2

Post-Brexit UK Data Protection: Staying the Course or Charting a New Direction?

Karen Mc Cullagh

in Celeste et al, Data Protection and Digital Sovereignty Post-Brexit (Bloomsbury/Hart, 2023)

I. Introduction

When the UK was preparing to leave the EU and become a third country for EU data protection purposes, it opted to maintain alignment with EU data protection laws, including the General Data Protection Regulation (GDPR), and considered a variety of mechanisms to effectuate seamless EU–UK personal data transfers before applying for a GDPR adequacy assessment by the European Commission (the Commission).[1] Then, after the adoption of the adequacy decision by the Commission on 28 June 2021, the UK government announced an intention to consult on proposed changes to UK data protection law with a view to modernising the law to foster and encourage innovation removing barriers and reducing burdens on organisations, to allow the UK to 'operate as the world's data hub' while maintaining high data protection standards so as not to jeopardise the EU–UK adequacy decision.[2] Mindful of these developments, this chapter has two goals, the first of which is to explain why the UK was initially reluctant to apply for an adequacy decision, before outlining how the Commission assesses adequacy. The second is to outline proposed changes to UK data protection law and consider whether the UK is seeking merely to make appropriate use of the white space in the GDPR and the degree of divergence permitted from the EU standard with assessing adequacy or to substantially diverge from the GDPR.

---

[1] European Commission, Implementing Decision of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021) 4800 final, https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

[2] DCMS, 'Data: A New Direction' (10 September 2021) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf.

The chapter demonstrates that the UK government has, over time, resiled from many of the more radical reform proposals it initially consulted on. It concludes that if implemented in their current form, many of the proposed changes are minor and only a few of the proposed changes would result in significant divergence from the GDPR and would cause the EU to question whether to attach conditions to the renewal of the adequacy decision or refuse to renew it in due course.

II. Rationale for Seeking to Obtain and Retain an Adequacy Decision

During post-Brexit referendum negotiations, the UK government acknowledged that personal data transfers between the EU and the UK were vital to the UK economy: EU personal data-enabled services exports to the UK were worth approximately £42bn (€47bn) in 2018 and exports from the UK to the EU were worth £85bn (€96bn), and this motivated the UK to ensure the continued free flow of personal data between the two.[3] It also acknowledged that the GDPR would continue to have extraterritorial application to data controllers offering goods or services to individuals or monitoring the behaviour of individuals in EEA countries, thereby necessitating ongoing compliance with the GDPR,[4] but that as a third country for data protection purposes it would not benefit from de jure recognition of its data protection laws as providing an adequate standard of protection to facilitate EEA–UK personal data transfers, and it therefore reviewed the appropriateness of a variety of mechanisms for effectuating such transfers for meeting the UK's needs. In this regard, it considered whether data flows would be best facilitated by requiring data controllers and processors to rely on model clauses or other legal mechanisms to effectuate transfers such as consent or seeking either a sectoral or whole-country adequacy decision from the Commission.[5]

Although it concluded that an adequacy decision would be the 'least burdensome' option and would offer 'stability and certainty for businesses', particularly small and medium-sized businesses that could not easily absorb the legal costs associated with drafting and obtaining

[3] DCMS, 'Explanatory Framework for Adequacy Discussions, Section A: Cover Note' 1, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872228/A_-_Cover_Note.pdf.

[4] GDPR, Art 3, 679.

[5] House of Lords, European Union Committee, 'Brexit: The EU Data Protection Package' (18 July 2017) HL Paper 7, ch 3, paras 112–15.

approval for model clauses or other legal mechanisms to effectuate transfers,[6] it was reluctant to apply for one because that would require the UK to accept the jurisdictional element of an adequacy assessment. That is, the UK would have to submit to an evaluation of its laws and practices by the Commission; to accept that whilst there would be dialogue between the EU and the UK regarding its legal framework and practices pertaining to data protection, the decision whether to make a finding (or not) of adequacy would be made by the Commission on a unilateral basis; to accept that EU law would continue to have extraterritorial impact in the UK in respect of personal data transferred to it from EEA countries; and further, to accept that if an adequacy decision were adopted, it could, as a 'living document', be revoked or not renewed by the Commission on a unilateral basis if it formed the view that the UK no longer provides an adequate level of protection. It was anathema to some government ministers who had promoted Brexit as an opportunity for the UK to 'free' itself from the EU law and EU institutions, which they viewed as imposing burdensome and unnecessary red tape that hindered business competitiveness.[7]

Accordingly, the UK government initially pursued a strategy of exceptionalism, calling for the EU and UK to agree to 'mutually recognise' each other's data protection frameworks, with UK data protection law 'deemed' adequate, that is, without the Commission conducting a GDPR adequacy assessment.[8] The UK further proposed to deal with disputes through the inclusion of horizontal data protection clauses in any bilateral agreement concluded between the EU and the UK; the underlying motivation was to prevent a *Schrems* scenario, that is, the EU having the power to unilaterally revoke an adequacy decision, thereby immediately

[6] ibid.

[7] For further discussion of the UK's pre- and post-Brexit data protection laws and rationale for continued compliance with the GDPR, see K Mc Cullagh, 'Post-Brexit Data Protection in the UK – Leaving the EU but not EU Data Protection Law Behind' in G González Fuster, R Van Brakel and P de Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar Publishing, 2022) 35–58.

[8] HM Government, **'**The Exchange and Protection of Personal Data – a Future Partnership Paper' (24 August 2017) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf.

halting EU–UK data transfers should the UK be found to be substantially in breach of the GDPR.[9]

The UK was likely emboldened to pursue this course of action because the Commission has drafted horizontal clauses on cross-border data flows and personal data protection for inclusion in trade agreements with the aim of reducing barriers to trade, such as forced data localisation in a state's territory.[10] However, the UK only partially succeeded in realising this goal because the Commission currently envisages using horizontal clauses in situations only when an adequacy decision cannot be realistically adopted; instead, it advocates that trade negotiations and applications for an adequacy assessment follow separate but parallel tracks[11] 'to keep trade deals uncontroversial'.[12] Therefore, whilst the EU–UK Trade and Cooperation Agreement (TCA) does contain data protection clauses and does not, at the UK's insistence, refer to data protection as a fundamental right, it is important to note that the insertion of data protection provisions and the wording thereof was agreed upon only after the UK had conceded that it would need to apply for an adequacy assessment such that the horizontal data protection provisions would have limited transitional effect, that is, pending the conclusion of

[9] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (*Schrems I*) ECLI:EU:C:2015:650. For case commentary, see L Azoulai and M Van Der Sluis, 'Institutionalizing Personal Data Protection in Times of Global Institutional Distrust: *Schrems*' (2016) 53 *CML Rev* 1343.

[10] TFEU, Art 216(1) allows authority for the conclusion of an international agreement to be 'provided for in a legally binding Union act', which would allow EU legislation to set out criteria for data protection agreements with third countries. In 2018, the European Commission endorsed horizontal provisions for inclusion in trade agreements that allow the EU to tackle protectionist practices in third countries in relation to digital trade while ensuring that trade agreements cannot be used to challenge the high level of protection guaranteed by the EU Charter of Fundamental Rights and the EU legislation on the protection of personal data. See European Commission, 'EU Horizontal Provisions on Cross-Border Data Flows and Protection of Personal Data and Privacy in the Digital Trade Title of EU Trade Agreements' https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf. For further discussion on the inclusion of horizontal clauses in EU trade agreements, see S Yakovleva and K Irion, 'Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade' (2020) 10 *International Data Privacy Law* 201.

[11] Commission, 'European Commission Letter on Cross-Border Data Flows and EU Trade Agreements' (1 March 2018) https://data.consilium.europa.eu/doc/document/ST-6687-2018-INIT/en/.

[12] JH Vela, J Plucinska and H von der Burchard, 'EU Trade, the Martin Selmayr Way' *Politico* (21 February 2018).

the adequacy assessment.[13] Moreover, whilst the EU did agree to 'mutual adequacy recognition', it was in conjunction with the UK's acceptance that this did not eliminate the need for the Commission to assess the adequacy of the UK's data protection framework.[14]

The Commission insisted on conducting an adequacy assessment because, as Lynskey has observed, whilst mutual respect for fundamental rights and data protection standards is assumed within EU Member States, such trust does not automatically exist in relation to third countries; rather, it must be built through formal legal relationships, and an adequacy assessment provides that mechanism.[15] The UK's change in status from trusted Member State to third country explains why the UK was de facto 'adequate' on the eve of the end of the transition period, whereas the following day it was not. The UK applying for and obtaining an adequacy decision would reinstate that trust, because rather than negotiating the standard of protection that the UK would agree to provide, the Commission was instead empowered to unilaterally determine whether the UK provided an adequate level of protection. Relatedly, to ensure that the UK would address any deficiencies in its law and practices, and not immediately seek to diverge from the GDPR after adoption of an adequacy decision, the Commission inserted both monitoring provisions and a sunset clause in the adequacy decision. To this end, the EU–UK adequacy decision adopted on 28 June 2021 is subject to continuous monitoring (the Commission may suspend, repeal or amend the decision at any time if it forms the view that developments render the UK's legal framework inadequate)[16] and includes a sunset clause which stipulates that it will expire on 27 June 2025 if the Commission has not made a renewed finding of adequacy by then.[17]

III. A post-Brexit opportunity for GDPR divergence?

[13] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the UK of Great Britain and Northern Ireland, of the other part [2020] OJ L444/14, Art FINPROV.10A.

[14] For further information on mutual adequacy recognition, see Mc Cullagh (n 7).

[15] O Lynskey 'Extraterritorial Impact in Data Protection Law through an EU Law Lens' in F Fabbrini, E Celeste and J Quinn (eds), *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart Publishing, 2021) 191–210.

[16] GDPR Art 45(4); European Commission, Implementing Decision (n 1) recital 281.

[17] GDPR, Art 45(3); European Commission, Implementing Decision (n 1) Art 4, recitals 289–90.

Soon after the adoption of the adequacy decision, the UK government published its National Data Strategy, in which it announced an intention to reform its data protection laws by identifying post-Brexit opportunities for 'unlocking the value of data' and securing 'a pro-growth and trusted data regime', while preserving strong data subject rights and seeking to retain its adequacy status under the GDPR.[18]

To this end, the Data Protection and Digital Information Bill (DPDI Bill) was laid before Parliament on 18 July 2022,[19] after the government had published its response[20] to the 'Data: A New Direction' (DaND) consultation.[21] The DPDI Bill was positioned as part of a series of legislative proposals intended to seize the benefits of Brexit by creating an 'ambitious, pro-growth and innovation-friendly data protection regime'. A central theme in the consultation and the DPDI Bill was reducing perceived burdens on organisations by updating and simplifying the UK's data protection framework and removing the red tape and administrative burden on businesses.

The DPDI Bill's passage through the UK's legislative process was unexpectedly paused in September 2022 to 'allow ministers to consider the legislation further' following changes to the UK's governmental leadership (Liz Truss replaced Boris Johnson as Prime Minister and leader of the Conservative Party). That same month, the government announced the Retained EU Law (Reform and Revocation) Bill (Reform and Revocation Bill). This Bill proposes to amend the European Union (Withdrawal) Act 2018, which was the basis for the retention of the GDPR (as the UK GDPR), in UK law post-Brexit. It proposes to revoke any EU-derived subordinate legislation and any retained direct EU legislation unless specifically listed under retained law. It was unclear whether this would include revocation of the UK GDPR as part of a 'bonfire of regulations'.

Thereafter, in October 2022, the Secretary of State for Culture, Media and Sport (DCMS), Michelle Donelan, gave a speech in which she announced that 'We inherited GDPR from the

---

[18] DCMS policy paper, 'National Data Strategy' (9 September 2020).

[19] Data Protection and Digital Information Bill (DPDI Bill) 143, 2022–23, 18 July 2022, https://publications.parliament.uk/pa/bills/cbill/58-03/0143/220143.pdf.

[20] DCMS, Data: A New Direction – Government Response to Consultation' (23 June 2022) www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#:~:text=The%20government%20launched%20its%20consultation,the%20UK's%20National%20Data%20Strategy.

[21] DCMS, 'Data: A New Direction' (n 2).

EU, and its bureaucratic nature is still limiting the potential of our businesses … We will be replacing GDPR with our own business-and consumer-friendly British data protection system'.[22] Her speech initially caused a stir in the business, legal and technology communities, not least because no warning had been given and it created uncertainty and confusion regarding the status of the DPDI Bill. It left unanswered the question whether the DPDI Bill would be abandoned or would be revised to change some provisions in the UK GDPR, and relatedly whether this would be the endpoint of reforms or merely a stopgap measure whilst a new bespoke data protection regime is created.

The Secretary of State's citation of findings of a survey of businesses conducted by her department in which half of the respondents reported 'excessive caution' amongst staff when handling people's data[23] and of a working paper by researchers at Oxford University suggesting they found the GDPR 'caps businesses profits by 8%' in support of her claim that a reduction in red tape could unlock economic gains[24] gave some credence to reports that the UK GDPR could be repealed.

If the UK GDPR were repealed and UK data protection laws completely rewritten, a nuanced approach to its redrafting would be needed, for if the protections currently found in the UK GDPR were watered down, the EU–UK adequacy decision would be jeopardised. It could also bring about a two-tier data rights system – with the UK being on the lower tier, falling behind the EU level of protection. It could also increase the compliance burden and associated costs of businesses operating in both the EEA and the UK as they would be required to comply with the GDPR for EEA–UK personal data transfers and any new law introduced by the UK.

Unsurprisingly, concern was expressed that there was a lack of evidence of the need for radical reform. For example, one commentator observed that the Secretary of State may have selectively reported the Oxford University research in support of political goals, since the researchers had caveated their research as a 'work in progress' and urged caution when interpreting findings – noting, for example, that negative effects on business performance which the paper links to the GDPR 'may partly reflect temporary adjustment costs, meaning

[22] M Donelan, '2022 Speech to Conservative Party Conference', www.ukpol.co.uk/michelle-donelan-2022-speech-to-conservative-party-conference/.

[23] ibid.

[24] ibid.

that its effects might taper-off in the future'.[25] A data protection solicitor similarly commented that:

> It would seem to me that the premise that the GDPR limits the potential of businesses is unfounded. The GDPR provides a moral and ethical approach to data protection to standardise the responsibilities of those who process personal data. The UK GDPR and Data Protection Act 2018 build on these standards.[26]

And another law firm reported that 'the general consensus from many of our clients with [p]an-European operations is that any substantial divergence from the EU could potentially increase the costs of compliance'.[27]

On a positive note, the deputy director for domestic data protection policy at DCMS, subsequently confirmed that 'The adequacy agreement with the EU, which allows seamless EEA–UK personal data flows, will be "at the heart" of the finalised bill'.[28] However, he also advised that the return of the DPDI Bill to Parliament would be further delayed to facilitate additional consultation, stating that ministers

> need space to work with all groups to check we go as far as we can to enable growth and innovation while protecting high standards and maintaining our parallel policy objective of looking after EU adequacy and doing so as quickly as possible.[29]

This announcement allayed fears that the government was planning to diverge to a significant degree from the GDPR or use powers in the Reform and Revocation Bill to repeal the UK GDPR in due course.

Thereafter, on 8th March 2023 the Secretary of State for Science, Innovation and Technology (DSIT, formerly DCMS), introduced the Data Protection and Digital Information (No. 2)

---

[25] N Lomas, 'UK Pauses Data Reform Bill to Rethink How to Replace GDPR' (Tech Crunch, 4 October 2022) https://techcrunch.com/2022/10/03/uk-data-reform-bill-replace-gdpr/; C Chen, CB Frey and G Presidente, 'Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally', The Oxford Martin Working Paper Series on Technological and Economic Change, Working Paper No 2022-1, 25.

[26] Bindmans, 'The Future of UK Tech Law – Data Privacy Laws in the UK' (*Bindmans Blog*, 4 October 2022) www.bindmans.com/knowledge-hub/blogs/the-future-of-uk-tech-law/.

[27] Ashurst, 'Is This Goodbye to the UK GDPR?' (*Ashurst Blog*, 7 October 2022) www.ashurst.com/en/news-and-insights/legal-updates/is-this-goodbye-to-the-uk-gdpr/; Ashurst, 'Themes and Discussions from Ashurst Data Protection Roundtable' (*Ashurst Blog*, 7 October 2022) www.ashurst.com/en/news-and-insights/legal-updates/themes-and-discussions-from-ashurst-data-protection-roundtable/.

[28] O Rowland, 'Update on Data Policy' Westminster eForum Policy Conference (31 October 2022).

[29] ibid.

Bill (DPDI Bill No2) to Parliament,[30] taking the place of the DPDI Bill which will now not proceed further in Parliament. The accompanying press release states that it will "introduce a simple, clear and business-friendly framework that will not be difficult or costly to implement – taking the best elements of GDPR and providing businesses with more flexibility about how they comply with the new data laws".[31] It further notes that the Bill will "ensure…[the] new regime maintains data adequacy with the EU", a point which has been questioned since it was originally announced that the UK would reform its data protection laws.[32]

While the DPDI Bill (No2) proposes to amend both the UK GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003, the analysis in this chapter focuses solely on a selection of proposals relating to the UK GDPR. It explores whether the proposals would, if implemented, lead to significant divergence from the GDPR or would merely clarify definitions, reduce administrative burdens, and make appropriate use of white space in the GDPR to facilitate innovation.

It is imperative that the proposals in the DPDI Bill (No2) strike the correct balance between improving on the UK GDPR yet not diverging too far from the GDPR to satisfy the 'essentially equivalent' standard. If the latter occurs, then the EU may revoke the existing EU–UK adequacy agreement or refuse to renew it in due course with serious financial and legal consequences for the UK economy. Indeed, if the adequacy decision were to be revoked or not renewed, UK businesses could lose more than £1bn in reduced trading revenue and £420m in compliance costs over five years,[33] something the government is keen to avoid. Accordingly, at this juncture, it is appropriate to explain how UK adequacy was and will be assessed.

---

[30] Data Protection and Digital Information (No2) Bill (DPDI Bill No 2) 265, 2022-23, 8 March 2023, https://publications.parliament.uk/pa/bills/cbill/58-03/0265/220265v2.pdf

[31] DSIT, Press Release: British Businesses to Save Billions Under New UK Version of GDPR, (8 March 2023), https://www.gov.uk/government/news/british-businesses-to-save-billions-under-new-uk-version-of-gdpr

[32] Ibid.

[33] DCMS, 'Data: A New Direction: Analysis of Expected Impact' para 71, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016471/Data_Reform_Impact_Analysis_Paper.pdf.

IV. Assessing Adequacy: 'Essential Equivalence'

When assessing adequacy, the Commission was and will be (when the UK seeks renewal of the existing adequacy decision) tasked with determining whether the UK provides an 'essentially equivalent' level of protection to that guaranteed in the EU. As confirmed in *Schrems,* UK law does not need to mirror the GDPR point by point[34] so long as it contains the core requirements set out in Article 45 GDPR and further elaborated on in Court of Justice of the EU (CJEU) case law and the European Data Protection Board (EDPB)'s Recommendations on Essential Guarantees for Surveillance Measures[35] and its 'adequacy referential'.[36] In effect, the Commission conducts an in-depth assessment of (i) de jure substantive protection of personal data in UK data protection law, (ii) de facto procedural protection and remedies and (iii) access to EU personal data by a third country's law enforcement authorities, each of which are discussed below.

A. De Jure Substantive Protection of Personal Data in UK Data Protection Law

The de jure substantive protection of personal data in UK law is assessed by reference to the criteria set out in Article 45(2) of the GDPR. This involves reviewing the UK's legislative framework and making a normative judgement about the UK's political structures and values, including respect for the rule of law, human rights and fundamental freedoms. It also necessitates an assessment of UK data protection law and derogations therein, and the UK's international commitments in respect of the European Convention on Human Rights (ECHR) and the Council of Europe.

When the UK applied for an adequacy assessment, the Commission reviewed several aspects of the UK's legislative framework to make a normative judgement about its political structures and values, including respect for the rule of law, human rights and fundamental

---

[34] *Schrems I* (n 9) para 81.

[35] EDPB Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures, adopted on 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

[36] Article 29 Working Party, 'Adequacy Referential' adopted on 28 November 2017, as last revised and adopted on 6 February 2018, WP254 rev.01 (endorsed by the EDPB, the Article 29WP successor body) https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines.

freedoms, by reference to the fundamental right to a private and family life (Article 7) and to protection of personal data (Article 8) enshrined in the Charter of Fundamental Rights of the European Union 2000 (the Charter). ~~Although~~ The UK government had refused to retain the Charter in UK law on the basis that it 'only applies to Member States when acting within the scope of EU law, so its relevance is removed by our withdrawal from the EU.'. It had similarly refused, in the name of restoring legislative sovereignty, to accept a proposed amendment that would have retained wording from Article 8 of the Charter in the Data Protection Bill (now the Data Protection Act 2018 (DPA)) during the legislative enactment process.[37] The Commission was nevertheless satisfied that, by virtue of a combination of common law, Article 8 of the ECHR (as incorporated into UK law by the Human Rights Act 1998 (HRA)) and the data protection rights in both the UK GDPR[38] and the DPA, the UK provides an essentially equivalent level of protection to the EU.[39] However, both the EDPB and the European Parliament (EP) emphasised the importance of UK adherence to the ECHR, implying that if the UK were to withdraw from the ECHR in the future it would trigger a review of the decision.[40] Significantly, in response to a petition asking the UK Government to withdraw the UK from the ECHR and the jurisdiction of the European Court of Human

---

[37] HM Government, *Legislating for the United Kingdom's Withdrawal from the European Union* (Cm 9446, 16 May 2017) [2.23]; HM Government, *Charter of Fundamental Rights of the EU Right by Right Analysis* (5 December 2017) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664891/05122017_Charter_Analysis_FINAL_VERSION.pdf; European Union (Withdrawal) Bill, HC Deb 21 November 2017, vol 631 col 902; Joint Committee on Human Rights, *Legislative Scrutiny: The EU (Withdrawal) Bill: A Right by Right Analysis, Appendix: Commentary on the Right by Right Analysis* (2017–19, HL 70, HC 774).

[38] The Data Protection, Privacy and Electronic Communications (EU Exit) (Amendments etc) (EU Exit) Regulations 2019, SI 491/2019 came into effect at the end of the transition period on 31 December 2020. It retained the GDPR in UK law. All references to EU institutions were removed and replaced with appropriate UK bodies, and it was renamed as the UK GDPR

[39] DCMS, 'Explanatory Framework for Adequacy Discussions, Section B: Wider Context'; DCMS, 'Explanatory Framework for Adequacy Discussions, Section C: The UK's Legislative Framework'.

[40] EDPB Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom, para 49; see also the European Parliament's concern over the UK's recognition of Gibraltar as adequate without conducting an assessment equivalent to the EU GDPR adequacy assessment; European Parliament Resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom (2021/2594(RSP)) General Observation 2; European Commission, Implementing Decision (n 1) recital 277.

Rights, the UK government confirmed that 'It is not currently government policy to seek withdrawal from ECHR,'[41] so this aspect of the EU-UK adequacy decision should not prove problematic when it is reviewed in due course.

The Commission also considered the UK's international commitments in the form of 'legally binding conventions or instruments', as well as its 'participation in multilateral or regional systems'. In this regard, the UK's accession to both Convention 108 (the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) and the additional (modernising) protocol[42] was looked upon favourably, particularly as the intelligence services data protection obligations in the DPA are based on Convention 108. Likewise, the membership of the Information Commissioner's Office (ICO) to a number of international initiatives, including the Global Privacy Assembly[43] and the Global Privacy Enforcement Network,[44] through which it and other supervisory authorities from member countries share best practices for addressing cross-border challenges and the practical aspects of privacy law enforcement cooperation, develop shared enforcement priorities and support joint enforcement initiatives and awareness campaigns, was accepted as evidence of the UK's strong and continuing commitment to data protection.[45]

---

[41] UK Government and Parliament, Response to Petition to Withdraw the UK from the European Convention on Human Rights, 28 February 2023, https://petition.parliament.uk/petitions/618456

[42] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, CM/Inf (2018)15-fina; Convention for the protection of individuals with regard to automatic processing of personal data: ETS No108, 28 January 1981 (entered into force 1 October 1985).

[43] Formerly known as the International Conference of Data Protection and Privacy Commissioners. It is a global forum for more than 130 data protection and privacy authorities from across the globe which seeks to connect and support efforts at domestic and regional level, and in other international forums, to enable authorities better to protect and promote privacy and data protection.

[44] Global Privacy Enforcement Network, www.privacyenforcement.net. In June 2007, the Organisation for Economic Cooperation and Development (OECD) governments adopted a Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy and established an informal network of Privacy Enforcement Authorities Discuss to develop and share best practices regarding the practical aspects of privacy law enforcement cooperation; cross-border challenges; enforcement and awareness campaigns.

[45] DCMS, 'Explanatory Framework for Adequacy Discussions, Section A: Cover Note' (n 3) 3.

UK data protection laws and derogations therein were also examined because Article 45(2)(a) provides that the third country shall have 'relevant legislation'. As the GDPR was implemented during the pre-withdrawal period and was retained in UK law upon exit (albeit renamed as the UK GDPR), the Commission was for the most part easily satisfied that UK law contained essentially equivalent concepts and definitions regarding, for example, personal data, processing principles, rights and safeguards, and material and geographic scope, with only a few immaterial differences in the UK law.

Yet it was not all plain sailing. A provision in the DPA exempted public bodies from certain aspects of the fundamental data protection rights and principles, such as the right of access and the right of a data subject to know with whom their data has been shared when processing personal data for purposes related to immigration control, was closely scrutinised.[46]

Whilst the Commission noted in its draft adequacy decision that the immigration exemption was broadly formulated, it was nonetheless satisfied that an adequate level of protection was provided in UK law because the exemption would 'be applied on a case-by-case basis, only to the extent necessary to achieve a legitimate aim and in a proportionate manner'.[47] However, both the EDPB and the EP voiced concerns, with the EDPB calling on the Commission 'to provide further information on the necessity and proportionality of the immigration exemption, in particular having regard to the broad scope of application *ratione personae*',[48] and to further explore whether additional safeguards exist in the UK legal framework or could be envisaged, for example 'through legally binding instruments that would complement the immigration exemption enhancing its foreseeability by and the safeguards for data subjects, also allowing for a better and prompt assessment and monitoring of the necessity and proportionality requirements'.[49] The EP similarly called upon the Commission to either seek the removal of the immigration exemption from the DPA or for it to reformed to 'provide sufficient safeguards for data subjects'.[50] The Commission did not act in response to these concerns. Rather, shortly before the adequacy decision was adopted, the

[46] DPA, Sch 2, part 1, para 4.

[47] Draft adequacy decision, para 65.

[48] EDPB Recommendations 02/2020 (n 35) para 13.

[49] ibid.

[50] European Parliament Resolution (n 40) para 11.

Court of Appeal in England & Wales ruled in *The Open Rights Group & Anor, R (On the Application Of) v The Secretary of State for the Home Department & Anor* that the exemption did not include the necessary limitations and safeguards to protect the fundamental rights and freedoms of individuals.[51] This ruling prompted the Commission to exclude transfers for the purposes of UK immigration control from the scope of the adopted adequacy decision, but it agreed to reassess the exemption once UK legislators had addressed the issues raised in the judgment, which is appropriate given that an adequacy decision is a 'living' document that can and should be revised in light of changing circumstances.[52]

As for proposed changes, four are worthy of discussion to illustrate that if implemented in their current form, they represent minor changes by providing additional flexibility for organisations and addressing unnecessary administrative burdens and are therefore unlikely to jeopardise the EU–UK adequacy decision or its renewal in due course.

Firstly, the UK is proposing to redefine the parameters of what constitutes personal data by revising its test of identifiability to allow more data to be considered anonymous and outside the scope of the UK GDPR.

Currently personal data is defined as "any information relating to an identified or identifiable natural person". An "identifiable individual" is one who can be identified directly or indirectly. To determine whether an individual is indirectly identifiable, account should be taken of all the means 'reasonably likely' to be used either by the controller or by another person. Data which has been anonymised to the extent that it does not meet the standard of "personal data" does not fall within scope of the UK GDPR.[53]

The DPDI Bill proposed, and the DPDI No 2 Bill continues to propose, that information will relate to identifiable living individual' only where they are: "identifiable by the controller or processor by 'reasonable means' at the time of the processing", or "where the controller or processor knows, or ought reasonably to know, that another person will, or is *likely to, obtain*

[51] [2021] EWCA Civ 800.

[52] European Commission press release 'Data Protection: Commission Adopts Adequacy Decisions for the UK (28 June 2021) https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183. UNTIL the incompatible immigration exemption is remedied, personal data transfers for immigration control purposes may only be made using the transfer mechanisms in Arts 46–49 of the GDPR.

[53] Article 4 UK GDPR.

the information as a result of the processing, and the living individual will be, *or is likely to be, identifiable that person by reasonable means at the time of the processing."*[54]
This would limit the assessment of identifiability to the controller or processor and persons who are likely to receive the information, rather than anyone in the world (who might have the means to identify the data subject but are unlikely ever to access the data). It also proposes that identifiability be assessed at the time of processing – for example, where an organisation receives personal data without identifiers, but with a right to gain access to the identifiers on the occurrence of defined events in the future, such data would not be considered personal data until such events occur. This aspect of the proposed definition merely reflects the wording of recital 26 of the GDPR, which states that 'To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used' to identify the natural person, and that in ascertaining reasonable likelihood, 'account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.' It confirms that account should not be taken of means that are technically feasible but are unlikely to be used. This reflects the approach of Advocate General Campos Sánchez-Bordona in *Breyer v Bundesrepublik Deutschland,* in which he opined that if the contrary perspective were adopted, it would never be possible to rule out with absolute certainty 'that there is no third party in possession of additional data which may be combined with that information and are, therefore, capable of revealing a person's identity'.[55] As the UK was in the past the subject of infraction proceedings[56] for an overly narrow interpretation of personal data it will no doubt attract intense scrutiny when adequacy is reviewed. However, given that it mirrors the position adopted in *Breyer* and is a

[54] DPDI Bill (n 19) cl 1(2); DPDI Bill No 2 (n 30), cl 1(2).
[55] See Opinion of AG Campos Sánchez-Bordona in Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:339 para 65.
[56] Pounder, C. 'European Commission explains why UK's Data Protection Act is deficient, http://amberhawk.typepad.com/amberhawk/2011/02/european-commission-explains-why-uks-dataprotection-act-is-deficient.html; Pounder, C. 'Copy correspondence between Dr Chris Pounder and EU Commission & Ombudsman,' http://amberhawk.typepad.com/files/dp_infraction_reasons.pdf; Pounder, C. 'European Commission raises infraction threat to UK on failing to implement Directive 95/46/EC properly via the Data Protection Act,' http://amberhawk.typepad.com/amberhawk/2014/10/european-commission-raises-infraction-threat-touk-on-failing-to-implement-directive-9546ec-properly.html; the infraction proceedings were halted when Directive 95/46/ec was repealed and replaced by the GDPR.

mere gloss on the definition in the GDPR that adds clarity, this change is unlikely to prove problematic when the UK adequacy decision is reviewed.

Secondly, the DPDI Bill proposed (and the DPDI Bill No 2) continues to propose to introduce a new lawful basis for processing, namely processing that is necessary for the purpose of 'recognised legitimate interests'. Under the current law, data controllers are required to identify a lawful ground before processing personal data. These grounds include processing that is necessary for the legitimate interest of a data controller.[57] However, this can only be relied on to the extent that the organisation's interests are not outweighed by the interests of the individual (the 'balancing test'). In the DaND consultation, the UK government contended that applying the balancing test is too complex and forces organisations to inappropriately rely on another lawful ground: consent. This prompted the government to remove the balancing test (though not the necessity test) for a limited list of legitimate interests specified in the DPDI Bill. The proposed list (in a new annex to the UK GDPR) is automatically deemed to have a legitimate interest lawful basis without requiring an assessment balancing such interest with the rights and interests of the relevant data subject(s). At present, the lists of purposes include processing for reasons of 'public interest,' and includes public security, emergency response, crime prevention and detection, democratic engagement, and safeguarding children/vulnerable adults.

The DPDI Bill (No2) proposes to add to the non-exhaustive list of activities that may be regarded as in a data controller's legitimate interest to process data by moving illustrative activities currently listed in recitals to the operative part of the UK GDPR.[58] The activities are direct marketing, intraorganizational transmission of data and network and information systems security. Data controllers will still be required to ensure their interests are not outweighed by the data subject's rights and interests. And, as commentary in the Explanatory Notes to the Bill confirms that any legitimate commercial activity can be a legitimate interest, provided the processing is necessary and the balancing test is carried out, this change is unlikely to prove problematic when the EU-UK adequacy decision is reviewed. However, the DPDI Bill further stipulates that the Secretary of State for Science, Innovation and Technology (DSIT) may in the future amend this list so that more processing may be conducted on a legitimate interest basis without necessitating a balancing test. The Secretary

[57] UK GDPR, Art 6(1)(f).

[58] Recitals 47, 48 and 49 of the UK GDPR become a new Article 6(9).

of State will therefore need to ensure that any additional categories comply with forthcoming EDPB guidance on legitimate interests once it is issued to retain the current UK adequacy decision and ensure its renewal in due course.

Thirdly, the DPDI Bill proposed and the DPDI Bill No 2 includes a proposal that was not included in the DaND consultation. The proposal is to remove Article 27 of the UK GDPR, which would mean that overseas controllers and processors without an office or other establishment in the UK but who offer goods or services in the UK or monitor the behaviour of UK data subjects would no longer be required to appoint a UK representative as their local point of contact. The government's rationale is that 'in order to identify an organisation's representative, one must first identify the relevant controller or processor anyway, resulting in duplication and an unnecessary burden on organisations'.[59] Whilst this is viewed as an example of the government seeking to remove unnecessary red tape and barriers to trade, some legal experts have commented that 'the evidence presented on the impact of the change is far less convincing'[60] because 'it is increasingly being adopted around the world',[61] noting that the requirement to appoint a representative is also a feature of data protection of other countries beyond the EEA, including China, Thailand, Turkey, Serbia, Switzerland and Thailand. In effect, the UK could remove the Article 27 requirement without jeopardising the EU–UK adequacy decision only to find that it needs to include a similar provision to secure data transfers with another country.

Fourthly, a proposal in the DaND consultation for the UK to use a different test than that in the GDPR when assessing the adequacy of third countries could, if implemented, have given the Commission serious pause for thought when reassessing UK adequacy. It proposed that UK adequacy assessments would involve a risk- and outcome-based approach that considered 'actual risks' to data subjects' data protection rights in the applicant third country, rather than 'academic or immaterial' risks. The underpinning rationale was that practices undermining data subject rights may exist in some specific sectors but not in others such that transfers to the sectors in which the risk to the data subject is low or immaterial should not be impeded.

---

[59] DPDI Bill Explanatory Notes, https://publications.parliament.uk/pa/bills/cbill/58-03/0143/en/220143en.pdf, para 185.

[60] A Mätzler and C Mason, 'The Value of a UK Representative: A Response to the Data Protection and Digital Information Bill', Privacy Law & Business UK Report (November 2022).

[61] ibid.

However, it was not clear how the 'likelihood and severity of risks to data protection rights' would be assessed. The ICO was therefore not alone in calling for clarification of 'how a risk-based approach would work in practice'.[62] Ultimately, this proposal was not included in the DPDI Bill.

Instead, the DPDI Bill includes what appears at first glance to be a new 'data protection test' involving a determination of whether the standard of protection provided for data subjects in a third country is 'not materially lower' than the standard of data protection provided in the UK. The test would be applied by both the Secretary of State (when making adequacy decisions) and data controllers (when deciding whether it is safe to use other transfer mechanisms).[63] The test mirrors the criteria of Article 45 GDPR inasmuch as it specifies that the following factors should be considered: respect for the rule of law and for human rights, and any relevant international obligations; the existence of a data protection regulator and the extent of their enforcement powers; arrangements for redress by individuals, whether through the courts or otherwise; and the constitution, traditions and culture of the country in question. The explanatory notes to the Bill clarify that the test would not require a 'point-by-point comparison' between the other country's regime and the UK's. Rather, the assessment would be 'based on outcomes i.e., the overall standard of protection for a data subject'.[64]

While there is some scope for flexible interpretation of what constitutes a 'material' lowering of the standard of protection, the change looks at first glance like mere semantics, ie replacing the words 'essentially equivalent' with 'not materially lower', a view confirmed by a Department for Digital, Culture, Media and Sport (DCMS) representative (the government department sponsoring the Bill) when speaking at a National Data Strategy Forum in mid-July 2022, who emphasised that there had been discussions with the Commission and EU Member States to check that these proposed changes would not jeopardise the adequacy decision, which suggests that the changes are cosmetic and would be unproblematic when UK adequacy were reviewed in due course. However, if the wording changes significantly

---

[62] ICO, 'Response to DCMS Consultation "Data: A New Direction"' (6 October 2021) https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf; Open Rights Group, 'Response to Data: A New Direction' (19 November 2021) www.openrightsgroup.org/publications/open-rights-group-response-to-data-a-new-direction/.

[63] DPDI Bill (n 19) Sch 5; DPDI Bill No 2 (n 30) Sch 5.

[64] DPDI Bill Explanatory Notes (n 59) para 704.

during the passage of the Bill or its interpretation subsequently results in a significant lowering of the UK standard such that a third country (eg the USA) is found adequate by the UK when it has not been found adequate by the EU, this element of the DPDI Bill would warrant intense scrutiny by the Commission and could jeopardise the renewal of the EU–UK adequacy decision in due course.

B. De Facto Procedural Protection and Remedies

The Commission is also required, when assessing adequacy, to make a de facto determination that data protection does not just exist on paper but is effectively operationalised. In this regard, Article 45(2)(a) GDPR requires the UK to have 'effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred',[65] and also to have 'an effective independent supervisory authority with adequate enforcement powers for assisting and advising data subjects in exercising their rights, and for cooperation with EU supervisory authorities'.[66] In effect, the Commission seeks confirmation that the oversight and enforcement powers exercised by the UK national supervisory authority (the ICO) and the courts do not just exist on paper but are real and operational, so that data subjects have effective rights, means of recourse and remedies available to them.

When assessing adequacy, the Commission commented favourably on the relatively large number of staff at the ICO, together with the sources of its funding, and on the high number of complaints received and investigations opened by the ICO since the GDPR came into effect. It also recorded that UK domestic courts have oversight of data protection matters, and that there are mechanisms for EU data subjects to obtain redress either from the ICO or from the courts. However, the EP noted that it was not clear that the ICO was using its enforcement and fining powers effectively. Specifically, it noted that the ICO had a poor track record of enforcement action under predecessor legislation[67] and had not used its

---

[65] GDPR, Art 45(2)(a).

[66] GDPR, Art 45(2)(b).

[67] C Pounder, 'Adequacy of the UK's Data Protection Regime; now the UK Has Left the EU, the Battle Lines Are Drawn' (3 February 2020) https://amberhawk.typepad.com/amberhawk/2020/02/adequacy-of-the-uks-data-protection-regime-now- the-uk-has-left-the-eu-the-battle-lines-are-drawn.html; European Commission press release, 'Data Protection: Commission Requests UK to Strengthen Powers of National

enforcement powers under the GDPR while the UK was a Member State of the EU, leading the EP to question whether this is a structural weakness of the ICO.[68] Consequently, both the EDPB opinion and the EP resolution called for monitoring by the Commission of the ICO's exercise of its enforcement powers.[69] Specifically, the EDPB noted that it was satisfied that the ICO has adequate enforcement powers 'on paper', but asked for continuous monitoring to ensure that those powers are in fact exercised effectively.[70]

Although proposals in the DPDI Bill (No2) to replace the Information Commissioner with an Information Commission, a collegiate body with members appointed by the Secretary of State, are not likely to cause immediate concern, the Commission will undoubtedly review whether the appointments are undermining the independence of the Information Commissioner when reviewing adequacy.

In addition, the proposals to impose new duties on the Information Commission, including 'promoting innovation and competition',[71] and for it to have regard to the government's strategic priorities (which will be set out by the Secretary of State in an official 'statement of priorities' laid before Parliament) when exercising its regulatory functions,[72] and a power for the Secretary of State to approve statutory Codes of Practice are likely to warrant close scrutiny by the Commission. As the European Data Protection Supervisor has observed, 'any changes that make it less independent or require it to push through a political agenda will naturally force the Commission to raise concerns, ask questions, and seek assurances'.[73] If the UK government uses these provisions, either immediately or over time, to limit the independence and regulatory freedom of the ICO, they are likely to prove a bar to achieving a finding of adequacy when the UK adequacy decision is reviewed.

Data Protection Authority, as Required by EU Law' (24 June 2010); Ministry of Justice, 'Letter to Dr Chris Pounder' (5 May 2011) https://amberhawk.typepad.com/files/uk-deficiency-details_may-2011-1.pdf.

[68] European Parliament Resolution (n 40) General Observation 6.

[69] European Parliament Resolution (n 40) Enforcement of the GDPR, 6.

[70] EDPB Opinion 14/2021 (n 04), paras 111& 113.

[71] DPDI Bill (n 19) cl 27; s 120B; DPDI Bill No 2 (n 30) cl 27

[72] DPDI Bill (n 19) cl 28; DPDI Bill No 2 (n 30) cl 28

[73] N Hodge, 'EDPS: UK GDPR Reforms Could Create Friction with EU' (*Compliance Week*, 13 July 2022) https://www.complianceweek.com/data-privacy/edps-uk-gdpr-reforms-could-create-friction-with-eu/31851.article

C. Access to EU Personal Data by the Third Country's Authorities

The element of the UK adequacy assessment that was expected to be most unpredictable and controversial was the powers in the Investigatory Powers Act 2016 (IPA 2016) that permit UK security and intelligence services such as MI5, MI6 and GCHQ to both access personal data and share it with other countries for law enforcement and national security purposes.

As the CJEU expressly held in *Schrems II* that the national security exemption in the EU Treaties only applies to national security-related activities of the EU Member States and does not apply to national security-related activities of third countries',[74] the UK could not rely on this exemption to shield its surveillance law from scrutiny by the Commission. Moreover, as a third country, it should have been assessed by reference to the EU Charter and related CJEU jurisprudence and the essential security guarantees developed by the EDPB, and not by reference to the ECHR and related jurisprudence (by which the bulk interception by security intelligence agencies in Member States are assessed). The main difference between CJEU jurisprudence and that of the European Court of Human Rights (ECtHR) is that in *Digital Rights Ireland* the CJEU held that 'generalised, indiscriminate' collection of personal data is incompatible with the Charter (while making a very limited exception in relation to bulk collection to deal with a most serious, real threat to the very foundations and functioning of the state, which must still be strictly limited in time and place),[75] whereas the ECtHR held in *Big Brother Watch* that the decision to operate a bulk interception regime falls within the wide margin of appreciation granted to countries and instead requires very strong oversight and supervisory procedures, and that all the relevant parameters should be expressly stated in the relevant law.[76]

It is highly doubtful that the processing of personal data by UK security and intelligence agencies, especially bulk communication data, complies with the EU Charter of Fundamental Rights. Specifically, the indiscriminate bulk collection of communications metadata ('related communications data') from transatlantic undersea cables is contrary to principles

---

[74] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd* (*Schrems II*) ECLI:EU:C:2020:559, para 81.

[75] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Other*s, ECLI:EU:C:2014:238, paras 48 and 52.

[76] *Big Brother Watch And Others v The United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (Grand Chamber judgment) paras 338–40.

established by the CJEU (*Tele2/Watson*,[77] *Digital Rights Ireland*,[78] *Schrems II*,[79] *Privacy International*,[80] and *La Quadrature du Net*),[81] as reflected in the EDPB's 'European Essential Guarantees for Surveillance Measures'.[82]

Yet, the Commission selectively highlighted compliance with the ECHR and EU Charter and glossed over problematic aspects to find the UK adequate.[83] For instance, it cited paragraphs in the *Big Brother* ECtHR judgment that found predecessor UK surveillance law compliant with the ECHR[84] as evidence that the UK provides an adequate level of protection. Notably, it did not mention that the *Big Brother* case held that some aspects of the UK's predecessor legislation were in violation of the ECHR, merely noting, in a footnote, that 'It is important to bear in mind that this judgment concerned the previous legal framework (RIPA 2000) that did not contain some of the safeguards (including prior authorisation by an independent Judicial Commissioner) introduced by the IPA 2016'.[85] Significantly, the Commission did not expressly assess whether these safeguards in the IPA 2016 met the ECHR standards. Likewise, although the Commission considered *Tele2/Watson,* a case in which the CJEU ruled that the UK's predecessor legislation[86] breached EU law because it allowed for general and indiscriminate retention of citizens' data by law enforcement authorities and further determined that access to and use of mandatorily retained communications data should, with

---

[77] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson and Others* ECLI:EU:C:2016:970, para 120.

[78] *Digital Rights Ireland* (n 75).

[79] *Schrems II* (n 74).

[80] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790.

[81] Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* ECLI:EU:C:2020:791.

[82] EDPB Recommendations 02/2020 (n 35).

[83] Korff contends, inter alia, that the draft decision completely failed to assess (or even note) the UK's intelligence agencies' actual surveillance practices: D Korff, 'The Inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, Executive Summary' (3 March 2021); www.ianbrown.tech/wp-content/uploads/2021/03/KORFF-The-Inadequacy-of-the-EU-Commn-Draft-GDPR-Adequacy-Decision-on-the-UK-210303final.pdf.

[84] European Commission, Implementing Decision (n 1) fnn 269, 294, 365, 385, 441 and 505 and para 269.

[85] ibid fn 37.

[86] The Data Retention and Investigatory Powers Act 2014.

the exception of cases of validly established urgency, 'be subject to a prior review carried out either by a court or by an independent administrative body',[87] it did not explore in detail whether these deficiencies are addressed in the IPA 2016.

The Commission's conclusion that any interference with the fundamental rights of individuals 'will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists',[88] was therefore criticised by both the EDPB and the EP. Nevertheless, the Commission did not require the UK to amend the surveillance powers in IPA 2016 prior to adoption of the adequacy decision.

The adequacy assessment also required a review of procedures and practices for the onward data transfers of personal data from an applicant third country to other third countries for intelligence purposes since such transfers could undermine the GDPR and fundamental rights protections. The UK's membership of the Five Eyes alliance countries[89] and past sharing of personal data of individuals in EEA countries with each other and the UK's continued sharing of data with the USA via the US–UK Communications and Intelligence Agreement should have been a cause for concern for the Commission when assessing adequacy.[90] In an explanatory framework document, the UK government cited positive comments in a report from the UN Special Rapporteur for the Right to Privacy regarding how the UK has 'equipped itself with a legal framework and significant resources designed to protect privacy without compromising security' as confirmation that the UK has world-leading measures in place.[91] But in that same report, the Special Rapporteur was critical of international intelligence-sharing arrangements on the basis that they are 'not transparent to the public' and safeguards to avoid facilitating non-compliant surveillance by allies are not clearly set out in the IPA 2016,[92] and further commented that:

---

[87] *Tele2/Sverige* (n 77) reaffirming *Digital Rights Ireland* (n 75).

[88] Draft adequacy decision, recital 268.

[89] The Five Eyes alliance comprises the UK, the USA, Canada, Australia and New Zealand.

[90] European Parliament, 'Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs' (2013/2188(INI)).

[91] DCMS, 'Explanatory Framework for Adequacy Discussions, Section H: National Security Data Protection and Investigatory Powers Framework', 1.

[92] OHCHR, 'End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland,

> Intelligence sharing must not result in a backdoor to obtain or facilitate for others the obtaining of intelligence free from domestic safeguards, nor a loophole for foreign Governments with lower standards on the protection of privacy (or other human rights) to obtain intelligence from UK intelligence that could give rise to human rights violations.[93]

Consequently, he endorsed calls for greater public scrutiny of such arrangements and for the establishment of strong safeguards and an oversight system to ensure that intelligence sharing is subjected to the same standards of privacy protection – and the Commission should have paid keen attention to this aspect of the IPA 2016 when assessing adequacy. These concerns were echoed by the EDPB, which called for further examination of safeguards in respect of overseas disclosures and in the EP resolution, which observed 'in relation to the US, UK citizens are subject to some informal safeguards between GCHQ and the NSA … these safeguards would not protect EU citizens or residents whose data may be subject to onward transfers and sharing with the NSA'.[94] Even so, the Commission did not make these amendments prior to adoption of the adequacy decision.

Although a review of powers in the IPA 2016 was outside the scope of the DaND consultation, the provisions in the IPA 2016 could nevertheless prove problematic when the UK applies for a renewal of the adequacy decision because the Commission has a track record of seeking incremental changes to bring a third country's laws and practices into closer alignment with EU law when it seeks renewal of its adequacy decision.[95]

V. Conclusions: Alignment with or Divergence from the GDPR?

In conclusion, the legal and trade benefits of securing an adequacy decision to facilitate seamless EEA–UK personal data transfers persuaded the UK government to overcome its initial reluctance to apply for one when the UK left the EU and became a third country for data protection purposes, and it is now keen to retain it for those same reasons.
Whilst some of the political rhetoric accompanying the consultation and legislative proposals emphasised divergence from the GDPR and EU Institutions as a supposed 'Brexit Dividend,'

London, 29 June 2018' www.ohchr.org/en/statements/2018/06/end-mission-statement-special-rapporteur-right-privacy-conclusion-his-mission?LangID=E&NewsID=23296.

[93] ibid.

[94] European Parliament Resolution (n 40) Mass Surveillance, 16.

[95] The Commission used annual reviews of the (now revoked) EU–US Privacy Shield Decision to require the USA to make changes to its laws and practices.

the government appears to have resiled from the more radical divergence proposals in response to consultation feedback and input from the ICO. Many of the proposals seek to clarify definitions, make appropriate use of white space in the UK GDPR to facilitate innovation, and reduce administrative burdens. For example, the DaND consultation proposed to utilise a risk-based approach when assessing third country adequacy, but this proposal was not included in the DPDI Bill, nor is it included in DPDI Bill No2. Instead, it proposes to use a 'not materially lower' test akin to the 'essentially equivalent' test in the EU GDPR when assessing third country adequacy. Several other proposed changes in the DPDI No2 Bill (eg the proposed narrower definition of personal data) represent an evolution rather than revolution in UK data protection law and are therefore likely to be favourably received during any review of the adequacy decision by the Commission.

Nevertheless, a few proposed changes, eg in the potential reduction of ICO independence and the Secretary of State having the power to add to the list of recognised legitimate interests, will, if implemented unchanged, attract scrutiny by the Commission, who will seek confirmation that they do not constitute significant divergence from the GDPR. To avert this, the UK should seek to maintain a close working relationship with the Commission and heed any guidance issued by it on how to revise provisions in the UK GDPR in a manner that maintains alignment with the GDPR; otherwise, the EU–UK adequacy decision or some aspects of it might not be renewed in due course.

The UK's continued alignment with the GDPR is necessary as significant divergence from it would not be a prudent course of action when the global trend is towards higher rather than lower data protection standards and many of the UK's trading partners are using the GDPR as their operational benchmark on a global basis. Diverging from the EU standard of data protection would not give the UK a competitive advantage since many organisations are subject to both the UK and the EU regime. Instead, it could jeopardise the renewal of the EU–UK adequacy decision in due course and place additional burdens on businesses with multinational operations since it would require them to operate multiple standards to trade in the UK, the EU and beyond.