the EU has

---

[59] 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 and freedoms: Case C-1/15 Opinion of the Court (Grand Chamber) (ECLI:EU:C:2016:656).

[60] 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]. There is also a challenge underway in the CJEU against the PNR Directive (Case C-727/19 P). Judgment is awaited but the oral hearing took place in July 2021, see the blogpost by Christian Thönnes on EU Law Analysis (17 September 2021).

[61] 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".

[62] We are not aware of a challenge having been filed at this stage, but the prospects of one have been considered in academic commentary. See Anastasia Choromidou "EU data protection under the TCA: the UK adequacy decision and the twin GDPRs" (2021) *International Data Privacy Law*, p. 13 ("the UK Adequacy Decision may be invalidated on the basis of the possible current incompatibility between the EU and the UK on account of the 'immigration exemption' and the national security carve-outs. A challenge on either account might reach the CJEU soon"). See also Oscal Stephen Kelly, "The UK Adequacy Decision and the Looming Possibility of a Schrems III" on the King's Law School EU Law Blog.

proposed ambitious new rules under the Digital Services Act and Digital Markets Act.[63] These proposals reinforce the GDPR and reflect the EU's commitment to tightening data protection laws in coming years.[64] The Commission is likely to be guided by this regulatory and policy climate, in addition to its evaluation of the legal risks identified above.

17. In the normal course, the Adequacy Decision will expire on 27 June 2025, and could be renewed for a further period.[65] However, the Commission is required to monitor developments in the UK on an ongoing basis.[66] It is also empowered to suspend, repeal or amend the decision at any point if the UK no longer ensures an adequate level of protection.[67] This would be a unilateral move on the part of the Commission, though in most cases would require consultation with the UK to remedy the situation.[68] In addition, if there are "grounds for urgency", the Commission can act immediately.[69]

18. Given the time that will most likely be needed to decide upon, enact and implement the changes floated in the Consultation, the default stage for the Commission to revisit the issue of data adequacy would be prior to but in the context of the scheduled 2025 renewal decision. We cannot however exclude the possibility of earlier action under the powers identified above.

19. We note that (in contrast to the more forthright approach of the CJEU) the Commission has not to date revoked an earlier adequacy decision on the grounds that a third country's laws or practices have changed. It seems to us likely however that the UK's position, rightly or wrongly, will be scrutinised with particular care. The fact that the UK was previously subject to the full panoply of EU rules means that any divergences are

---

[63] These proposals are outlined in the Commission's policy page for the Digital Services Act Package. The Digital Services Act proposes reforms to improve consumer protection, transparency and accountability online, while The Digital Markets Act is directed at creating competition between the major platforms.

[64] For example, the Explanatory Memorandum to the Digital Markets Act notes that the proposal "complements the data protection laws" in particular as regards transparency and privacy. As presently drafted, the Digital Markets Act would require gatekeeper platforms to refrain from combining personal data sourced from its platforms with data sourced elsewhere: Article 5(a). It would also require gatekeepers to provide effective portability and real-time access to data: Article 6(1)(h), (i).

[65] Adequacy Decision, Recitals 289-290, Article 4.

[66] Adequacy Decision, Article 3(1), Recital 272, 281-284, 288. The general obligation of monitoring adequacy decisions derives from GDPR, Article 45(4). See also GDPR, Recital 106.

[67] Adequacy Decision, Article 3(4). These powers derive from GDPR, Articles 45(5), 93(2)-93(3).

[68] Adequacy Decision, Recitals 284-286, GDPR Article 45(6). See also GDPR Recitals 103, 107.

[69] Adequacy Decision, Recital 287, GDPR Articles 45(5), 93(3).

immediately identifiable, and so capable of minute examination to a greater extent than will be true of national laws which had a different starting point. Persistent political tensions between the EU and UK, and a sense in some quarters that the drawbacks of Brexit must be made visible to the European public,[70] are factors which, if not decisive of the adequacy issue, are nonetheless relevant background.[71]

C. Assessing the proposed changes to UK law

20. We are unable to comment on the political factors which will influence the Commission's decision, but in order to assess the legal risk of the Adequacy Decision being revoked in response to changes in UK law, we consider below the materiality and extent of the divergences proposed by the Consultation.

21. At present, the proposals in the Consultation are expressed at a high level of generality, but they can be summarised as covering the following topics:

    (1) ***Reducing burdens on business***,[72] with a consequent dilution of individual rights.[73]

    (2) ***Reducing barriers to data flows*** by taking a more lenient approach to adequacy and the other mechanisms for transfers.[74]

    (3) ***Delivering better public services*** by increasing the use and access to data by public authorities and others in the UK, in particular in relation to health and public safety.[75]

---

[70] A leaked letter of 28 October 2021 from the French Prime Minister to the Commission President exemplifies this strand of opinion. It read in the original as follows: "*Il est indispensable de montrer clairement aux opinions publiques européennes que le respect des engagements souscrits n'est pas négociable et qu'il y a davantage de dommages à quitter l'Union qu'à y demeurer.*"

[71] Hence an EU spokesperson has been quoted as saying that Brussels is monitoring the UK's consultation "very closely" and that "in [a] case of justified urgency" that threatened its citizens, it would "immediately" revoke its data-sharing arrangement with the UK. See "EU takes aim at UK plan to rewrite data laws" in the Financial Times (26 August 2021).

[72] Consultation, Chapters 1-2 [25]-[228].

[73] While the Consultation affirms a commitment to strong data protection rights, it views the strict protection of those rights under the GDPR and the DPA in their present form as impeding business outcomes. The point is discussed further below.

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

[75] Consultation, Chapter 4 [271]-[306].

(4) ***Reform of the ICO***, including by reference to strategic goals set by the Government.[76]

22. The above categories represent significant shifts in priority, and are likely to be subject to close scrutiny by the EU. Each is discussed further below.

(i) "Reducing burdens on business"

23. Primary aims of the Consultation are to reduce the perceived technicality and complexity of the law and encourage the free flow of data.[77] In our opinion, the measures proposed would have the consequence of watering down the protection of data rights in a number of ways.

Re-use of data for new purposes

24. The Consultation proposes allowing the re-use of data for a new purpose, i.e. a purpose which is different from the original purpose for which the data was collected.[78] In particular, re-use could be permitted wherever it is necessary for "safeguarding an important public interest".[79] Re-use would also be permitted by a secondary controller who is different from the original controller who collected the data.[80]

25. This is a marked change from the principles of the GDPR, pursuant to which data must be collected for "specified, explicit and legitimate purposes" (the "**purpose limitation**") and so that it is "not further processed in a manner that is incompatible with those purposes" (the "**compatibility test**").[81] These principles have a provenance going back decades in the EU Data Protection Directive 1995 and the UK Data Protection Act 1998.[82]

---

[76] Consultation, Chapter 5 [307]-[410].

[77] 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].

[78] Consultation, [45]-[54].

[79] Consultation, [54(a)].

[80] Consultation, [54(b)].

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

[82] 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].

26. The proposal significantly cuts across the protection of rights which has been sought to be achieved by the purpose limitation and the compatibility test: this is likely to be a serious cause for concern as regards the EU assessment of adequacy. As a starting point, it will be noted that the Adequacy Decision was premised on the assumption that the purpose limitation and the compatibility test would be kept in place after Brexit.[83] More specifically:

(1) Purpose limitation is a cornerstone of the GDPR principles. 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.[84] But the proposed changes, taken together, could allow data to be used in ways that a data subject can neither foresee nor control. It could also lead to data being passed to third parties and beyond for a wide range of purposes without oversight or control.[85]

(2) The only limitation on the current proposal appears to be the requirement that the secondary processing be for the purpose of "an important public interest".[86] That term is not defined in the Consultation, nor are examples given. It is also not clear how this differs from the ambit of the more tightly drafted restrictions in the GDPR which apply to "important objectives in the public interest".[87] Finally, it is not made clear whether the tests of necessity and proportionality will be included (i.e. to ensure that the secondary processing is necessary to achieve the public interest and that the interference with privacy is proportionate to achieving that purpose).

---

[83] Adequacy Decision, Recital 44.

[84] "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).

[85] The Consultation separately discusses the importance of "innovative data sharing solutions" at [126].

[86] Consultation, [54(a)]. The Keeling Schedule to the UK GDPR also shows that the Government has included national security and defence in the list of interests in Article 6(4).

[87] Article 23(1)(e) of the GDPR and the UK GDPR sets out restrictions which can limit data protection rights if they, among other things, are necessary and proportionate measures to safeguard "other important objectives of general public interest" in particular "an important economic or financial interest … including monetary, budgetary and taxation matters, public health and social security". The ICO's comment that any exceptions to the purpose limitation "should be limited to circumstances of genuine important public interest (as already permitted under the current law)" also indicates that it is unclear what additional public interests are sought to be protected here: ICO Response to Consultation, [6].

(3) The proposal has the potential to undermine the principle of transparency,[88] because consent could be given for the original purpose without knowledge of the potentially incompatible, secondary use. This does not give proper recognition to the concept of consent under the GDPR which is given "for one or more specific purposes" of data processing.[89]

Expansion of processing for legitimate interests

27. The Consultation proposes an expansion of the lawful grounds for data processing by extending the ambit of a "legitimate interest" and removing the need to balance that legitimate interest against the interests of data subjects (the "**balancing test**").[90] These proposals would work in concert with other proposals discussed further below, for example those concerning access to data by political parties and public authorities.

28. The confined ambit of legitimate interests, and the balancing test, under the GDPR and UK GDPR constitute fundamental protections of individual privacy and data rights.[91] They have also been in place for many years in the EU and the UK.[92] The continuation of these key concepts was presumed by the Commission in the Adequacy Decision.[93] It is therefore likely that this will be a cause for concern. In particular:

(1) The proposed list of legitimate interests is extremely broad. It includes, for example, internal research and development, or business innovations aimed at improving services for customers.[94] The difficulty is that one or more of these legitimate interests could, for example, permit a range of activities in the AdTech

---

88 See the ICO Response to Consultation, [6].

89 Article 6(1)(a) of the GDPR and the UK GDPR.

90 The Government proposes to "create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test in order to give them more confidence to process personal data without unnecessary recourse to consent": Consultation, [60].

91 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".

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

93 Adequacy Decision, Recital 25.

94 Consultation, [61].

industry, such as real-time bidding.[95] While the Consultation recognises that real-time bidding should be regulated, at the same time it supports the view that organisations could collect or store information from a user's device and analyse their behaviour without their consent by relying on the legitimate interest of "enhanced functionality on websites".[96]

(2) The balancing test is of central importance in protecting individual rights. It requires controllers to weigh up the legitimate interest against the rights of the individual, taking a case-by-case approach which inevitably depends on the information, the individual, and the reason the information is sought. This concept is embedded in UK case law.[97] 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.[98]

(3) Going forward, the EU's approach to these issues is going to be one of strengthening individual rights protection under the proposed Digital Markets Act and Digital Services Act, rather than broadening commercial uses which can justify the processing of data without consent.[99] This is likely to be relevant to the Commission's decision-making in the future.

---

[95] Real-time bidding is where blank advertising space on websites is auctioned to bidders for the purpose of delivering personalised advertisements. This process occurs behind the scenes from the user's perspective and involves huge numbers of commercial entities and large volumes of personal data. See the ICO's Work on Adtech.

[96] Consultation, [200] and Q 2.4.3.

[97] See for instance the recent decision in *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."

[98] 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.")

[99] The European Parliament had commented on the UK's National Digital Strategy that the view that "withholding data can negatively impact society" was not compatible with the principles of data minimisation and purpose limitation under the GDPR: Resolution, [7].

Expansion of processing for political purposes

29. The Consultation proposes to remove restrictions on direct marketing for political campaigns.[100] It also proposes to expand the lawful grounds of processing, again by relying on legitimate interests, to enable political parties to process personal data, including sensitive data such as a person's political opinion.[101] As the ICO has pointed out, these rules are already relatively permissive in the UK.[102] In particular, reductions in protections of sensitive data are unlikely to be viewed favourably by the EU, given its special status under the GDPR.[103]

Automated decision-making

30. The Consultation proposes removing or limiting rights in relation to automated decision making.[104] At present, Article 22 of the UK GDPR provides that data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, subject to certain exceptions. Again, this right was contained in the earlier legislation,[105] and the continuation of that right was taken into account by the Commission in its Adequacy Decision, including the minor amendments that had been made at the time.[106] The EU has also proposed introducing a Regulation on Artificial Intelligence which in part addresses the use of data in AI.[107]

---

[100] Consultation, [222]-[223]. As the ICO notes in its response, the details are extremely unclear at this stage: ICO Response to Consultation, [105], [107].

[101] Consultation, [226]-[227].

[102] ICO Response to Consultation, [106], [111]. Currently, para. 22 of Part 2 of Schedule 1 to the DPA 2018 already permits registered political parties to process sensitive data about political opinions without consent, subject to certain conditions. Section 8(e) of the DPA also already extends the ambit of public interests to include "democratic engagement", a point noted in the Adequacy Decision, [25].

[103] GDPR, Recital 51 and Article 9 ("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 rights and freedoms.") The EDPB has emphasised the importance of protecting such data when political parties process personal data in the course of electoral activities: EDPB Statement on the use of personal data in the course of political campaigns (13 March 2019).

[104] Consultation, [94]-[101]. The proposal to remove Article 22 altogether is at [101].

[105] Article 15 of the Data Protection Directive and s. 12 of the Data Protection Act 1998.

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

[107] Proposal for an Artificial Intelligence Act dated 21 April 2021. It includes specific rules in Chapter 2 about data and data governance for high-risk AI systems which would complement the GDPR.

Other measures

31. There are a number of other proposals which seek to reduce burdens on organisations and in doing so reduce an individual's practically enforceable rights over their data. These measures include but are not limited to:

    (1) ***Reforming accountability*** by replacing the current approach with "privacy management programmes" and removing the requirements for having a data protection officer.[108] As the ICO has said, accountability is a central element of a high standards data protection regime, both in the UK and internationally.[109] The purpose is to ensure the controller is responsible for and able to demonstrate compliance with the data protection principles.[110] That the UK had adopted the EU approach to accountability was a point taken into account by the Commission in its decision.[111] While these amendments appear technical, they will affect meaningful compliance with the rules and therefore the substantive rather than theoretical protection of individual rights.

    (2) ***Removing Data Protection Impact Assessments and the need to consult with the ICO in high risk situations***.[112] These requirements are already limited to situations which create "high risks" to rights of individuals, including where there is large scale or automated processing.[113] Again, these features were assumed by the Commission to be part of the UK framework in its assessment.[114] While the Consultation takes the view that these are unnecessary burdens, they had been introduced by the EU as reflecting a proportionate and balanced approach to protecting rights.[115]

---

[108] Consultation, [142]-[164].

[109] ICO Response to Consultation, [43].

[110] Article 5(2) of the GDPR and the UK GDPR.

[111] Adequacy Decision, Recitals 83-84.

[112] Consultation, [165]-[173].

[113] Article 35(1) of the GDPR and the UK GDPR.

[114] Adequacy Decision, Recitals 83-84.

[115] See GDPR, Recitals 75, 84, 89, 91-92. The ICO has provided guidance explaining how Data Protection Impact Assessments are part of an approach which favours "data protection by design and by default". See further the background discussed in Eleni Kosta, "Article 35. Data protection impact assessment" in Kruner et al, *The EU General Data Protection Regulation* (OUP 2020).

(3) ***Introducing fees for subject access requests and changing the threshold for a response***.[116] Subject access requests or SARs give individuals rights of access to the data that an organisation holds about them.[117] The Commission noted that these rights were included in the UK GDPR and were practically enforceable.[118] The new proposals impede this access to data. They also give greater discretion to organisations to refuse requests. The current proposal is that an organisation could refuse a SAR if it is likely to cause a disproportionate or unjustifiable level of "distress, disruption or irritation".[119] This opens the door to data controllers asking subjects about why they are seeking the information, contrary to the Court of Appeal's guidance that a request has to be answered even if the subject has a collateral purpose in making that request.[120] The amendment is also excessively protective of controllers in circumstances where there is a nuanced set of principles about refusing SARs if they are abusive.[121]

32. Proposals such as these operate cumulatively to dilute the protection of individual data rights vis-à-vis controllers. Given the importance in the Adequacy Decision of practical enforcement, these amendments could help tip the balance against a conclusion that the UK provides essentially equivalent protection.

(ii) Reducing barriers to data flows

33. The Consultation proposes an overhaul of the mechanisms for international transfers of data from the UK to other countries. The changes include:

---

[116] Consultation, [185]-[189].

[117] Article 15 of the GDPR and the EU GDPR.

[118] Adequacy Decision, Recitals 51, 53, 104, 124-125, 170 fn 251.

[119] Consultation, [189(b)]. This adopts non-binding guidance which applies to "vexatious" requests under Freedom of Information legislation. But that is a situation where public bodies are asked for information, a rather different situation as compared with individuals seeking access to their own data.

[120] *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").

[121] *Lees v Lloyds Bank plc* [2020] EWHC 2249 (Ch) [48]. In this case, Chief Master Marsh took into account a number of cumulative factors in order to refuse the disclosure, including that there had been numerous and repetitive SARs, which was abusive.

(1) ***A flexible approach to assessing the adequacy of other countries' data protection regimes***, by focusing on "actual risks" to data protection rights.[122] The Government has indicated its intention to publish adequacy decisions in respect of the USA, Australia, South Korea, Singapore, the Dubai International Finance Centre and Colombia.[123] In addition, the Consultation intends to relax the requirement for reviews every four years.[124]

(2) ***Increased reliance on existing and new alternative transfer mechanisms***.[125] It will be recalled that 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. The Government proposes to reduce the burden on organisations by only requiring proportionate safeguards,[126] and allowing them to develop their own alternative transfer mechanisms such as a bespoke contract.[127]

(3) ***Increased reliance on derogations*** so that they can be used repetitively rather than on an infrequent basis.[128] This would be a shift from the EU approach which treats derogations as rather exceptional.[129]

34. These changes would seriously risk jeopardising the Adequacy Decision, because the Adequacy Decision would enable the UK to become a conduit for data transfers from the EU to third countries with lesser protections, including the US as well as other countries for which the EU has not yet undertaken any adequacy analysis. While this is ameliorated by the fact that the UK intends to review other legal systems in a robust way and by reference to human rights,[130] this does not resolve the difficulty that individual

---

[122] Consultation, [242]-[243]. As the ICO has pointed out, while the Consultation refers to the relevance of "different cultural, legal and linguistic factors" in different countries it is unclear how this will be taken into account when assessing whether adequate protection is achieved: ICO Response to Consultation, [121].

[123] Press Release titled "UK unveils post-Brexit global data plans to boost growth, increase trade and improve healthcare" dated 26 August 2021.

[124] Consultation, [250].

[125] Consultation, [257], [266].

[126] Consultation, [259].

[127] Consultation, [261]-[262], [265]. This draws from an approach taken in New Zealand, though it should be noted that even there the regulator has published detailed model contract clauses and guidance.

[128] Consultation, [270].

[129] GDPR, Recitals 112-113, EDPB Opinion, [97]-[98], Resolution, [39].

[130] Consultation, [244], [246].

countries such as the US are the subject of specific findings by the CJEU as not providing adequate protection. As noted above, the legal risks associated with the CJEU's stringent approach to the US is an important factor in the Commission's ability to retain the current Adequacy Decision.

35. In many ways, this proposal is the most obvious roadblock for the continuation of the Adequacy Decision. Under the GDPR, any adequacy decision has to take into account "onward transfers". Article 44 and Article 45(2)(a) require the Commission to consider "rules for the onward transfer of personal data to another country" as part of its assessment of a particular third country. The logic is that the level of protection should not be reduced despite the transfers across borders.[131] If transfers are allowed *via* the UK on lower conditions than the EU would require, there is likely to be difficulty in concluding that adequate protection is provided by the UK.

36. The alternative proposals in the Consultation, for example relying on standard contractual clauses, are unlikely to resolve this difficulty. As the CJEU found in *Schrems II*, these alternative transfer mechanisms still have to be considered against the background of the foreign laws and have to ensure essentially equivalent protection as the EU.[132]

(iii) Delivering better public services

37. The Consultation proposes to expand the situations where public authorities use personal data. This includes extending the protection to private entities acting on behalf of public authorities,[133] permitting the use and retention of biometric data by the police,[134] and streamlining provisions which deal separately with law enforcement and intelligence services under the DPA.[135]

38. The precise nature of these amendments remains to be seen, but as explained above the Commission reviewed the UK's rules as to law enforcement and intelligent services carefully in light of *Schrems II*. It formed the view that the current arrangements were adequate, despite criticisms from the European Parliament and the EDPB that too low

---

[131] GDPR, Recital 101.

[132] *Schrems II* [92]-[96], [104]-[105].

[133] Consultation, [282].

[134] Consultation, [301].

[135] Consultation, [304]-[306].

a standard was being applied. Ultimately, it was reassured by the existence of safeguards, for example in the form of independent supervision. But the new proposals are directed to "encourage and facilitate the effective sharing of data for law enforcement and national security purposes" and to support "private and public sector collaboration".[136] Accordingly, even minor changes to this aspect of the regime are likely to be subject to anxious scrutiny by the EU going forward.

(iv) Reform of the ICO

39. The Consultation proposes a number of changes to the ambit and operation of the ICO including:

    (1) The imposition of the Government's strategic objectives on the ICO to advance economic growth and innovation, and to encourage the responsible use of data.[137]

    (2) The requirement to take into account public safety, which is a reference to the activities of UK intelligence services and law enforcement bodies.[138]

    (3) The discretion not to investigate complaints unless a minimum threshold is met, for example by reference to individual harm.[139]

40. These proposals are in very general terms at present, but they are likely to be significant from the EU's perspective because the independence of the ICO was a critical safeguard that was taken into account in the Adequacy Decision.[140] Independent supervision was also noted to be of importance because it ensured that any interference with privacy rights under human rights legislation had the necessary quality of law.[141] Indeed, the

---

[136] Consultation, [304], [306].

[137] Consultation, [320]-[331], [344]-[346].

[138] Consultation, [340]-[341].

[139] Consultation, [387].

[140] Adequacy Decision, Recital 85, 87 ("The authority should act with complete independence and impartiality in performing its duties and exercising its powers"). See also 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. The significance of independence to the Commission is evidenced by its recent actions against the Belgian data protection authority for violating the requirement of independence under Article 52, see the infringement decisions for October 2021 available online.

[141] Adequacy Decision, Recital 117.

European Parliament had gone further and recommended that the ICO should be made entirely independent from the Department for Culture Media and Sport.[142]

41. In addition to independence, the proposals indicate a curtailing of ICO powers by reference to the goals of intelligence services and law enforcement. These are areas over which the EU institutions have already expressed reservations in terms of the proper protection of individual rights.

42. The proposals as to complaints also impede the ability to enforce data rights in practice. The ability of individuals to complain was taken into account in the EU's assessment in the Adequacy Decision.[143] 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".[144] In addition, the ICO considers that an "outcome" does not need to be a substantive outcome.[145]

43. These proposals further impact on the practical enforcement of data rights, jeopardising the prospect of establishing essentially equivalent protection given that adequacy requires infringements to be "identified and punished in practice".[146] The risk is increased in circumstances where 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.[147]

D. Conclusion

44. The scope of the proposed changes is not in all respects clear at this stage, and much will depend on the precise outcome of the Consultation and on the surrounding political circumstances. The express purpose of the Consultation is however to take data

---

[142] Resolution, [8].

[143] 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.

[144] Section 165(5)(a) of the DPA.

[145] Section 165(4)-(5). The right to apply to the First Tier Tribunal under s. 166 of the DPA is currently seen as 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]. That position is being considered by the Upper-Tribunal in the case of *Killock & Veale v the Information Commissioner* (judgment is awaited).

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

[147] 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").

protection in a “new direction”. Whatever the merits of that path may be, it is clear that it leads the UK away from the standards applied by the EU to protect the rights of data subjects: standards to which the EU institutions, led by the CJEU, have shown a strong and continuing commitment. The divergence is most obvious in respect of the rules governing transfer of data to other countries ([33] to [36] above); but the other proposals we have considered will also require EU institutions to re-assess the key question of whether the UK ensures an adequate level of protection for personal data, essentially equivalent to that guaranteed within the EU.

45. To proceed decisively in the direction mapped out in the Consultation would undoubtedly increase the risk (which to some extent already exists) of the Adequacy Decision being struck down by the CJEU. We further conclude that the adoption of these proposals will reduce the chances of obtaining a renewed Adequacy Decision from the Commission in 2025, and could even jeopardise its continuation in advance of that date.

LORD ANDERSON OF IPSWICH KBE QC

AARUSHI SAHORE

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

12 November 2021