Cambridge Yearbook of European Legal Studies (2025), 1–22
doi:10.1017/cel.2025.10018

RESEARCH ARTICLE

Digital Empire or Digital Fiefdoms? Institutional Tensions and the EU Right to Data Protection

Orla Lynskey[1], Maria Helen Murphy[2] and Katherine Nolan[3]

[1]UCL Laws, Chair of Law and Technology, London, UK; [2]Associate Professor, School of Law and Criminology, Maynooth University, Ireland and [3]Assistant Lecturer in Law, Technological University Dublin, Dublin, Ireland
Corresponding author: Orla Lynskey; Email: o.lynskey@ucl.ac.uk

All authors contributed equally to the development and drafting of this article.

Abstract
The EU has been represented as a singular 'Digital Empire' speaking with one voice on matters of EU digital regulation. Closer examination of discrete areas of EU digital regulation reveals a more nuanced picture suggesting clear institutional divergence between the EU institutions regarding the substantive protection afforded by EU law. A detailed analysis of EU data protection adequacy decisions brings to the surface intra-EU tensions concerning the substance of core EU fundamental rights. This analysis reveals that the EU Commission has taken on a more prominent role in adequacy decision-making since the entry into force of the EU's General Data Protection Regulation at the expense of other relevant stakeholders. Furthermore, the Commission's decisional practice does not align fully with the stance of the Court of Justice on the right to data protection. New sites of intra-EU human rights tensions are therefore uncovered with consequences for the legitimacy of the EU as a digital regulator and the role of the Commission as a guardian of the treaties.

Keywords: digital regulation; fundamental rights; data protection; institutional balance; judicial review; data adequacy; EU Commission

I. Introduction

The EU approach to digital regulation is characterized as a rights-centric regulatory approach, which seeks to ensure that digital actors are governed in a way that respects and upholds EU values.[1] As former Internal Market Commissioner Thierry Breton infamously reminded Elon Musk following his acquisition of the micro-blogging platform Twitter (now X), 'In Europe, the bird will fly by our rules'.[2] Presented as such, the EU represents a singular 'Digital Empire' speaking with one voice on matters of EU digital regulation and, more fundamentally, the digital social contract in Europe. Indeed, this rights-based regulatory agenda enjoys strong popular support from EU residents.[3] Nevertheless, empirical analysis of discrete areas of EU digital policy, in this instance EU data protection adequacy decisions, reveals a more nuanced picture suggesting clear divergence between EU institutions regarding the appropriate balancing of fundamental rights and other interests. This divergence has significant consequences for the level of substantive protection afforded by EU law. The EU is therefore less of a digital empire and more of a series of digital fiefdoms each with its

[1]A Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press, 2023).
[2]'Musk's Twitter "bird will fly by EU rules," Brussels warns on takeover', *Euronews*, 28 October 2022 <https://www.euronews.com/next/2022/10/28/done-deal-elon-musk-now-has-control-of-twitter-and-has-already-fired-its-top-executives>
[3]Bradford, note 1 above, p 107.

own conception of what rights-centric regulation entails. This finding is of particular salience as core elements of more recently adopted EU digital regulation will be enforced directly by the Commission.

This paper proceeds as follows. It first provides a brief introduction to EU data protection law, including the 'adequacy' regime for data transfers from inside the EU to outside the EU. Next, the paper examines the inner workings of the adequacy framework, by conducting a qualitative analysis of all adequacy decisions adopted by the EU Commission under both the 1995 Data Protection Directive and the General Data Protection Regulation (GDPR).[4] This analysis reveals two key findings. First, procedurally, expert input has been progressively marginalized in the process of adopting adequacy decisions, thereby strengthening the role of the European Commission. Second, substantively, the Commission deviates from the high standards set by the European Data Protection Board (EDPB) and the Court when adopting and renewing adequacy decisions. This analysis surfaces important questions for EU data protection law, in particular about which institution is driving the development of the right to data protection and how. However, it also raises broader questions about the legitimacy of the Commission's actions and the extent of judicial oversight in this sphere. These challenges are relevant not only to other areas of EU digital regulation (such as the enforcement of the EU's digital acquis) but also, more broadly, to the Commission's role as guardian of the treaties. These consequences are examined in the final section.

II. An introduction to adequacy

EU data protection law regulates personal data processing, legitimizing such personal data processing where it complies with principles relating to personal data processing, which internalize proportionality requirements,[5] and has a legal basis.[6] This system of checks and balances for personal data processing places an obligation of demonstrable accountability on those who spearhead data processing obligations ('data controllers'), gives rights to individuals vis-à-vis these data controllers and creates national supervisory authorities responsible for overseeing enforcement within their respective Member States.[7] From its inception in 1995, the EU data protection framework has pursued dual objectives: it seeks to ensure the free flow of personal data within the EU while protecting fundamental rights when personal data are processed. These dual objectives are interconnected insofar as the presumptively equal (and high) level of data protection offered by all EU Member States as a result of regulatory harmonization eliminates objections to the free flow of personal data by Member States on the basis of fundamental rights concerns. While interconnected, the emphasis in the jurisprudence of the CJEU on one or the other of these objectives has fluctuated over time. Early data protection jurisprudence remained more aligned to data protection's market harmonization objective (and legal basis) while later case law, particularly following the entry into force of the EU Charter has emphasized its fundamental rights ambitions. Moreover, some of the Court's case law has been met with resistance from national courts (and indeed, national parliaments).[8] This is particularly true of the Court's invalidation of the EU's Data Retention Directive for its breach of Articles 7 and 8 EU Charter,[9]

[4]Respectively, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 and 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 (General Data Protection Regulation) [2016] OJ L 119/1.

[5]*Mousse v CNIL and SNCF*, C-394/23, EU:C:2025:2, para 24.

[6]GDPR, Arts 5 and 6.

[7] H Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (Springer, 2016).

[8]See discussion in N Vainio and S Miettinen, 'Telecommunications Data Retention after Digital Rights Ireland: Legislative and Judicial Reactions in the Member States' (2015) 23(3) *International Journal of Law and Information Technology* 290 and A Turmo, 'National security as an exception to EU data protection standards: The judgment of the Conseil d'État in French Data Network and others', (2022) 59(1) *Common Market Law Review* 203.

[9]*Digital Rights Ireland and Seitlinger and Others*, Joined cases C-293/12 and 594/12, ECLI:EU:C:2014:238.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

and its subsequent specification of the requirements stemming from these rights in that context.[10] These requirements ringfence the margin of manoeuvre of the EU and domestic legislatures should they wish to adopt similar legislative initiatives.[11] The data protection 'adequacy' regime must be understood against this backdrop. The presumption of equal human rights protection that applies between EU Member States because of their common commitment to the EU data protection framework, including the Charter, does not apply when data is transferred beyond the EU's borders. As a result, Chapter V of the GDPR contains a series of provisions that ensure the protection offered by EU data protection law is not circumvented when data is transferred from within the EU to entities outside the EU's borders.[12]

Chapter V envisages four categories of mechanism that facilitate transfers from within the EU to outside its borders (what we shall call 'international data transfers').[13] Such transfers can take place when one of an enumerated list of 'appropriate safeguards' are in place (including standard contractual clauses (SCCs) adopted between the parties to the transfer).[14] They can also take place when data is transferred within a group of undertakings or enterprises who adhere to 'binding corporate rules' regulating the conditions of personal data processing.[15] In the absence of an alternative mechanism, the GDPR foresees derogation for specific situations (for instance, on the basis of the consent of individual data subjects).[16] Each of these mechanisms entails a regulatory burden on the data controller as a data exporter. As a result, although SCCs are the most widely used transfer mechanism, the preferred mechanism for international data transfers of data controllers is an adequacy decision.[17] Through an adequacy decision, the EU Commission recognises that a 'third country, a territory or one or more specified sectors within that third country' ensures an adequate level of protection. An adequacy decision thus allows personal data transfers to occur without specific prior authorization (although still subject to compliance with the GDPR beyond Chapter V regarding such transfers).[18]

The CJEU has delivered important jurisprudence specifying the use of adequacy assessments by the EU Commission. In *Schrems*, the Court was asked by a national referring court to clarify the powers and responsibilities of a national data protection authority (DPA) when the validity of an EU act (a Commission adequacy decision) was in doubt.[19] The adequacy decision in this instance was the EU–US Safe Harbor Decision, which facilitated frictionless transnational data transfers between the EU and the USA under a self-regulatory scheme. Following the revelations of Edward Snowden,

[10] *Tele2 Sverige*, Joined cases C-203/15 and C-698/15, EU:C:2016:970; *Privacy International*, C-623/17, EU:C:2020:790; *La Quadrature du Net and Others*, C-511/18, EU:C:2020:791; *Ligue des droits humains*, C-817/19, EU:C:2022:491; *Commissioner of an Garda Síochána and Others*, C-140/20, EU:C:2022:258.

[11] A similar dynamic was at play in Opinion 1/15 when the Court assessed the compatibility of a draft international agreement with Article 8 Charter and deemed it incompatible. As Kuner notes, the Court's 'listing in its summation of how the Draft Agreement should be amended to meet the criticisms it made could be seen as an attempt to lend a helping hand to parties as they negotiate PNR agreements'. C Kuner, 'International Agreements, Data Protection, and EU Fundamental Rights on the International Stage: Opinion 1/15, EU-Canada PNR' (2018) 55 *Common Market Law Review* 857, p 874.

[12] Article 44(1) GDPR states 'All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined'.

[13] On the ambiguity of the 'transfer' concept, see G González Fuster, 'Un-mapping Personal Data Transfers' (2016)(2)2 *European Data Protection Law Review* 160.

[14] GDPR, Art 46.

[15] GDPR, Art 47.

[16] GDPR, Art 49.

[17] For instance, an annual survey of EU and US privacy professionals concluded in 2021 that following CJEU case law in *Schrems II* (discussed below) 94% of EU respondents rely on SCCs to conduct data transfers to third countries. IAPP-EY, Annual Privacy Governance Report 2021, Executive Summary, p. ix.

[18] GDPR, Art 45(1). International organisations can also be recognised as adequate.

[19] *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, EU:C:2015:650.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

a former National Security Agency contractor turned whistleblower, US national security and intelligence data processing practices came to public attention.[20] Bolstered by prior jurisprudence of the Court declaring mass and indeterminate data retention for law enforcement purposes to be illegal,[21] *Schrems* and other campaigners argued that the personal data transferred pursuant to the Safe Harbor decision could not be regarded as offering 'adequate' protection from an EU perspective. Regarding the powers of DPAs, the Court provided guidance in keeping with its Foto-Frost doctrine.[22] DPAs must examine individuals' complaints regarding the compatibility of Commission adequacy decisions with fundamental rights with due diligence, however, crucially, only the CJEU can declare such adequacy decisions invalid.[23]

Although not expressly asked to do so by the referring Court, the CJEU examined the validity of the Safe Harbor decision in light of EU law. It took the opportunity to substantiate the meaning of adequacy, which was not defined in secondary law. It observed that 'adequate' protection does not require identical data protection but does require a level of protection that is 'essentially equivalent' to that offered by EU secondary law read in light of the Charter.[24] Importantly, the CJEU found that it is the legal order of the third country—both applicable rules and the practices designed to ensure compliance with them—that must be adequate and that the Commission is obliged to verify this adequacy in law and practice periodically.[25] Furthermore, because the adequacy decision engaged with fundamental rights, the Court held that the Commission enjoyed reduced discretion when adopting adequacy decisions while the Court adopted a strict standard of review when reviewing such decisions.[26] The Court went on to invalidate the Safe Harbor decision on technical grounds, as the Commission had not explicitly stated the USA offers an adequate level of data protection to data transferred from the EU.

The findings in *Schrems* were divisive. For some, they led to widespread disruption across industries dependent on transatlantic data transfers.[27] FTC Commissioner Julie Brill, for instance, noted that the judgment came as an 'enormous shock' to many policy makers and companies on a scale 'that would seriously test most bridges'.[28] For others, such as the Vice-President Timmermans of the EU Commission, *Schrems* was 'a confirmation of the European Commission's approach for the renegotiation of the Safe Harbour', suggesting the Commission and the Court were on the same page at this time.[29] The inability to rely on Safe Harbour as a transfer mechanism post-*Schrems* led EU–US data exporters to adopt new transfer mechanisms. While the Commission negotiated a new adequacy mechanism with the USA, many data exporters turned to SCCs (a model form contract set out in a Commission decision—the 'SCC decision') to continue transferring data to the USA. The investigation of Meta's international data transfers continued in Ireland. On the basis of a reformulated complaint from Max Schrems, the Irish DPA determined in a draft decision that the validity of the

[20] BBC, 'Edward Snowden: Leaks that exposed US spy programme', 17 January 2014. https://www.bbc.com/news/world-us-canada-23123964.

[21] *Digital Rights Ireland and Seitlinger and Others*, EU:C:2014:238

[22] *Foto-Frost v Hauptzollamt Lübeck-Ost*, C-314/85 EU:C:1987:230.

[23] *Schrems*, EU:C:2015:650, paras 62 and 63.

[24] Ibid, para 73.

[25] Ibid, para 76.

[26] Ibid, para 78.

[27] A Robinson, 'US Tech Companies Overhaul Operations after EU Data Ruling', *Financial Times*, 6 October 2015; M Scott, 'Data Transfer Pact Between U.S. and Europe Is Ruled Invalid', *New York Times*, 6 October 2015; C Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18 *German Law Journal* 881.

[28] J Brill, 'Transatlantic Privacy After Schrems: Time for An Honest Conversation: Keynote Address at the Amsterdam Privacy Conference' (23 October 2015) <https://www.ftc.gov/system/files/documents/public_statements/836443/151023amsterdamprivacy1.pdf>

[29] Commission, 'European Commission Press Release, First Vice-President Timmermans and Commissioner Jourová's Press Conference on Safe Harbour Following the Court Ruling in Case C-362/14 (Schrems)' (6 October 2015) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_15_5782>

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

SCC decision was in doubt. The logic underpinning this finding was that if the data were offered inadequate protection once transferred to the USA then this would be the case irrespective of the precise mechanism used for data transfer (whether an adequacy assessment or a contractual mechanism). The Irish DPA, relying on the *Schrems* finding that national DPAs must be able to put well-founded concerns before the national courts,[30] commenced litigation before the Irish High Court, culminating in a further reference to the CJEU in *Schrems II*.[31]

In *Schrems II*, the CJEU considered three sets of issues. First, it found that irrespective of whether the data transferred was used in the USA for national security purposes, when the initial transfer was between economic operators for commercial purposes, the GDPR applies.[32] Second, it clarified the role of SCCs in the scheme of international data transfers. In particular, it confirmed that irrespective of the transfer mechanism used, the same level of protection of rights must be guaranteed.[33] As a result, a data exporter cannot rely on SCCs alone but must independently assess relevant aspects of the legal system of the non-EU state taking account of the factors relevant for adequacy assessments found in Article 45(2) GDPR (known as a transfer impact assessment).[34] In other words, in 'inadequate' countries, SCCs may not always be relied upon if there are practices in those jurisdictions which undermine the contractual protections in the SCCs. Finally, the Court assessed whether Privacy Shield, a replacement adequacy decision for Safe Harbor adopted by the EU Commission, was compatible with EU law.

Ultimately, Privacy Shield was also found to be deficient by the Court. In assessing Privacy Shield, the Court observed that, like Safe Harbor, it contained a wide-ranging derogation enabling interference with fundamental rights on the basis of national security, public interest requirements or US domestic law.[35] Significantly, the Court disagreed with the Commission's assessment that such interferences with fundamental rights were limited to what was strictly necessary and that the legal protection offered to EU residents was effective.[36] The Court highlighted two shortcomings of the US legal framework from an EU fundamental rights perspective. First, the interferences were not 'in accordance with the law' as required by analogy with Article 52(1) EU Charter. The relevant US law indicated no limitations on the power it conferred to implement surveillance programmes for foreign intelligence purposes. This is contrary to the EU law requirement that the legal basis enabling an interference with fundamental rights must define the scope of the limitation on the right in compliance with proportionality requirements.[37] The second shortcoming was that elements of the US legal framework offered EU residents no possibility to seek a legal remedy if their rights were violated, in part due to the inability of EU individuals to assert privacy actions before US courts to challenge covert surveillance.[38] The Court reiterated its *Schrems I* finding that the complete absence of a possibility to pursue legal redress constituted an interference with the essence of the right to an effective remedy.[39] As a result, the Court could not conclude that Privacy Shield offered essentially equivalent protection to that offered by EU law.[40] In appraising available redress options, the Court found a number of shortcomings with the 'Ombudsperson' redress mechanism in Privacy Shield.

[30] *Schrems*, EU:C:2015:650, para 65.

[31] *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. II (Schrems II)* Case C-311/18, EU:C:2020:559.

[32] Ibid, paras 85 to 88.

[33] Ibid, para 92.

[34] Ibid, paras 112 and 114.

[35] Ibid, para 165.

[36] Ibid, paras 167 and 168.

[37] Ibid, para 180; paras 175 and 176.

[38] Costello J in the Irish High Court cites a series of US constitutional court cases concerning standing to find that standing rules 'made it exceedingly difficult to challenge secret government surveillance programmes'. *Data Protection Commissioner v Facebook Ireland Ltd & anor* [2017] IEHC 545, para 253.

[39] *Schrems II*, EU:C:2020:559 para 187.

[40] Ibid, paras 187, 191 and 192.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

Specifically, the Ombudsperson was deemed insufficiently independent, and doubt was cast on the binding nature of its decision-making and the resulting legal safeguards afforded to individuals.[41] In other words, this type of negotiated administrative solution was not a substitute for the availability of judicial review. The Court concluded that the Commission had disregarded the requirements of Article 45(1) GDPR, read in light of the Articles 7, 8, and 47 of the Charter, in adopting the Privacy Shield adequacy decision, and it invalidated the decision with immediate effect.

This judgment has been received in vastly different ways. It was warmly welcomed in some quarters for reaffirming the EU's commitment to fundamental rights when personal data are processed, while roundly criticized by others.[42] For instance, former general counsel of the National Security Agency, Stewart Baker, saw the judgment as a 'gobsmacking mix of judicial imperialism and Eurocentric hypocrisy'.[43] US academics Propp and Swire criticized the application of 'an idealized, formal standard set forth primarily in EU law', whereas 'in the real world', EU Member States' own national security practices are not subject to EU supervision due to the reservation of national security to the Member States.[44] Meanwhile, regulators began to draw consequences from the Court's findings, with the Irish DPA threatening to ban EU–US data flows in the absence of appropriate safeguards. In addition to imposing an administrative fine of €1.2 billion on Meta Ireland in its May 2023 decision, the Irish DPA ordered it to suspend transfers of personal data to the USA within five months.[45] Meta promptly announced plans to appeal the decision and indicated its intention to rely on the new EU–US Data Privacy Framework, adopted as adequate in July 2023, for future transfers.[46]

Stepping back from the immediate consequences of the judgments, two elements of the Court's approach bear emphasising. First, Commission adequacy decisions are subject to a strict standard of judicial review. Second, the Court sets out prescriptive criteria, firmly anchored in the EU Charter, to guide the Commission's adequacy assessment. The Court's case law indicates that the Commission and the Court differ in their interpretation and application of the right to data protection in a manner that has huge practical significance.

The aspect of the data protection adequacy story presented thus far is known to EU lawyers, in particular those with data protection expertise. However, what has been subject to limited discussion and scrutiny is the procedure by which adequacy decisions are adopted.[47] Close inspection of the existing decisional practice of the Commission for adequacy assessments confirms that the Commission has marginalized the expert input that lends democratic legitimacy to adequacy decisions and pursues its own vision of adequacy in the process. This shall now be examined.

[41] Ibid, paras 195 and 197.

[42] NOYB, 'CJEU—First Statement', 16 July 2020, https://noyb.eu/en/cjeu; European Data Protection Supervisor, 'EDPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II")', 17 July 2020 (https://www.edps.europa.eu/press-publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling_en).

[43] S Baker, 'How Can the US Respond to Schrems II?', *Lawfare*, 21 July 2020 https://www.lawfareblog.com/how-can-us-respond-schrems-ii.

[44] K Propp and P Swire, 'After Schrems II: A Proposal to Meet the Individual Redress Challenge' *Georgia Tech Scheller College of Business Research Paper No. 3,680,148*, 13 August 2020, https://ssrn.com/abstract=3680148 or http://dx.doi.org/10.2139/ssrn.3680148.

[45] Data Protection Commission, 'Data Protection Commission Announces Conclusion of Inquiry into Meta Ireland', *Data Protection Commission*, 22 May 2023, <https://www.dataprotection.ie/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland>; European Data Protection Board, Binding Decision 1/2023 on the Dispute Submitted by the Irish SA on Data Transfers by Meta Platforms Ireland Limited for Its Facebook Service (Art. 65 GDPR) Adopted on 13 April 2023 <https://www.edpb.europa.eu/system/files/2023-05/edpb_bindingdecision_202301_ie_sa_facebooktransfers_en.pdf>

[46] 'Our Response to the Decision on Facebook's EU-US Data Transfers', *Meta*, 22 May 2023, <https://about.fb.com/news/2023/05/our-response-to-the-decision-on-facebooks-eu-us-data-transfers/>

[47] M Czerniawski, 'Shrouded in Secrecy—Does the Comitology Procedure for GDPR Adequacy Decisions Fit Its Purpose?' (2024) 18 *Masaryk University Journal of Law and Technology* 215.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

III. A spotlight on adequacy dynamics

The institutional framework for EU data protection law is complex. In addition to the role of the Court of Justice, national DPAs, and the EU Commission alluded to above, the GDPR created a new EU body—the EDPB. The EDPB is comprised of representatives of the DPAs as well as of the European Data Protection Supervisor (EDPS). The Commission participates in the activities of the EDPB in a non-voting capacity.[48] The EDPS is the only supranational entity with voting rights (on limited issues[49]) pursuant to the GDPR, leading to the suggestion that the EDPB is more of an intergovernmental club than an EU Agency.[50] The EDPB replaces the 'Article 29 Data Protection Working Party' (A29WP) which had a similar composition under the 1995 Directive, but was not an official EU body and had no binding powers.[51]

The details of the process for adopting adequacy decisions are not specified in secondary legislation. Czerniawski notes that Commission adequacy decisions, which are implementing acts, are subject to *ex ante* and *ex post* control. The *ex post* control of adequacy decisions by the CJEU is discussed above. What receives less attention is the *ex ante* control of adequacy decisions. Such control is exercised by the 'Article 93 Committee', a comitology committee which within the framework of regulated comitology procedures issues a formal opinion on draft adequacy decisions. This Committee is quite active: for instance, between the entry into force of the GDPR and April 2025 it held 25 meetings.[52] The Article 93 Committee has the power (which has not yet been exercised) to prevent the Commission from adopting an adequacy decision, which ostensibly only gives the Committee a binary option to accept or reject the text proposed by the Commission. Czerniawksi concludes that this 'confirms the limited role played in practice by Member States in the whole procedure and the strong position of the European Commission'.[53]

However, historically there has been robust *ex ante* influence over Commission adequacy decisions by the A29WP who has guided and offered expert input into the process, a factor which is overlooked in many accounts of adequacy decisions. This role has two key elements. In the absence of detailed criteria for adequacy assessments in the legislative text, the A29WP adopted a working document in 1998 that has guided this substantive assessment. This is the so-called 'adequacy referential' (WP12).[54] An updated version of this working document was prepared following the adoption

[48] It is notable that the initial draft of the GDPR proposed a more central role for the Commission within the EDPB. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011, arts 59-60.

[49] These voting rights are limited only to cases 'which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation'. EDPS, 'The EDPS as an Advisor to EU Institutions on Policy and Legislation: Building on Ten Years of Experience', 4 June 2014, p 17.

[50] L Jančiūtė, 'European Data Protection Board: A Nascent EU Agency or an "Intergovernmental Club"?' (2020) 10(1) *International Data Privacy Law* 71.

[51] The EDPB secretariat is provided by the EDPS as opposed to the Commission as had been the case for the A29WP. GDPR, Art 75. The A29WP had advocated for a 'completely independent' secretariat. A29WP, 'Opinion 01/2012 on the data protection reform proposals' (WP 191 00530/12/EN), 23 March 2012, p 22 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf >; L Jančiūtė, 'European Data Protection Board: A Nascent EU Agency or an "Intergovernmental Club"?' (2020) 10(1) *International Data Privacy Law* 69. In reference to the EDPB's task of providing guidance in continuance of the work of the A29WP, Hijmans noted some potential 'competition with the role of the Commission as the guardian of the Treaties.' H Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (Springer 2016) 427.

[52] See, European Commission, Comitology Register, available at: https://ec.europa.eu/transparency/comitology-register/screen/committees/C49000/consult?lang=en.

[53] Czerniawski, note 47 above, 228.

[54] A29WP, 'Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive' 24 July 1998 (WP12) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

of the GDPR, and updated again following *Schrems I*, representing an extension rather than an overhaul of the original list of adequacy criteria (WP254).[55] Furthermore, an additional document was prepared setting out the 'essential guarantees' for public authority and law enforcement access to data for the GDPR era (WP237). Adequacy decisions have generally adhered closely to the criteria set out in these documents, however, the rigour in the application of these criteria has varied quite significantly, and some adequacy decisions adopted prior to the GDPR's adoption are quite cursory in their findings. The second key role played by the A29WP is to provide the Commission with an opinion on its assessment of the adequacy of the third country or entity under examination. For every adequacy decision that has been adopted to date, the A29WP or EDPB have provided an opinion. The GDPR formalized this role. It provides that the EDPB shall, on its own initiative or at the request of the Commission, provide the Commission with an opinion on its assessment of the adequacy of the level of protection offered by a relevant third party, including assessments where the entity no longer ensures an adequate level of protection.[56] This provision also states that the Commission shall provide the EDPB with 'all necessary documentation' with regard to that entity.

Our qualitative examination of the existing corpus of adequacy decisions and the associated A29WP/EDPB opinions, adopted both prior to the entry into force of the GDPR (11 decisions, excluding Safe Harbor) and following its entry into force (4 GDPR adequacy decisions, including the EU–US Data Privacy Framework) suggests that this expert input is now increasingly marginalized in important ways.[57]

A. The strengthened role of the commission and the marginalization of expert input

In this section, by reference to existing adequacy decisions, we can see how the EDPB now plays a more limited role than its predecessor in relation to the initial adoption of new adequacy decisions. Its role is even more minimal in the review of existing decisions.

When new adequacy decisions are adopted the Commission provides the information it has gathered to the EDPB for its opinion, as foreseen by the GDPR.[58] This reflects an important change to prior practice. Under the 1995 Directive, the A29WP was more involved and engaged directly with relevant third countries, most frequently via their DPAs. For example, the A29WP makes reference to the direct provision of information by the Faroese to them for the purposes of the assessment,[59] seeking information and clarification from the New Zealand Privacy Commissioner regarding the preliminary expert report commissioned by the Commission on New Zealand data protection laws,[60] and similar engagement with the Uruguayan authorities via their DPA.[61] When the Israeli Mission to the European Union requested an adequacy assessment from the Commission, the Safe Harbor Subgroup of the A29WP sent a letter to Israeli authorities emphasizing issues requiring reform. In response, the

[55] A29WP, 'Adequacy Referential,' 27 November 2017, as last revised and adopted on 6 February 2018, (WP 254 rev.01) https://ec.europa.eu/newsroom/article29/items/614108.

[56] GDPR, Art 70(1)(s).

[57] The methodology for our approach is set out in the Annex.

[58] This is explicitly noted in the adequacy decisions for Japan; Korea; the UK and the US.

[59] 'The Faroe Islands has informed the Article 29 Working Party that the original translation of Article 22, part 1, no. 5, in the Faroese Act is inaccurate. … The Faroe Islands has further informed the Article 29 Working Party that the exemption has to be assessed in connexion with the Faroese Act concerning Access to Documents in Administrative Files to which the Faroese Act on Processing of Personal Data has references. … The Faroe Islands has finally informed the Article 29 Working Party that the exemption in Article 22, part 1, no. 5, is copied directly from the Norwegian Act concerning the processing of personal data.' A29WP, 'Opinion 9/2007 on the level of protection of personal data in the Faroe Islands,' 9 October 2007, (WP 192), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp142_en.pdf, p 7.

[60] A29WP, 'Opinion 11/2011 on the level of protection of personal data in New Zealand,' 4 April 2011, (WP 182) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp182_en.pdf, p 2.

[61] A29WP, 'Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay,' 12 October 2010, (WP 177), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf pp 2-3.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

Israeli authorities sent an 'extensive report' to the A29WP via the Israeli DPA, prompting the A29WP to seek further clarification of certain issues from the Israeli authorities.[62]

Beyond this procedural change, there is a fundamental ambiguity regarding the status of the EDPB's adequacy opinions. Their classification as opinions rather than decisions indicates that they are not binding. This therefore allows the Commission to ignore the reservations expressed by the EDPB should it wish. There is some evidence that this is occurring in practice. For instance, in its opinion on Japanese adequacy, the EDPB observed that having analyzed the draft adequacy decisions and the Japanese legal framework, 'a number of concerns, coupled with the need for further clarifications, remain'.[63] The Commission also published its draft decisions on UK adequacy before initiating the formal procedure for its adoption.[64] It was only following this provisional 'greenlighting' of the adequacy decision that the EDPB was asked for its opinion which it delivered in April 2021. The decision was then adopted in June 2021 following Member State input through the comitology procedure. The sequencing—which minimises the scope for meaningful input—was similar for the US Data-Privacy Framework. The Commission reached an 'agreement in principle' with the USA (announced jointly by President Biden and European Commission President von der Leyen) in March 2022 before a draft adequacy decision was reached in December 2022. The EDPB delivered its opinion in February 2023 with the decision adopted and the formal process completed by 5 months later. This political stage of adequacy is recognized in the doctrine, albeit that its legitimacy is not addressed. Kuner, for instance, observes that:

> the Commission always holds detailed discussions with a third country before issuing an adequacy decision, resulting in an informal commitment to bring its legal standards in line with those of the EU, which can be regarded as an 'agreement in principle'.[65]

This late involvement of the EDPB, in contrast to the role of the former A29WP in adequacy decisions from the outset, suggests its influence on adequacy is much more limited than was previously the case.

In addition to this enhanced role of the Commission at the expense of the EDPB in adopting new adequacy decisions, the EDPB is also marginalized when adequacy decisions are reviewed. The Commission is under an obligation pursuant to the GDPR to review existing adequacy decisions periodically. While immediate review of all previous adequacy decisions following the GDPR's entry into force may have been impractical, the Commission came under significant scrutiny for the considerable delay in reviewing the 11 adequacy decisions adopted under the 1995 Directive following the GDPR's entry into force in May 2018. When it did conduct this adequacy review (over five and a half years later, in January 2024), the materials published consisted of a short review document[66] and a more detailed staff working document (SWD).[67] Its substantive finding that the legal offering of all

[62] A29WP, 'Opinion 6/2009 on the level of protection of personal data in Israel,' 1 December 2009, (WP 165) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp165_en.pdfpp 2-3.

[63] EDPB, 'Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan,' 5 December 2018, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282018-regarding-european-commission-draft_en para 30 and 55/56.

[64] Commission, 'Press Release: Data Protection: European Commission Launches Process on Personal Data Flows to UK', 19 February 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.

[65] C Kuner, 'International data transfers and the EDPS: current accomplishments and future challenges' in EDPS, *Two decades of personal data protection. What next? EDPS 20th Anniversary* (Publications Office of the European Union, 2024) https://www.edps.europa.eu/system/files/2024-06/edps_20thanniversary-book_en.pdf.

[66] Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC COM/2024/7 final, 15 January 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024DC0007.

[67] Commission Staff Working Document Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC Accompanying the document Report from the Commission to the European Parliament and the Council

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

11 countries reviewed remained adequate has been the subject of criticism.[68] Our primary concern here is not the substantive merit of these review findings but rather the process by which the findings were made. The EDPB was not formally consulted by the Commission about these findings. The wording of Article 70(1)(s) GDPR states that the EDPB provides the Commission with an opinion for the assessment of adequacy 'including for the assessment whether a third country …no longer ensures an adequate level of protection'. This has seemingly been interpreted to mean that where the Commission considers that a third country retains its adequacy status, no EDPB opinion is required. An alternative reading is that the EDPB should provide an adequacy opinion not only when initial adequacy assessments are being made but also when they are under review. This latter interpretation is supported by Article 97(4) GDPR, which provides that when the Commission is conducting its evaluations and reviews, including adequacy decisions adopted pursuant to Article 45(3) GDPR and Article 25(6) of the 1995 Directive, the Commission 'shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources'. In an open letter from the Chair of the EDPB to the Justice Commissioner, the EDPB Chair hints at the Commission's failure to present its adequacy evaluations in a comprehensive and structured manner. The Chair recommends that future evaluations 'contain a detailed description of the elements of the adequacy assessment for each country and territory or at least include references to previous reports or adequacy decision where those elements are referred to'.[69] The Chair also drew to the attention of the Commission that criteria found in the adequacy referential were not mentioned consistently in all 11 evaluation reports. For instance, despite the growing significance of AI technologies for fundamental rights, the existence of equivalent 'due process' safeguards in the regimes being evaluated is not consistently assessed.[70]

While there has certainly been evidence of law reform in all concerned states during the intervening years between the adoption of the 1995 Directive era adequacy decisions and the 2024 review, the Commission's laudatory tone in its review may suggest a rosier situation than is evident. In multiple areas, gaps in protection identified by the A29WP in relation to the 1995 Directive adequacy decisions have not been resolved, yet the Commission has deemed these states adequate under the higher threshold of essential equivalence with the GDPR. For example, the lack of a specific protection of special categories of personal data under Canadian data protection law was highlighted as an area for attention, encouraging the Canadian authorities 'to work towards this goal in 2001,'[71] but the Commission's review in 2024 indicates only that there is some regulatory interpretation on the types of data considered sensitive.[72] The situation regarding special category data in New Zealand is similar,[73] despite earlier expressed concerns by the A29WP.[74] Even more concerning, there are still no

on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC SWD/2024/3 final, 15 January 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024SC0003.

[68]EDRi European Digital Rights et al. (2024) Concerns Regarding European Commission's Reconfirmation of Israel's Adequacy Status in the Recent Review of Adequacy Decisions, a letter sent on 22 April 2024. https://edri.org/wp-content/uploads/2024/04/Concerns-Regarding-European-Commissions-Reconfirmation-of-Israels-Adequacy-Status-in-the-Recent-Review-of-Adequacy-Decisions-updated-open-letter-April-2024.pdf.

[69]Letter of Anu Talus, EDPB Chair, to Michael McGrath, Commissioner for Justice, 5 December 2024. https://www.edpb.europa.eu/system/files/2024-12/edpb_letter_20241205_european-commission-review-of-11-existing-adequacy-decisions_en.pdf, p 3.

[70]The letter notes that this aspect is referred to with reference to Andorra, the Faroe Islands, Guernsey, Isle of Man, Jersey, Switzerland and Uruguay but not with reference to Argentina, Canada, Israel and New Zealand. Ibid, fn 16.

[71]A29WP, 'Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act, 26 January 2001 (WP39) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp39_en.pdf, p 4.

[72]SWD note 67, p 62.

[73]SWD note 67, p 251.

[74]A29WP, 'Opinion 11/2011 on the level of protection of personal data in New Zealand,' 4 April 2011, (WP 182) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp182_en.pdf, p 251.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

constraints on onward transfers of data from Canada other than transparency requirements,[75] while the A29WP indicated in 2001 that such transfers should not occur without some form of contractual or comparable safeguards.[76] While the Commission strikes its least encouraging tone in relation to Israeli reforms which are not yet on a statutory footing, it nevertheless concludes that Israel may be deemed adequate even without such statutory codification.[77]

Thus, it becomes apparent that the adequacy review undertaken by the Commission often falls short of the EDPB standards and, despite indicating its availability, the role of the EDPB in this review process has been reduced over time.

B. Divergence from judicial guidance

The Court of Justice has twice annulled Commission adequacy decisions for their failure to respect EU fundamental rights. While the initial *Schrems* judgment might have been a cause for surprise in some quarters, the Court's findings in *Schrems II* were aligned significantly with the direction of travel of its jurisprudence and were foreseeable in this regard. The Commission's approach to adequacy assessments nevertheless remains stubbornly out of line in some important regards with judicial authority. Three examples will be used to illustrate this point.

First, following the *Schrems* jurisprudence in particular, it was possible to adduce clear criteria from the Court's case law regarding the essential safeguards required for intelligence data processing. Amongst these safeguards are necessity and proportionality requirements. In its opinion on review of the EU–US Data Privacy Framework the EDPB observes that it would have been helpful to clarify what changes (if any) the introduction of necessity and proportionality requirements through an Executive Order in the US had for the day-to-day operations of intelligence agencies.[78] More specifically, the EDPB had previously expressed concerns about bulk access to data by intelligence agencies without prior authorization.[79] During the first review of the EU–US Data Privacy Framework, the EDPB maintained its initially raised concerns. In particular, it also noted that 'recent case law of the ECtHR further supports its standpoint, as the Court has once again emphasized the importance of independent prior authorization of surveillance measures'.[80] The implication here is clear: despite prior EDPB warnings and clear jurisprudence on prior authorization, the Commission continues to overlook this judicial authority in its adequacy decisions and appraisals.

The determination of what constitutes a data transfer provides a further example of where the Commission appears to depart from the EDPB but also judicial guidance. The notion of a 'transfer' is not defined in the GDPR, which leaves fundamental questions unanswered such as whether it constitutes a transfer to make data available via cloud storage. One question which has divided opinion is whether it constitutes a transfer when a controller makes data available to an entity in a third country that is already subject to the GDPR under its extraterritorial rules (for instance, if they offer goods or services to EU residents, or monitor their behaviour).[81] The Commission considers that in such circumstances such transfers should not be subject to Chapter V GDPR and the adequacy framework. For instance, its decision on 'standard contractual clauses' provides that SCCs may be used for

[75] SWD note 67, pp 63-64.

[76] Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act, note 71, p 6.

[77] SWD note 67, p 183: 'While the developments in terms of guidance, interpretation and case law that are described in more detail below contribute to an increased level of data protection in Israel, codifying these developments in legislation would be important to enhance legal certainty and solidify the protection for personal data. The ongoing debate on a draft bill that would amend the PPL1381 seems to offer such an opportunity.'

[78] EDPB, 'Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework,' 28 February 2023 https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en, paras 29-30.

[79] **Ibid, paras 33-34, para 36.**

[80] Ibid, para 37.

[81] GDPR, Art 3(2)(a) and (b).

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

such transfers 'only to the extent that the processing by the importer does not fall within the scope of [the GDPR]'.[82] In other words, the Commission's apparent position is that where the GDPR applies to the data recipient in a third country, no adequacy mechanism is required. Similarly, in its Privacy Shield adequacy decision, it was noted that the principles in the decision 'apply solely to the processing of personal data by the U.S. organization in as far as processing by such organizations does not fall within the scope of Union legislation'.[83] According to Kuner, the Commission has also indicated that it is 'likely to insert language in adequacy decisions mirroring that used in the SCCs, i.e. indications that an adequacy decision does not apply to transfers to a data importer whose processing of the data is directly subject to the GDPR.'[84]

However, the EDPB has adopted a much broader approach to what is deemed a transfer. It identifies three cumulative conditions for a processing operation to qualify as a transfer. These are that the data exporter (controller or processor) is subject to the GDPR for the given processing; that the exporter discloses by transmission 'or otherwise makes personal data available to another controller, joint controller or processor (the importer); and, that the importer is in a third country.[85] What is significant is that in the recent judgment of the General Court in *Bindl v Commission*, the Court repeats these conditions thereby judicially endorsing the EDPB definition of a transfer.[86] This definition is notable for its failure to exclude transfers from an exporter to an importer who is already subject to the GDPR from its scope. Moreover, this approach by the General Court is consistent with the rationale which underpins the Court of Justice's *Schrems* judgments. In *Schrems II*, in considering the necessity of effective redress for individuals in third countries, the CJEU states that such redress was particularly important because

> as is apparent from recital 116 of the GDPR, data subjects may find that the administrative and judicial authorities of the Member States have insufficient powers and means to take effective action in relation to data subjects' complaints based on allegedly unlawful processing, in that third country, of their data thus transferred, which is capable of compelling them to resort to the national authorities and courts of that third country.[87]

The same is true of data processed by data importers in third countries, regardless of a formal extraterritorial application, when beyond the territorial borders of EU Member States, enforcement actions by DPAs and judicial authorities are extremely challenging. Should the Commission continue to adhere to its more limited definition of what is deemed a transfer, it will deliberately remain out of step with the Court on this matter, to the detriment of data subjects who may be left without capacity to enforce their rights.

Finally, the first review of the UK's adequacy decisions may draw further attention to this difference in approach between the Commission and the Court and serve to illustrate the potential practical implications of their lack of alignment on the fundamental rights conditions circumscribing data transfers. On leaving the EU, the UK no longer benefitted from the presumption of a high

[82] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (SCC Decision), OJ L 199/31, recital 7.

[83] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, LJ L208/1, recital 15.

[84] C Kuner, 'Protecting EU data outside EU borders under the GDPR' [2023] 60(1) *Common Market Law Review* 77, p 93.

[85] EDPB, 'Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR,' 14 February 2023, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en.

[86] *Bindl v Commission*, T-354/22, EU:T:2025:4 paras 186-188.

[87] *Schrems II* EU:C:2020:559, para 189.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

level of data protection that adheres between EU Member States and the ensuing free flow of personal data. As a third-country, the UK was assessed and recognized as adequate by a time-limited Commission adequacy decision in 2021. While experts speculated that the legal regime concerning law enforcement and national security personal data processing in the UK might lead to a negative evaluation of the UK's adequacy status, this was not the case.[88] Following several failed attempts, the UK has introduced a reformed data protection law - the Data Use and Access Act 2025 (DUAA). The DUAA retains the underpinning logic of the GDPR, with data processing engaging a series of data controller responsibilities and data subject rights with public and private enforcement options. Yet, the Act represents a reorientation of this framework with more emphasis placed on expanding data processing while individual rights are substantially weakened. For instance, the Act introduces a new list of 'recognised legitimate interests'. These allow a controller (such as the provider of a smart home speaker or doorbell) to justify its legal processing on the basis that it is 'necessary for the purposes of protecting public security'[89] or 'apprehending or prosecuting offenders'. [90] Unlike the GDPR, which would allow such processing only where it was not outweighed by the rights and interests of the data subject, individual rights no longer feature in this assessment under the DUAA 2025. Similarly, in the GDPR the principle of purpose limitation is designed to ensure the contextual integrity of data flows – that data initially processed for one purpose will not be further processed in other incompatible ways, thereby undermining the reasonable expectations of the public about data processing. The DUAA contains a list of purposes of further processing deemed compatible, including processing necessary for protecting public security and apprehending offenders, although such processing might be entirely at odds with the original purposes of the processing. The combined effect of these provisions is that data can be originally processed by private providers without consideration of individual rights and then further processed in incompatible ways with the original purposes to serve a broad range of loosely worded interests. It is difficult to discern how such categorical classifications of legitimate interests and compatible data processing could respect the principle of proportionality which permeates the data protection framework[91] and the data protection case law of the Court of Justice.[92,93,94,95]

In addition to this data protection reform, other changes to the UK legal framework since the adoption of its GDPR and Law Enforcement adequacy decisions may still lay bare the misalignment between the Commission and the Court on appropriate levels of oversight and scrutiny when fundamental rights are at stake. In its initial opinion on UK adequacy, the EDPB had invited the Commission to assess further the independence of the entities supervising actors conducting surveillance in the UK.[96] Subsequently, the UK has amended the Investigatory Powers Act 2016 (pursuant

[88]Notably, a series of successful or partially successful challenges have been brought to the UK's surveillance laws before the European Court of Human Rights. See e.g. *Liberty v United Kingdom* (Application no. 58,243/00) (1 July 2008); *Big Brother Watch v United Kingdom* (Application nos. 58,170/13, 62,322/14 and 24,969/15) (13 September 2018); *Privacy International v United Kingdom* (Application no. 46,259/16) (4 September 2020); *Big Brother Watch and Others v United Kingdom* (Application nos 58,170/13, 62,322/14, 24,960/15) (25 May 2021).

[89]Schedule 4, Annex 1(2)(b)

[90]Schedule 4, Annex 5(b).

[91]Lee A. Bygrave, Data Privacy Law: an International Perspective (OUP 2014) 147.

[92]Lorenzo Dalla Corte, 'On Proportionality in the Data Protection Jurisprudence of the CJEU' (2022) 12 International Data Privacy Law 259

[93]The GDPR is silent as to strategic priorities which Hijmans suggests 'is the logical consequence of the complete independence as laid down in Article 8 Charter and Article 16 Treaty on the Functioning of the European Union (TFEU) and underlined in the case law of the Court of Justice of the EU (CJEU).' See H Hijmans, 'How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner? A Reaction to Christopher Hodges' (2018) 1 *European Data Protection Law Review* 80, p 80.

[94]Data (Use and Access) Bill; *Schrems* EU:C:2015:650, para 41.

[95]*Commission v Austria*, Case C-614/10, EU:C:2012:631, para 43.

[96]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,' 13 April 2021, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en p 33.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

to the Investigatory Powers (Amendment) Act 2024) in pertinent ways. Most significantly, this creates a new bulk personal dataset warrant. This new warrant is longer in duration (from 6 months to 12 months) and allows access to bulk personal datasets where there is low or no reasonable expectation of privacy based on individual authorization (by the head of intelligence or a person acting on their behalf).[97] Furthermore, there is no need for judicial authorization if urgent, or in a particular category of authorizations found in the legislation.[98] Such weak oversight would not be compatible with the requirements of independent prior judicial authorization stemming from the Court of Justice, yet it remains to be seen whether and how this jurisprudence features in the Commission's adequacy review assessment.

What then should we take from the selective approach of the Commission to the criteria set by the CJEU? Some of the implications for EU data protection law, and for EU law more broadly, shall now be considered.

IV. Implications

A. New sites of intra-EU human rights tension

A first observation that flows from the analysis above is that it reflects a new site of intra-EU human rights 'dialogue' largely overlooked in the EU human rights doctrine. Such dialogues at both the vertical and the horizontal level have been identified, as involved actors adopt divergent conceptions of human rights. A vertical dialogue generally refers to Member State to EU discussions, particularly when higher echelon domestic courts, such as national constitutional courts, challenge or dispute EU fundamental rights measures. The result of this dialogue has been the emergence of an understanding between these domestic courts and the Court of Justice. Domestic courts typically refrain from reviewing the compatibility of EU law measures with domestic fundamental rights provided that European law safeguards the essential content of those fundamental rights.[99] A well-known reflection of this settlement was the reaction of national constitutional courts to the domestic implementation of the EU's Data Retention Directive. When domestic legislation was challenged before national courts on the grounds of its incompatibility with fundamental rights, these courts did not challenge the primacy of EU law by assessing the compatibility of the EU legislation with domestic fundamental rights standards.[100] Rather, they preferred to assess the compatibility of the domestic implementing legislation with domestic fundamental rights standards thereby avoiding any tension with the Court of Justice until ultimately the question of the compatibility of the parent legislation with fundamental rights was raised before the Court of Justice in *Digital Rights Ireland*. This uneasy understanding has been unsettled following subsequent case law specifying the conditions under which law enforcement and national security agencies can mandate the targeted retention of data, provoking strong responses from national courts. This tension between uniform human rights protection across the EU and respect for the constitutional plurality of Member States, and the ensuing vertical dialogue between courts, is a long-standing theme in EU law.[101]

The Opinion states that the 'European Commission is invited to further assess the independence of the judicial commissioners, also in cases where the Commissioner is not (anymore) serving as a judge, as well as to assess the independence of the Commissioner for the Retention and Use of Biometric Material, and of the Surveillance Camera Commissioner.'

[97] **Investigatory Powers (Amendment) Act 2024, s 226A.**

[98] Ibid, s 226B.

[99] Solange II (Re Wünsche Handelsgesellschaft 1986; contra French Data Network.)

[100] See note 8 above.

[101] See, for example S Prechal and B van Roermund (eds), *The Coherence of EU Law: The Search for Unity in Divergent Concepts* (Oxford, 2008); J Masing, 'Unity and Diversity of European Fundamental Rights Protection' [2016] 4 *European Law Review* 490; M Claes, 'National Identity and the Protection of Fundamental Rights [2021] 27(3) *European Public Law* 517; F Bieber and R Bieber, *Negotiating Unity and Diversity in the European Union* (Palgrave Macmillan, 2021).

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

Since the adoption of the Charter, in particular, the CJEU reviews EU legislative acts for their compatibility with the Charter. The rights to protection of private life and to data protection have played a central role in the early development of this doctrine with the Court invalidating, first, elements of secondary legislation[102] and then an entire legislative instrument[103] on the basis of its incompatibility with these rights. In such situations, the Court essentially enters into horizontal dialogue with the legislature which must take account of the Court's specifications if it wishes to re-enact similar legislation.[104] The Court has a similar horizontal dialogue with the Council. For instance, in *Opinion 1/15* the Court was asked to assess the compatibility of a draft international agreement, the EU–Canada Passenger Name Record (PNR) agreement, with the EU Charter. Contrary to the submissions of the Commission, the Council and all intervening Member States, the Court pointed to what it considered to be a litany of shortcomings and held the agreement was incompatible with the Charter. A horizontal dialogue that is not envisaged in the doctrine, or contemplated by the Court, is the one that ensues if the Commission (consistently) does not faithfully implement the fundamental rights findings of the Court. Thus, a new—and unexpected—site for intra-EU human rights tensions emerges.

This necessarily raises questions about the Commission's ability to act as 'guardian of the treaties' in this context. Article 17 TEU sets out the Commission's role as guardian of the treaties, requiring the Commission to ensure and oversee the application of the Treaties. Under Article 16 TFEU, there is a clear mandate to ensure the fundamental right to data protection. The Treaties grant the Commission significant powers to enable it to fulfil its role. In spite of these powers, the Commission has in recent times been accused by some of 'enforcement paralysis' in the area of data protection law.[105] Challenges are not only observed in the field of data protection. Air pollution is just one of the many other cases that illustrate the EU's 'compliance deficit.'[106]

Some scholars have begun to consider the role of NGOs as supplementary guardians of the treaties where the EU relies less on Commission initiated infringement procedures,[107] and there has been significant discussion on the role of collective actors and strategic litigation as 'guardians of digital rights', including data protection.[108] In other contexts, such as the rule of law crisis, it is suggested that

[102] *Volker und Markus Schecke and Eifert*, C-92/09, [2010] I-11,063.

[103] *Digital Rights Ireland and Seitlinger and Others*, EU:C:2014:238.

[104] In this way, this horizontal dialogue mirrors earlier back and forth between the Court and EU legislature in relation to legislative competence. e.g. *Germany v Parliament and Council*, Case C-376/98, [2000] ECR I-8419. See S Weatherill, 'The Limits of Legislative Harmonization Ten Years after Tobacco Advertising: How the Court's Case Law has become a 'Drafting Guide' (2011) 12(3) *German Law Journal* 827.

[105] J Ryan, 'Europe's Enforcement Paralysis: ICCL's 2021 GDPR Report', *Irish Council for Civil Liberties*, 13 September 2021 <https://www.iccl.ie/news/2021-gdpr-report/>; J Ryan, 'ICCL Launches European Ombudsman Complaint against European Commission's Failure to Take Ireland to Court over the GDPR', *Irish Council for Civil Liberties*, 29 November 2021 <https://www.iccl.ie/news/iccl-launches-european-ombudsman-complaint-against-european-commissions-failure-to-take-ireland-to-court-over-the-gdpr/>

[106] K Reiners and E Versluis, 'NGOs as New Guardians of the Treaties? Analysing the Effectiveness of NGOs as Decentralised Enforcers of EU Law' (2023) 30 *Journal of European Public Policy* 1518, p 1518.

[107] Ibid, p 1532.

[108] V Golunova and S Tas, 'Guardians of Digital Rights: Exploring Strategic Litigation on Data Protection and Content Moderation in the EU' (2024) 7 *Nordic Journal of European Law* 49; O Lynskey, 'The Role of Collective Actors in the Enforcement of the Right to Data Protection under EU Law' in E Muir et al (eds), *How EU Law Shapes Opportunities for Preliminary References on Fundamental Rights: Discrimination, Data Protection and Asylum* (EUI Working Papers 2017/17) <https://cadmus.eui.eu/bitstream/handle/1814/49324/LAW_2017_17.pdf?sequence=3&isAllowed=y>; W Jang and AL Newman, 'Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation' (2022) 60(2) *Journal of Common Market Studies* 283; I Mizarhi-Borohovich, A Newman and I Sivan-Sevilla, 'The Civic Transformation of Data Privacy Implementation in Europe' (2023) 47(3) *West European Politics* 671. See, among others, L Vanhala, 'Anti-Discrimination Policy Actors and Their Use of Litigation Strategies: The Influence of Identity Politics' (2009) 16(5) *Journal of European Public Policy* 738; J Peel and R Markey-Towler, 'Recipe for Success?: Lessons for Strategic Climate Litigation from the Sharma, Neubauer, and Shell Cases' (2021) 22(8) *German Law Journal* 1484; A Pijnenburg and K van der Pas, 'Strategic Litigation against European Migration Control Policies: The Legal Battleground of the Central Mediterranean Migration Route' (2022) 24(3) *European Journal of Migration and Law* 401.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

the Court of Justice has had to step into the role in order to defend EU values[109] and has 'confirmed its position as a guardian of the 'constitutionality' of EU acts.[110]

While the rule of law crisis and the upholding of data protection law differ in political implications and complexity, there are some parallel concerns about the Commission's willingness or capacity to act as the primary guardian of the treaties. It has been argued that non-enforcement became a deliberate policy of the Commission in an effort to avoid conflict with Member States in the rule of law context.[111] While the political stakes in data protection decisions may not match the existential concerns raised by the rule of law crisis, the Commission approach to adequacy, strongly influenced by economic and diplomatic considerations, reflects the EU's trade-oriented foundations. Czerniawski argues that the Commission cannot be considered an 'independent assessor' of adequacy 'as it is interested in a particular outcome of the procedure' and may be 'politically motivated in its actions'.[112] We shall turn to this now.

B. A political approach to human rights?

While the Commission's adequacy decisions are legal appraisals of the protection offered to individuals by third country law in the context of personal data transfers, it is difficult to disentangle them from the economic and political context in which they sit.

One might, for instance, infer from the sequence of the steps taken to adopt an adequacy decision that adequacy is initially a political decision, with expert input and the legal means of achieving adequacy being hammered out at a later stage. This is consistent with the process by which the Commission initiates adequacy decisions. Some of the adequacy opinions of the A29WP are more forthright in disclosing details of how adequacy dialogue was initiated. For instance, for Andorra,[113] Argentina,[114] Israel,[115] and Uruguay[116] the adequacy opinions state that the request came from the relevant ambassador/mission to the EU. Under the GDPR, the logistics of how and when adequacy

[109]Scheppele has argued that the Court of Justice has been 'in practice the primary Guardian of the Treaties on duty for the last decade.' KL Scheppele, 'The Treaties Without a Guardian: The European Commission and the Rule of Law' (2023) 29 *Columbia Journal of European Law* 159; L Pech and D Kochenov, 'Respect for the Rule of Law in the Case Law of the European Court of Justice: A Casebook Overview of Key Judgments Since the Portuguese Judges Case', *SIEPS*, September 2021; M Mandujano Manriquez and T Pavone, 'Follow the Leader: The European Commission, the European Court of Justice, and the EU's Rule of Law Revolution' (2025) 32 *Journal of European Public Policy* 444; D Kochenov and P Bárd, 'The Last Soldier Standing? Courts Versus Politicians and the Rule of Law Crisis in the New Member States of the EU', *European Yearbook of Constitutional Law 2019* (TMC Asser Press, 2020).

[110]E Muir, 'The Court of Justice: A Fundamental Rights Institution among Others within the EU Legal Order' in M Dawson, B de Witte and E Muir (eds), *Revisiting Judicial Politics in the European Union* (Edward Elgar, 2024) p 121.

[111]KL Scheppele, 'The Treaties without a Guardian: The European Commission and the Rule of Law' (2023) 29 *Columbia Journal of European Law* 98; R Kelemen and T Pavone, 'Where Have the Guardians Gone? Law Enforcement and the Politics of Supranational Forbearance in the European Union' (2023) 75 *World Politics* 779.

[112]Czerniawski, note 47, p 220.

[113]'On 21 May 2008 the Ambassador of Andorra to the European Union requested the Commission to handle the procedure for the declaration of Andorra as a country that offers an adequate level of protection within the meaning of article 25(6) of Directive 95/46/EC, on Personal Data Protection.' A29WP, 'Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra,' 1 December 2009, (WP 166), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp166_en.pdf p 2.

[114]The Opinion refers to a request via letter by the Ambassador of the Republic of Argentina before the European Union of 23 January 2002. A29WP, 'Opinion 4/2002 on the level of protection of personal data in Argentina,' 3 October 2002, (WP 63), p 2.

[115]'On 12 July 2007, the Israeli Mission to the European Union requested the Commission to
launch the procedure to declare Israel as a country that ensures an adequate level of protection
for the purposes provided for in Articles 25 and 26 of the Directive.' A29WP, Opinion 6/2009 on the level of protection of personal data in Israel, WP 165, 1 December 2009, p 2.

[116]A29WP, Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay, WP 177, 12 October 2010, p 2.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

procedures are initiated are not explicitly defined. While the EU–US Data Privacy Framework decision explicitly notes that the Commission entered into talks with the US government following the *Schrems II* judgment, existing adequacy decisions do not consistently disclose the details of how they were initiated.[117]

In 2017, the Commission published a communication clarifying its approach to data transfers, including adequacy.[118] It sets out four criteria, which should be taken into account when determining whether adequacy dialogue should be pursued. These include factors specific to data protection ('the pioneering role' of the country in privacy and data protection and whether it could serve as a model for other countries in the region, as well as the extent of data flows from the EU to the country). However, they also include economic considerations (the extent of the EU's actual or potential commercial relations, including existing trade agreements or ongoing negotiations) and political considerations ('the overall political relationship' with the third country in question). The latter confirms that the Commission views adequacy as part of its legal arsenal in navigating relations with non-EU states and entities. Kuner and Zanfir-Fortuna characterize this communication as the Commission admitting to the influence of political and economic factors in its approach to data flows.[119]

Similar conclusions might be drawn from some more recent Commission documents. For instance, in its report on the first review of adequacy decisions, it noted that:

> …rather than being an 'end point' adequacy decisions have laid the foundation for closer cooperation and further regulatory convergence between EU and like-minded partners. By enabling the free flow of personal data, these decisions have opened up commercial channels for EU operators, including by complementing and amplifying the benefits of trade agreements, as well as eased cooperation with foreign partners in a broad range of regulatory fields.[120]

It is difficult to glean from such statements whether adequacy decisions are simply viewed as having positive externalities for trade and international cooperation or whether they are being pursued in order to further these aims. Speaking extra judicially after *Schrems II*, the President of the CJEU has been more forthright. He has stated that 'the rule of law is not up for sale' and that if upholding rule of law requirements 'is also affecting some dealings internationally, why would Europe not be proud to contribute its requiring standards of respect for fundamental rights to the world in general?'.[121]

Furthermore, there is no reason to believe that the disagreement between the Commission and other EU actors regarding data protection standards is reduced to the area of international data transfers. For example, in the Commission's second report on the application of the GDPR, there are a number of (polite) rebukes to the EDPB. The Commission notes that:

> In the 2020 report the Commission called on the Board to adopt guidelines on scientific research, but the guidelines have not yet been adopted. Recognising the importance of scientific research in society, in particular to monitor diseases and develop treatments, and to foster

[117]Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ L231/118, Recital 6.

[118]Commission, Communication from the Commission to the European Parliament and the Council, 'Exchanging and Protecting Personal Data in a Globalised World' COM [2017] 7 final.

[119]C Kuner and G Zanfir-Fortuna, 'Geopolitical Fragmentation, the AI Race, and Global Data Flows: The New Reality', *Future of Privacy Forum*, 26 February 2025 <https://fpf.org/blog/geopolitical-fragmentation-the-ai-race-and-global-data-flows-the-new-reality/>.

[120]Commission, Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC COM/2024/7 final, 15 January 2024, p 2 and 3, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024DC0007.

[121] V Pop, 'ECJ President On EU Integration, Public Opinion, Safe Harbor, Antitrust', *Wall Street Journal*, (14 October 2015) <http://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/>

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

> innovation, it is essential that data protection authorities act to clarify these questions without further delay.[122]

Regarding the priorities of the EDPB and DPAs, reflecting on stakeholder concerns about the development of the digital economy and media freedom, the Commission recalls that DPAs and the Board are

> tasked with ensuring both the protection of natural persons in relation to the processing of their personal data and the free flow of personal data within the EU. As recognized in the GDPR, the right to protection of personal data must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.[123]

The EU uses external trade policy to extract human rights commitments from its trade partners.[124] One might query then whether there is any difference in principle between such conditionality measures and the geo-political dimension of adequacy decisions. Two distinctions are immediately apparent. The first is that the CJEU sees adequacy decisions only from the human rights perspective and holds the Commission to a strict standard of review as a result. The second is that human rights conditionality in trade relations is used to ratchet up the level of human rights protection offered by third countries[125] rather than to accept lower levels of human rights protection for EU residents to secure economic benefits for the EU. The prioritization of trade and economic imperatives over human rights resonates with the criticism of the EU that it has pursued neoliberal ideals under the cover of other stated values.[126]

C. Standards of review at the CJEU

The Court when reviewing the adequacy decisions in *Schrems I* and *II* declared that the Commission's discretion would be limited, while the standard of review it adopted would be strict. It made a similar finding when reviewing the Data Retention Directive in *Digital Rights Ireland*. The Court justified this strict standard of review in *Digital Rights Ireland* as follows:

> in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that the review of that discretion should be strict. [127]

The Court had performed a similarly strict review in *Kadi II*.[128] This strict standard of review can be contrasted with instances, such as when reviewing competition law decisions, when the Commission is afforded a wide margin of appreciation as it makes complex economic and social appraisals.

[122] Commission, Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, Brussels 25.7.2024, COM(2024) 357 final p 6.

[123] Ibid, p 9.

[124] I Govaere, 'Promoting the Rule of Law in EU External Relations: A Conceptual Framework', *College of Europe—Department of European Legal Studies Research Paper in Law*, 03/2022, p 6.

[125] The legitimacy of such behaviour has been challenged for its influence on the internal affairs of non-EU states. For instance, ME Odijie, 'Unintentional Neo-colonialism? Three Generations of Trade and Development Relationship Between EU and West Africa' (2022) 44(3) Journal of European Integration 347.

[126] See, for instance, M Wilkinson, *Authoritarian Liberalism and the Transformation of Modern Europe* (2021, Oxford University Press) or, earlier, C Hermann, 'Neoliberalism in the European Union' (2007) 79(1) *Studies in Political Economy* 61.

[127] *Digital Rights Ireland and Seitlinger and Others*, EU:C:2014:238, para 48.

[128] *Commission and Others v Kadi*, Joined cases C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

In the aftermath of the *Schrems* judgments, commentators (particularly those outside of the EU) queried whether the Court had played an overly interventionist role in reviewing the adequacy decisions. As Baquero Cruz highlights, rather than debating whether a court has been 'activist' or not, it is more fruitful to assess the impact of judicial review on other institutions 'which have their own legitimacy and expertise, on the distribution of power among levels of government, on participation and representation'.[129] As the human rights mandate of the Court of Justice has been strengthened by the Charter, it now interacts more intensely with these other stakeholders.[130]

The Court has, to date, largely been spared from allegations of 'juristocracy' when it comes to its fundamental rights jurisprudence.[131] The central tenet of such allegations is that the meaning of contestable rights is determined by courts rather than by democratically elected legislatures. As Craig notes, this counter-majoritarian perspective may have been largely absent in the EU so far because the democratic credentials of the legislature itself were relatively limited.[132] However, this suggests that as the democratic legitimacy of the legislature has been enhanced, and the legislature takes on a more active role expounding the meaning and limits of fundamental rights, we might expect this counter-majoritarian perspective to become more visible.

Muir suggests that a key challenge facing the Court of Justice in this new human rights landscape will be to recalibrate its relations with relevant actors. In such an environment, the Court might be more attentive to the democratic imprimatur of legislative instruments and therefore exercise a lighter touch review of their compatibility with human rights. However, acts of the Commission have no such democratic legitimacy. Indeed, as Dawson observes:

> …the Court of Justice in *Schrems* invalidated a political decision of the EU institutions, but one adopted by a body (the Commission) with weak political accountability and limited responsiveness to EU citizens. In this decision-making process, neither of the Union's legislative institutions was present (with one, the European Parliament, being critical of the Commission's action).[133]

It could be argued that the *ex ante* role of the Article 93 Committee through the comitology procedure lends democratic legitimacy to the Commission's adequacy decisions. While the Commission publishes documents relating to this Committee on its comitology transparency register, the information published is extremely limited. For instance, the EU–US Data Privacy Framework was subject to a written procedure which culminating in a vote with the relevant document simply indicating the number of states in favour and against the EU–US Data Privacy Framework and the number of residents they represent.[134] More significantly, the Commission exercises a significant influence throughout the Article 93 process: by 'chairing the meetings, setting the timeframe for the committees' activities and preparing agendas for the meetings' while it also determines the text put before the Committee to vote.[135] The Commission thus dominates the early phases of adequacy, determining who to enter into adequacy negotiations with and on what grounds and by drafting the adequacy decision to be put before the Article 93 Committee while still exercising influence over this final

[129] B Cruz, 'Unstable Structures: The Institutional Balance and the European Court of Justice' in M Dawson, B de Witte and Elise Muir (eds), *Revisiting Judicial Politics in the European Union* (Edward Elgar, 2024) 142, p 144.

[130] Muir, n 110 above, p 122.

[131] See, M Loughlin, *Against Constitutionalism* (2022, Harvard University Press), pp. 124-135.

[132] P Craig, 'Democracy' in R Masterman and R Schütze (eds), *The Cambridge Companion to Comparative Constitutional Law. Cambridge Companions to Law* (Cambridge University Press, 2019) 201, p 225.

[133] M Dawson, 'The Governance of EU Fundamental Rights' (Cambridge University Press, 2017), p 81.

[134] Formal results of voting on Revised draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, Document D091003/01, https://ec.europa.eu/transparency/comitology-register/screen/documents/091061/1/consult?lang=en

[135] Czerniawski, note 47 above, 224.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

phase. Thus, while a valid debate may emerge in the coming years over the appropriate standard of review for the Court to adopt when assessing the compatibility with the Charter of EU legislative instruments, this debate lacks the same credibility when it comes to review of the adequacy decisions of the EU Commission.

V. Conclusions

It is a pivotal moment for the EU and for EU digital regulation. The GDPR forms a cornerstone of a broader suite of digital regulation which places safeguards in place to constrain the economic and social power of digital technology operators with the aim of preserving fundamental rights in the EU.[136] The ultimate aim of these regulatory measures is to protect European democracy and the rule of law.[137] Yet, abrupt geo-political changes are likely to render more visible the underlying tensions between trade, politics and human rights in EU digital regulation. In such a context, it becomes even more important to remain attentive to the distribution of powers amongst democratic institutions.

While the story of international data transfers is often presented primarily as a clash between rival states or regions, this article engages in a close inspection of the process behind the adoption of adequacy decisions to tell a different story.[138] What this close inspection reveals is that the Commission has assumed an increasingly powerful role when it comes to the adoption of adequacy decisions. Czerniawksi suggests that, while in principle Member States exercise *ex ante* control over such adequacy decisions through a comitology committee, in reality the Commission retains an upper hand in this process.[139] Our analysis demonstrates that the expert input of DPAs through the EDPB is increasingly marginalized in the adequacy process with the Commission exercising commensurately more power. Independent DPAs who are unsatisfied with this outcome from the perspective of fundamental rights may, per *Schrems*, manufacture a route to judicial review of Commission adequacy decisions by the Court of Justice. Given the weak democratic legitimacy of the Commission's adequacy decisions, the Court appropriately applies a strict standard of review when assessing the compatibility of such acts with the Charter. Nevertheless, there remains in practice a divergence between the fundamental rights standards set by the Court and the Commission's decisional practice when it comes to adequacy.

These empirical observations have consequences for EU law beyond data protection. These insights from GDPR adequacy also cast a spotlight on the increasingly complex human rights landscape that the Court of Justice must navigate. As Muir notes, the Court's stronger mandate on fundamental rights meets with that of other key players and 'it now interacts more intensely than before with domestic constitutional courts, the EU legislator, and the European Court of Human Rights'.[140] To this list, we must now add the European Commission.

What emerges from our analysis is an under-examined site of intra-EU tension concerning fundamental rights, between the Commission and the Court. This is significant for two reasons. First, it requires us to consider who watches the watchdog, or how the Commission can be held to account in its role as 'guardian of the treaties'. Second, it calls into question the effectiveness (and wisdom) of centralizing enforcement power in the Commission for violations of digital rights instruments that navigate similar geo-political tensions (including the Digital Markets Act and the Digital Services Act). It is not a foregone conclusion that the EU will remain a rights-centric digital power without appropriate and effective intra-institutional checks on power.

[136] Bradford, note 1 above, chapter 3.

[137] Husovec, for instance, examines the EU's Digital Services Act as 'part of a bigger struggle to defend the liberal democracy'. See, Tech Policy Press, 'Unpacking the Principles of the Digital Services Act with Martin Husovec', 27 October 2024, https://www.techpolicy.press/unpacking-the-principles-of-the-digital-services-act-with-martin-husovec/.

[138] Bradford, note 1 above, pp 231-236.

[139] See Czerniawksi, note 47.

[140] Muir, note 110 above, p 122.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

VI. Annex: methodology

In order to conduct an analysis of the adequacy decisional practice of the European Commission, a corpus of relevant documents was assembled and subjected to a comparative analysis. The initial corpus comprised of all adequacy decisions adopted by the European Commission to date under the Data Protection Directive or GDPR (18 decisions), and the corresponding opinions adopted by the A29WP or EDPB. The only adequacy decision adopted to date under the Law Enforcement Directive was excluded due to its outlier status. Documents were sourced from the archive of the Article 29 Working Party documents, the EDPB's documents, and the Commission's own website. These documents are listed and cited in Table 1:

Table 1. Corpus of documents

Country	Commission decision	A29WP or EDPB Opinion
Andorra	Commission Decision 2010/625/EU	Opinion 7/2009
Argentina	Commission Decision 2003/490/EC	Opinion 4/2002
Canada	Commission Decision 2002/2/EC	Opinion 2/2001
Faro	Commission Decision 2010/146/EC	Opinion 9/2007
Guernsey	Commission Decision 2003/821/EC	Opinion 5/2003
Hungary	Commission Decision 2000/519/EC	Opinion 6/99
Isle of Man	Commission Decision 2004/411/EC	Opinion 6/2003
Israel	Commission Decision 2011/61/EU	Opinion 6/2009
Japan	Commission Implementing Decision 2019/219/EU	Opinion 28/2018
Jersey	Commission Decision 2008/393/EC	Opinion 8/2007
Korea	Commission Implementing Decision 2022/254/EU	Opinion 32/2021
New Zealand	Commission Decision 2013/65/EU	Opinion 11/2011
Switzerland	Commission Decision 2000/518/EC	Opinion 5/99
United Kingdom (GDPR)	Commission Implementing Decision 2021/1772/ EU	Opinion 15/2021
United States (Safe Harbour)	Commission Decision 2000/520/EC	Opinion 2/99
United States (Privacy Shield)	Commission Implementing Decision 2016/125/EU	Opinion 01/2016
United States (Data Privacy Framework)	Commission Implementing Decision 2023/4745/EU	Opinion 5/2023
Uruguay	Commission Implementing Decision 2012/484/EU	Opinion 6/2010

The comparative review was deductive, based on iterative engagement with the corpus, read together with the adequacy referentials and in light of the underlying doctrinal framework. Once the typical form of the adequacy decisions became familiar, a series of parameters were developed to draw comparison. As the difference of form between the pre and post *Schrems* era adequacy decisions became apparent, additional points of comparison were identified. A database was assembled extracting and organising key aspects of the decisions according to the criteria set out in Table 2 below.

https://doi.org/10.1017/cel.2025.10018 Published online by Cambridge University Press

Table 2. Comparison criteria

	Adequacy decision	A29WP/EDPB Opinion
Formal dimensions	• Status • Date • Expiration • Scope of adequacy determination • Adequacy standard applied • Statement of adequacy	• Date
Substantive analysis	• Constitutional law protections • National law standards • International law protections • Exceptions/exclusions • Onward transfers	
Procedural dimensions	• National supervisory authorities • Independence of national supervisory authorities • Enforcement by supervisory authorities • Redress	
National security/LE access to data	• National supervisory access • Law enforcement access	
Process of negotiation/adoption	• Negotiation/adoption process • Law reform pursuant to negotiation/adoption	

These points of comparison were used to understand trends, changes, and differences in the practices associated with the adoption of adequacy decisions, the content of such decisions and the gaps between A29WP/EDPB opinions and Commission assessments.

This comparison formed the core of our empirical investigation, and later as the Commission's review reports and the EDPB's responses to those reports were released, these reports were reviewed to observe continued practices, particularly by tracking persistently raised issues through the jurisdictional appraisal.

Competing interest declaration. The qualitative analysis described in this article was originally conducted in association with a report by the authors, which was commissioned by the Department for the Economy of Northern Ireland. The full report is available at: https://www.economy-ni.gov.uk/sites/default/files/publications/economy/Understanding-the-risks-to-cross-border-transfer-of-personal-data-EU-UK-data-adequacy.pdf

Between 2014 and 2017, Katherine Nolan worked on aspects of the *Schrems II* litigation while employed at an Irish law firm. All contributions by Dr Nolan to this article are in her personal capacity and rely only on information available in the public domain.

Cite this article: O Lynskey, MH Murphy and K Nolan, 'Digital Empire or Digital Fiefdoms? Institutional Tensions and the EU Right to Data Protection' (2025) *Cambridge Yearbook of European Legal Studies* pp. 1–22. https://doi.org/10.1017/cel.2025.10018