British Institute of International and Comparative Law

DEFICIENT BY DESIGN? THE TRANSNATIONAL ENFORCEMENT OF THE GDPR

GIULIA GENTILE AND ORLA LYNSKEY*

Abstract Four years following the entry into force of the EU data protection framework (the GDPR) serious questions remain regarding its enforcement, particularly in transnational contexts. While this transnational under-enforcement is often attributed to the role of key national authorities in the GDPR's procedures, this article identifies more systemic flaws. It examines whether the GDPR procedures are deficient-by-design and, if not, how these flaws might be addressed. The conclusions reached inform our understanding of how to secure effective protection of the EU Charter right to data protection. They are also of significance to EU law enforcement more generally given the increasing prevalence of composite decision-making as the mechanism of choice to administer EU law.

Keywords: human rights, data protection, enforcement, composite procedures, administrative law.

I. INTRODUCTION

The EU data protection rules are often touted as the most comprehensive and stringent in the world. Yet their enforcement offers a different, darker side of the EU data protection story, with suboptimal enforcement leading to a disconnect between the law on the books and its impact in practice. Such suboptimal enforcement was already evident under the 1995 Data Protection Directive (the 1995 Directive),[1] which preceded the General Data Protection Regulation (GDPR).[2] The GDPR was designed to remedy these enforcement deficiencies by bolstering public administrative enforcement and, in so doing,

* Fellow in Law, LSE, G.Gentile1@lse.ac.uk; Associate Professor, LSE, O.Lynskey@lse.ac.uk. Both authors contributed equally to this work and the order of author names is merely alphabetical.

[1] Directive (EC) 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/23. COM(2012)11; Commission, '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 final (Commission GDPR Proposal), at 4.

[2] Regulation (EU) 2016/679 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 L119/1.

[*ICLQ* vol 71, October 2022 pp 799–830] doi:10.1017/S0020589322000355

rendering the application of EU data protection more consistent and effective for EU residents.[3]

However, four years following the entry into force of the GDPR, serious questions remain regarding the functioning of this new regime. The focus of this article is on public enforcement in transnational proceedings. In this context, responsibility for the GDPR's under-enforcement is often laid squarely at the doors of some key domestic data protection authorities.[4] Scholars observe that 'data protection hawks and doves' have emerged threatening the coherent and uniform application of the law.[5] In this article, it is argued that the role played by these regulatory doves is a symptom of broader inadequacies of the GDPR enforcement framework, as well as a cause. While the national supervisory authorities (NSAs) charged with enforcing the GDPR could certainly do more to facilitate effective transnational enforcement, the GDPR's shortcomings also stem, in part, from the very design of the composite decision-making procedures it necessitates and are further exacerbated by the influence of national strategies in shaping its enforcement.

More specifically, the article identifies four flaws in the GDPR's transnational enforcement system. First, the composite administrative procedures provided for by the GDPR lead to ambiguities and divergences in the oversight and enforcement procedures applicable to complaints. This reveals an important tension between the procedural autonomy of national administrative bodies and the need to ensure the consistent and effective enforcement of the rulebook across the EU. Secondly, the GDPR fails to recognise the equality of NSAs, by giving an outsized role to—or placing an outsized burden on—the so-called 'lead supervisory authority' at the expense of other NSAs. Thirdly, the system presents evident weaknesses from a procedural fairness standpoint which translate into constraints on important procedural rights, such as the right to an effective remedy of data subjects. Fourthly, the divergences persisting in national approaches towards the enforcement of EU data protection law engender potential breaches of a central tenet of the rule of law, the equal application of the law.

[3] The Commission summarised the relevant GDPR changes as follows: '[The GDPR] equips the independent data protection authorities with stronger and harmonised enforcement powers and sets up a new governance system.' Commission, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation' (Communication) COM(2020)264 at 1.

[4] For instance, 2020/2789(RSP), 'European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 – *Data Protection Commissioner* v *Facebook Ireland Limited and Maximillian Schrems* ('Schrems II'), Case C-311/18'. The Parliament criticised the Irish Data Protection Commission (DPC), expressing 'deep concern that several complaints against breaches of the GDPR filed on 25 May 2018, the day the GDPR became applicable, and other complaints from privacy organisations and consumer groups, have not yet been decided by the DPC, which is the lead authority for these cases'.

[5] T Streinz, 'The Evolution of European Data Law' in P Craig and G de Búrca (eds), *The Evolution of EU Law* (3rd edn, OUP 2021) 902, 914.

These flaws contribute to the under-enforcement of the data protection framework and ultimately stymie the GDPR's ambition to enhance fundamental rights protection. The article outlines how these deficiencies might be addressed. The conclusions reached inform our understanding of how to secure the effective protection of data protection and other related EU Charter rights. However, this analysis is also of relevance to the study of EU administrative law, given the increasing prevalence of composite decision-making as the mechanism of choice to administer EU law. Data protection represents an under-examined yet significant example of such composite decision-making: GDPR procedures combine both horizontal composite procedures involving domestic administrative organs, and vertical composite procedures requiring cooperation between national and EU administrative organs. This analysis provides a further example of the challenges and gaps arising from composite administrative procedures in the EU legal landscape.

The article proceeds as follows. Section II outlines the main changes to the administrative enforcement of EU data protection law introduced by the GDPR: the cooperation and consistency mechanisms. Section III identifies four important flaws stemming from the design and the enforcement of these new oversight and enforcement mechanisms that hinder their practical effectiveness. Section IV briefly considers how these flaws might be remedied. It queries whether they might be tackled from within—by adapting the interpretation or application of existing GDPR procedures—and, if not, what alternative options exist. Finally, it offers some reflections on the relevance of these findings for the public enforcement of the GDPR and for the administrative enforcement of EU law more generally.

II. COMPOSITE ADMINISTRATIVE PROCEDURES UNDER THE GDPR: THE CONSISTENCY AND COOPERATION MECHANISMS

Prior to the enactment of the GDPR the 1995 Directive contained no strict rules for coordination between NSAs for data processing operations of transnational importance. Several NSAs could therefore concurrently claim competence to investigate and sanction the same data processing conduct.[6] In the absence of binding rules on cooperation, each NSA could apply its own rules and standards, thus avoiding the need to reach compromise that might entail a 'lowest common denominator' approach to the application of the Directive. However, such regulatory competition incentivised forum shopping by data controllers and detracted from the legitimacy of the rules because of their differentiated interpretation and application domestically. This, in turn, ultimately led to different levels of fundamental rights protection for European residents, depending on their place of residence. Although the

[6] See further, O Lynskey, 'The "Europeanisation" of Data Protection Law' (2017) CYELS 252, 255–72.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

NSAs devised an ad hoc mechanism to coordinate their activities under the aegis of the Article 29 Working Party, the Directive proved insufficient to ensure the effective application of the rules.[7] Hence, reforms of the EU data protection framework had to tackle not only the issue of under-enforcement but also the disparate levels of fundamental rights protection offered across the EU. The enforcement of the EU data protection rules at different speeds and to different degrees of intensity is problematic not only in the light of Article 8 EU Charter and Article 16 TFEU,[8] which protect the right to data protection, but also Article 21 EU Charter and Article 18 TFEU, which prohibit discrimination on the ground of nationality. It was further argued that the plurality of national administrative practices under the Data Protection Directive would jeopardise the 'entire *effet utile* of the Union regulatory framework' in a manner incompatible with the EU Charter.[9]

Accordingly, the 'name of the game' of the GDPR was the need to ensure consistent and effective transnational enforcement.[10] The GDPR introduced procedural mechanisms to streamline the cooperation among NSAs: the cooperation and consistency procedures.[11] These mechanisms have two peculiar features: first, they rely both on EU and national procedural law; secondly, they demand that NSAs act as both national and European agents. Mechanisms bearing these characteristics have been classified as 'composite administrative procedures'. According to Brito Bastos, 'what characterises composite administrative procedures is that the final decisions adopted pursuant to them require a cumulative exercise of decisional competences at procedural stages at national and then EU levels'.[12] Hofmann uses the terminology 'diagonal multi-jurisdictional composite procedure' to describe instances where there is horizontal and vertical cooperation among EU and national authorities.[13]

[7] See, for instance, the ad hoc cooperation to investigate changes into Google's privacy policy. C Watson, 'Google Has a Fight on Its Hands as it Faces CNIL's Challenge to Its Privacy Policy' (16 October 2012) <https://www.mondaq.com/uk/privacy-protection/201862/google-has-a-fight-on-its-hands-as-it-faces-cnils-challenge-to-its-privacy-policy>.

[8] The Commission's proposal for the GDPR notes that the right to data protection 'requires the same level of data protection throughout the Union' (para 3.2), Commission GDPR Proposal (n 1).

[9] J Zemánek, 'Case C-518/07, European Commission v. Federal Republic of Germany, Judgment of the Court of Justice (Grand Chamber) of 9 March 2010 ECR I-1885' (2012) CMLRev 1755, 1766.

[10] Case C-645/19, *Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit*, EU:C:2021:5, Opinion of AG Bobek, para 76.

[11] The rapporteur views the foreseen cooperation and consistency mechanism among national DPAs as a huge step towards a coherent application of data protection legislation across the EU. Explanatory Statement, European Parliament, A7-0402/2013 of 22 November 2013.

[12] F Brito Bastos, 'An Administrative Crack in the EU's Rule of Law: Composite Decision-making and Nonjusticiable National Law' (2020) EuConst 63, 66. For a general analysis of composite administrative procedures, see M Eliantonio and N Vogiatzis 'Judicial and Extra-Judicial Challenges in the EU Multi- and Cross-Level Administrative Framework' (2021) 22 German Law Journal 690.

[13] H Hofmann, 'Multi-Jurisdictional Composite Rrocedures: The Backbone to the EU's Single Regulatory Space' (2019) Law Working Paper Series, n. 3/2019, 18.

On paper, mechanisms of this nature appear to capture the complexity of the EU legal order, which relies on a plurality of actors pertaining to different levels of governance. In a way, composite administrative procedures are an expression of the procedural and administrative pluralism existing in the EU.[14] Recourse to these procedures in the field of data protection appears fitting prima facie: the EU data protection framework was traditionally driven by national administrative authorities, which made the system intrinsically pluralistic although governed by EU law. Under the GDPR, these procedures foster cooperation and thus enhance the European dimension of the GDPR's enforcement in transnational settings.

Yet, as will be discussed, these mechanisms are not exempt from hurdles and complications. As existing literature demonstrates, the problems stemming from horizontal and vertical composite administrative procedures for judicial accountability and the protection of individual rights are exacerbated in a diagonal context.[15] Hofmann rightly points out that these procedures reflect 'a lack of awareness of requirements of protection of individual rights and supervisory necessities' on the legislature's part.[16] It is useful to bear this in mind when discussing the pitfalls of GDPR enforcement. Before embarking on this discussion, the functioning of the cooperation and consistency mechanisms will be considered.

A. The Interdependence of NSAs: The Cooperation Mechanism

Independent NSAs, the mainstay of EU data protection enforcement since the 1995 Directive, remain the primary actors responsible for oversight and enforcement under the GDPR.[17] Like the Directive, the GDPR stresses that the independence of NSAs is an 'essential component' of the protection of individuals in the context of personal data processing.[18] Yet such independence has been enriched by interdependence through the main institutional innovation of the GDPR, the 'one-stop-shop' (OSS) mechanism.[19] This procedure applies in cases of cross-border processing[20]

[14] D Halberstam, 'Understanding National Remedies and the Principle of National Procedural Autonomy: A Constitutional Approach' (2021) CYELS, 128, 141.

[15] Hofmann (n 13) 23.

[16] ibid.

[17] Chapter VI GDPR is dedicated to independent supervisory authorities. Art 51(1) confirms that the overarching role of these NSAs is to monitor the application of the legal framework to promote the objectives of the GDPR.

[18] Recital 62, 1995 Directive (n 1); recital 117, GDPR. The importance of the independence of regulatory authorities has been emphasised in all areas of EU law. The centrality of this independence has, for instance, been emphasised in the energy sector: see A Johnston and G Block, *EU Energy Law* (OUP 2012) 125–43 and, more recently, K Huhta, 'C-718/18 Commission v. Germany: Critical Reflections on the Independence of National Regulatory Authorities in EU Energy Law' (2021) 30(6) EEELR 255.

[19] Art 60 GDPR; recitals 127 and 128 GDPR.

[20] According to Art 4(23) GDPR, cross-border processing exists where the data controller or processor has more than one relevant establishment in the EU for GDPR purposes or where there

and entails an obligation on the NSAs to engage in horizontal cooperation. This mechanism is thus an exception to the general competence of each NSA to conduct its tasks and exercise oversight, investigative and sanctioning powers on the territory of its Member State.[21]

Article 60 GDPR regulates the terms of the cooperation among NSAs under the OSS. The linchpin in this system is the idea of a 'lead supervisory authority' (LSA). The LSA is the supervisory authority of the place of main establishment for data protection purposes of the controller or processor,[22] which will be tasked with the supervision of GDPR cross-border processing. The LSA must work with other NSAs (designated 'supervisory authority concerned' or SAC) which have a stake in the outcome of the proceedings. An NSA may become a SAC for the purposes of the OSS when, in the context of cross-border processing: the data controller or processor also has an establishment in the NSA's jurisdiction; because data subjects who reside in the NSA's jurisdiction are likely to be substantially affected by the processing; or because the complaint being investigated was initially lodged with them.[23]

Therefore, in situations of cross-border personal data processing, the competent authority will be the LSA, but that authority does not act alone in handling complaints and the relevant investigation. To the contrary, there is a duty imposed on the LSA to endeavour to reach consensus with SACs and to exchange all relevant information with one another.[24] In leading the proceedings, the LSA should 'without delay' communicate relevant information to SACs and submit the draft decision to them to obtain their opinions.[25] The LSA is then obliged to take 'due account' of their views.[26] The Court considered the operation of this cooperation mechanism in *Facebook Belgium*.[27] It was asked whether, under the GDPR, an NSA can continue legal proceedings before a domestic court even though it is not the LSA. In its judgment, discussed further below, the Court confirmed that the cooperation mechanism was underpinned by the general principle of sincere and effective cooperation and emphasised the obligation of NSAs to cooperate to reach a single decision, binding on all authorities.[28] As a result, concurrent judicial proceedings before the courts in the territory of SACs should be discouraged.

As an interim conclusion, it can be observed that the OSS has a twofold rationale: first, to limit opportunities for fragmentation by creating a single point of contact for data controllers and processors for data protection oversight and enforcement in transnational contexts; and, second, to enhance

is a single EU establishment, but the personal data processing is likely to substantially affect data subjects in more than one Member State. An establishment is relevant for GDPR purposes where the processing of personal data takes places in the context of the activities of that establishment (Art 3(1) GDPR).

[21] Art 55 GDPR. [22] Art 56(1) GDPR and Recital 124 GDPR. [23] Art 4(22) GDPR. [24] Art 60(1) GDPR [25] Art 60(3) GDPR. [26] ibid.

[27] Case C-645/19 *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA* v *Gegevensbeschermingsautoriteit* EU:C:2021:483. [28] ibid para 75.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

cooperation among NSAs. Yet where this cooperation fails to reach consensus because the LSA does not wish to implement a 'relevant and reasoned' objection to its draft decision by a SAC, the adoption of the draft decision is temporarily blocked and the GDPR's consistency mechanism is engaged.[29]

B. Dispute Resolution through the Consistency Mechanism

There are two elements to the consistency mechanism: the power to issue opinions; and the power to engage in dispute resolution. Article 64(1) GDPR identifies certain circumstances in which the opinion of an EU body—the European Data Protection Board (EDPB)—must be sought, while Article 64 (2) provides that an opinion can be requested by any NSA, the Chair of the EDPB or the Commission on any matter of general application or producing effects in more than one Member State. The latter covers some failures in cooperation, with Article 64(2) GDPR explicitly noting that this includes instances where a competent supervisory authority does not comply with its mutual assistance or joint operations obligations. This opinion, if followed, should suffice to ensure consistency.

However, the GDPR also envisages circumstances where dispute resolution among NSAs is necessary. In these cases, the EDPB issues binding decisions as opposed to opinions. The EDPB skips straight to binding decisions where the LSA does not follow or rejects the reasoned and relevant objection of a SAC.[30] Binding decisions are also delivered where there is disagreement over the designation of the LSA and where the EDPB's Article 64 GDPR opinion is not followed.[31] This binding decision is addressed to the LSA and all SACs, and thus supersedes any conflicting decisions of NSAs.[32] The LSA and/or the NSA of the State where the complaint was lodged must then adopt a final decision based on the binding decision of the EDPB. Therefore, the EDPB's decision may be seen as a sort of 'preliminary act' to the binding decision adopted by the NSA. Such preliminary findings can be a feature of composite administrative decision making where:

> legislation requires an additional concluding procedural stage at the national level after an EU administration has adopted a decision, at which the national authority involved enjoys no discretion and fulfils a merely formal 'rubber-stamping' role.[33]

The final decision is adopted based on the following division of labour: the LSA notifies the controller or processor of the decision and the NSA of the State in which the initial complaint was lodged must notify the complainant.

[29] Art 60(4) GDPR. [30] Art 65(1)(a) GDPR. [31] Art 65(1)(b) and (c) GDPR.
[32] Art 65(2) GDPR.
[33] Brito Bastos (n 12) 67. See also S Fresa, 'Multilevel EU Governance in Energy Infrastructure Development: A New Role for ACER?' Working Paper (17 June 2015) <https://www.diw.de/documents/dokumentenarchiv/17/diw_01.c.508434.de/fresa.pdf>.

Nevertheless, where the complaint is rejected wholly or partially, the NSA of the complainant notifies both the controller or processor and the complainant of this dismissal or partial dismissal.[34] The presence of a 'chain' of EU and national acts is another feature of composite administrative decision-making.[35]

III. DEFICIENCIES OF THE COOPERATION AND CONSISTENCY MECHANISMS

The enforcement of the GDPR has become a focal point for scrutiny.[36] This section identifies and elaborates on the shortcomings of the cooperation and consistency mechanisms, including their potential incompatibilities with EU primary law. The four key deficiencies identified are: procedural ambiguities and divergences in the cooperation procedure; the lack of equality between regulators; procedural fairness flaws; and the preponderant influence of national, rather than European, priorities and regulatory approaches in the transnational GDPR enforcement by NSAs. These deficiencies share the dubious honour of hindering the effectiveness of the fundamental rights protected by EU data protection law.

A. Procedural Ambiguities and Divergences in the Cooperation Procedure

The cooperation mechanism is initiated at the national level and entails the application of national procedural rules jointly with (minimal) procedural rules foreseen by the GDPR. At present, there is a lack of clarity regarding the definition of key procedural concepts relevant for the cooperation mechanism under Article 60 GDPR. Such ambiguities are well-documented.[37] It can be confidently asserted that, as EU law concepts, the procedural notions included in Article 60 GDPR should be subject to the autonomous interpretation provided by EU institutions, especially the Court of Justice.[38]

[34] This division of labour is foreseen by Arts 60(7) to 60(9) GDPR.

[35] Brito Bastos (n 12) 66.

[36] For instance, the European Commission observed in its 2020 GDPR review that the new governance system had yet to 'deliver its full potential'. Commission, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - Two years of application of the General Data Protection Regulation', COM/2020/264 15 (2020 GDPR Review). See also the 'Vienna Statement' of European NSAs. EDPB, 'Statement on Enforcement Cooperation', adopted on 28 April 2022.

[37] Commission, 'Commission Staff Working Document Accompanying the document Communication from the Commission to the European Parliament and the Council: Data protection rules as a pillar of citizens empowerment and EUs approach to digital transition - Two years of application of the General Data Protection Regulation' SWD/2020/115, 9. At the national level, an Irish Parliamentary Committee noted that there was confusion regarding when a case could be said to be 'concluded' or 'resolved'. Houses of the Oireachtas – Joint Committee on Justice, 'Report on meeting on 27th April 2021 on the topic of GDPR' (July 2021) 23.

[38] e.g. Case C-66/85, *Lawrie-Blum* [1986] ECR 02121 regarding what counts as a 'worker' under Art 45 TFEU; Case C-246/80 *Broekmeulen* [1981] ECR 02311 regarding what counts as a 'court or tribunal' under Art 267 TFEU.

The EDPB's adoption of Guidelines on the functioning of Article 60 GDPR seeks to promote such an autonomous understanding of the concepts and rules included in the cooperation mechanism.[39] The Guidelines start from the premise that a 'common understanding of the terms and basic concepts is a prerequisite for the cooperation procedure to run as smoothly as possible'.[40] They emphasise that the endeavour to reach consensus required by the cooperation procedure is a legal objective which 'sets the direction for cooperative acting in such a way that SAs [ie supervisory authorities] do their utmost and make a ''serious determined effort'' in order to achieve consensus'.[41] It is clear that the EDPB envisages that an ethos and an obligation of sincere cooperation should permeate the interpretation and application of Article 60 GDPR. The EDPB Guidelines also specify the meaning of key procedural concepts found in the GDPR. It reads notions such as 'without delay', where it would be inappropriate to specify a single universally applicable time period, in light of the legislature's intent to increase 'the speed in the information flow connected with the draft decision'.[42] Moreover, the LSA 'has to act proactively and, as quickly as possible, appropriately to the case'.[43] While not precisely defining the term 'draft decision', the EDPB considers that it should be 'subject to the development of common minimum standards to enable all involved SAs to participate adequately in the decision-making process'. It therefore identified the minimum components of a 'draft decision'.[44]

It is evident that these Guidelines facilitate alignment of the understanding of GDPR terms while not entirely eliminating scope for divergence. They go some way towards providing the elements of a common administrative procedure, requested by both the Commission and prominent consumer organisation BEUC.[45] Yet, as Guidelines, they are non-binding. Therefore, as will be discussed below, if these Guidelines are not followed, it will fall to the Commission or the Court to rectify this failure, with procedural harmonisation via legislation acting as a final fall-back solution.

In any event, not all elements of the cooperation procedure lend themselves to an autonomous EU law interpretation. National procedural rules have a pivotal role to play in the cooperation mechanism. Yet disparities between national procedural rules have become a source of friction and delay.[46] Take, for

[39] EDPB, Guidelines 02/2022 on the application of Article 60 GDPR (Guidelines on Article 60) v.1.0, adopted on 14 March 2022.These Guidelines implement the EDPB's strategic priorities which resolve to promote 'a common application of key concepts in the cooperation procedure' and to encourage and to facilitate the use of the full range of tools provided in the GDPR.

[40] ibid 2. [41] ibid 12, para 39. [42] ibid 19. [43] ibid 19. [44] ibid 22 and 23.

[45] Commission, 2020 GDPR Review (n 36) para 21. BEUC, 'The long and winding road – Two years of the GDPR: A cross-border data protection enforcement case from a consumer perspective' (August 2020) 3.

[46] For instance, for an overview of the disparities between national procedures for complaint handling see: Access Now and Data Protection Law Scholars Network, 'The right to lodge a data protection complaint: OK, but then what? An empirical study of current practices under the GDPR', June 2022 <https://www.ivir.nl/publicaties/download/GDPR-Complaint-study-1.pdf>.

instance, rules on standing for representative bodies: the GDPR allows data subjects to mandate a non-profit organisation to lodge complaints and initiate legal actions on their behalf.[47] Nevertheless, divergences between the nature and the extent of the information required to verify the representation and standing of such organisations by, on the one hand, the NSA where a complaint is lodged, and, on the other hand, the LSA have emerged.[48] Such divergences have knock-on implications for the triggering of the cooperation procedure: the barriers encountered at the national level to submitting complaints may impede the initiation of the cooperation mechanism at the transnational level via the OSS. The ultimate result is a high risk of under-enforcement of the GDPR and ultimately of ineffectiveness of the cooperation mechanism. Moreover, standing is but one example of a wider problem: as we discuss below, procedural divergences and gaps lead to issues of procedural fairness for complainants in the OSS.

A by-product of this terminological ambiguity (what constitutes a 'draft decision') and national procedural divergences is that it is difficult to compare the performance of NSAs. As Advocate General Bobek suggested in *Facebook Belgium*, any assessment of the effectiveness of GDPR enforcement would need to be 'evidenced by facts and robust arguments' rather than speculation and assumptions.[49] Yet the absence of reliable comparator data renders this task more difficult.[50]

B. The Lack of Equality between NSAs

The LSA should function as a *primus inter pares*.[51] The GDPR supports this assertion. First, during the legislative process, there was a concern that the Commission's original proposal granted an outsized role to the LSA at the expense of the independence of other NSAs.[52] To address these concerns, the notion of a 'supervisory authority concerned' (SAC) was formalised[53]

[47] See art 80 GDPR.

[48] For instance, there have been several reports of the Irish NSA seeking additional information to assess the admissibility of such actions although they had already been deemed admissible by a SAC in Norway and the Czech Republic. BEUC (n 45) 11.

[49] *Facebook Ireland Ltd*, Opinion of AG Bobek, (n 10) paras 126 and 128.

[50] Oireachtas Joint Committee Report, (n 37), 11. This report states: 'Compared with other jurisdictions such as Austria, which has issued 852 decisions and Spain which has issued 700 decisions since the implementation of the GDPR in 2018, Ireland has only issued 4 decisions in the 196 cases it has been tasked with pursuing as LSA. For instance, civil society organisation NOYB claims that the Irish NSA had only addressed three decisions to private entities compared to over 600 by the Spanish NSA'. NOYB, 'Letter of Helen Dixon on the Draft Resolution on the CJEU judgment in C-311/18' <https://noyb.eu/sites/default/files/2021-03/Letter%20Max%20Schrems%20to%20LIBE.pdf>.

[51] *Facebook Ireland Ltd*, Opinion of AG Bobek, (n 10) para 111.

[52] European Parliament Rapporteur Albrecht, for instance, noted that 'The model proposed by the Commission however does not ensure the necessary independence of DPAs'. European Parliament, Explanatory Statement of 22 November 2013, A7-0402/2013.

[53] Art 4(22) GDPR; art 60(11) GDPR.

and the mechanisms for cooperation between the LSA and other concerned authorities were set out in Article 60 GDPR. Secondly, as the Court emphasised in *Facebook Belgium*, there is a legal obligation on the LSA to work with SACs to endeavour to reach consensus and to exchange all relevant information with one another.[54]

Thirdly, even if in principle the LSA is competent to deal with proceedings with a transnational dimension, there are exceptions to this rule. In *Facebook Belgium* the Court emphasised that where a LSA does not comply with a request for mutual assistance, a SAC may adopt a provisional measure on the territory of its own State and request the input of the EDPB if a final measure is urgently needed.[55] In this way, the Court reminded NSAs of their own obligations to take the reins to secure enforcement of the GDPR. Moreover, any NSA can request that any matter of general application or that produces transnational effects be examined by the EDPB.[56] In such circumstances, the SAC must be able to take measures necessary to ensure compliance with the EDPB's findings.

Fourthly, the LSA is given no special recognition in the voting procedure for binding EDPB decisions. Such decisions are adopted by a two-thirds majority of EDPB members and thus it is possible that the LSA's perspective is overridden in this context. In theory, therefore, although it is the competence of the LSA to coordinate the proceedings, the LSA and SACs remain on an equal footing throughout the cooperation procedure. Yet in reality, there is a discernible lack of equality between NSAs: the LSA can play an outsized role in administrative proceedings while the input of other concerned authorities is minimised.

To begin with, it should be recalled that the administrative enforcement of the GDPR involves the following five steps: (1) delimiting the scope of investigation and potential infringement based on an initial assessment of the facts; (2) establishing the facts; (3) establishing whether these facts amount to a violation of the Regulation or other data protection rules; (4) determining the corrective measures to be applied, including possible sanctions; and (5) ensuring that the corrective measures are enforced.[57] Early experience suggests that the LSA plays a decisive role in steps (1), (4) and (5) in these procedures and therefore can exercise a disproportionate influence on GDPR enforcement, to the exclusion of its peer regulators. How this comes about can be considered by taking the example of an investigation by the Irish NSA concerning Twitter which culminated in a binding decision of the EDPB pursuant to Article 65 GDPR.[58]

[54] Art 60(1) GDPR. [55] *Facebook Ireland Ltd* (n 27) para 74. [56] Art 64(2) GDPR.

[57] Council of the EU, 'Discussion note on possible thresholds for submitting cases to the EDPB' (2015) Doc nr 5331/15, (Council discussion note on EDPB thresholds) 4. The Council omitted (1) which we consider to be critical for GDPR enforcement purposes.

[58] EDPB, Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Art 65(1)(a) GDPR, adopted on 9 November 2020.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

First, the role played by the LSA in scoping the initial inquiry can shape the entire proceeding in a decisive way. The Irish NSA initiated an investigation of Twitter's data protection compliance, informing Twitter that its inquiry concerned the GDPR's data breach notification requirements.[59] Several SACs objected to the scope of the draft decision, which had been determined by the LSA alone at the outset of the process. They considered that Twitter engaged in further infringements of provisions such as the principles of integrity and confidentiality as well as accountability, amongst others.[60] However, the Irish NSA considered that it was within its discretion to limit the scope of the inquiry[61] and, given the original scope of the inquiry, the EDPB did not have sufficient material to establish the existence of these further infringements.[62] Although the GDPR does not explicitly grant SACs procedural rights until after a draft decision is submitted by a LSA, the exclusion of peer regulators from determining what violations will be investigated is incompatible with the general principle of loyal cooperation and throws cold water on the idea that the LSA is a *primus inter pares*.

Secondly, as the consistency mechanism does not cover the determination of corrective measures and fines—a task left to the LSA, the SACs have a limited role in defining the nature of corrective measures and sanctions, even though GDPR infringements may affect data subjects on their territory. During the legislative process, the Council considered this exclusion necessary to ensure that the workload of the EDPB remained reasonable and because NSAs are entitled to take account of many factors in exercising their corrective powers, including some which may be particular to that Member State.[63] In the Twitter proceedings, the German NSA had suggested a fine in the range of 7.3 to 22 million Euro. The Irish NSA ultimately imposed a fine of only 450,000 Euro on Twitter. The EDPB was seemingly unable to specify even the range in which the fine should fall.[64] The EDPB was more assertive in the subsequent WhatsApp decision, where the fine imposed increased fourfold following its intervention.[65] This is significant as the GDPR enforcement apparatus risks becoming devoid of purpose if the imposition of fines and corrective measures does not take into account the opinions of NSAs protecting the rights of those directly affected by the consistency mechanism decision.

Thirdly, it is notable that where there is disagreement between the LSA and SACs on a draft decision, SACs must meet a demanding threshold—that of

[59] Arts 33(1) and 33(5) GDPR.
[60] Further substantive infringements of art 5(1)(f), 5(2), 24 and 32 GDPR were alleged.
[61] EDPB (n 58) para 92.
[62] ibid, paras 132 and 133.
[63] Council discussion note on EDPB thresholds (n 57), 5.
[64] C Docksey, 'Article 65: Dispute Resolution by the Board' in LA Kuner et al (eds), *The EU General Data Protection Regulation (GDPR): A Commentary – 2021 Update* (OUP 2021) 227, 233.
[65] L Mustert, 'The EDPB's second Article 65 Decision – Is the Board Stepping up its Game?' (2021) 3 EDPL 416, 422–3.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

reasoned and relevant objection—for their objection to count.[66] According to the EDPB Guidelines, a SAC's reasoned objection must show why the LSA's draft decision would pose significant risks for the rights and freedoms of data subjects and/or the free flow of data.[67] Therefore, simple disagreement on the merits of the case is insufficient; rather, the difference must have a real impact.[68] This may seem an appropriate limitation on the role of SACs: one might wonder why they should intervene where the draft decision poses no significant risks to rights and freedoms. Yet its impact, it is suggested, must be considered in the aggregate: the requirement to prove a 'significant risk' is demanding and the SAC needs to show this in each individual case.[69] This becomes an onerous task for SACs and, de facto, creates a presumption in favour of the draft decision of the LSA while ultimately minimising the role of SACs.

What is clear is that, from its initial role in defining the scope and the direction of the investigation through to its determination of corrective measures, the LSA plays a preponderant role in proceedings. Meanwhile, the odds remain stacked against the perspectives of SACs which need to evidence their reasoned and relevant objections to LSA decision-making. This reality militates against the claim that the LSA acts as a first amongst equals. One might wonder, however, why equality between NSAs remains important. This equality matters for several reasons.

Equality between NSAs is desirable because it is necessary to flatten national interests in the context of these transnational administrative proceedings and to encourage NSAs to act as agents of EU law. Albeit composed of representatives of the NSAs and the European Data Protection Supervisor, the EDPB is an EU body. The member of the NSAs on the EDPB should 'act in the sole interest of the Union rather than act as vessels for a variety of national interests'.[70] Indeed, the cooperation and consistency mechanisms were designed to Europeanise EU decision-making on data protection, moving it away from disparate national interpretations and making oversight and enforcement in transnational contexts a collegial endeavour.[71] The price of this Europeanisation was that the level of protection offered in some Member States might be lower and that the pace of enforcement by active authorities might be slowed down.[72]

[66] Albeit that this threshold may be easier to reach than some of the alternatives proposed (such as quantitative thresholds of 1/3, 1/2 or 2/3 of all DPAs concerned). Council discussion note on EDPB thresholds (n 57) 3.

[67] EDPB, Guidelines 9/2020 on relevant and reasoned objection under Regulation 2016/679 Version 1.0, adopted on 8 October 2020, para 19.

[68] Docksey (n 64) 233.

[69] For instance, in the EDPB's second consistency decision several SACs submitted general comments rather than relevant and reasoned objections; however, these were not taken into consideration. Mustert (n 65) 417.

[70] M Busuioc, 'Rule-Making by the European Financial Supervisory Authorities: Walking a Tight Rope' (2013) 19(1) ELJ 111, 121.

[71] The EDPB rules of procedure refer to principles of collegiality as one of the pillars of the EDPB activities. See art 3 of the EDPB Rules of Procedure.

[72] For instance, the Commission acknowledges that at times 'finding a common approach meant moving to the lowest common denominator'. Commission, 2020 GDPR review (n 36) 5.

The *quid pro quo* for this erosion of national interests was consistency. The bargain struck might be thought of as follows: all Member States lost their individual stake, yet stood to gain from more effective enforcement.

However, to date, this bargain has not materialised: not all national interests have been flattened to the same extent as the LSA continues to play an oversized role in these mechanisms, but nor has there been more effective enforcement of EU data protection law. The role of SACs in the cooperation mechanism is deliberately designed to ensure maximum proximity between complainants and those investigating complaints.[73] Yet these entities encounter significant limitations in their potential influence in the cooperation mechanism. It is suggested that while there is no explicit principle of equality between NSAs, this lack of equality undermines the legitimacy of the framework.

A further by-product of the lack of equality between NSAs is that, failing the emergence of a truly cooperative culture between NSAs, resort to the consistency mechanism may well shift from being the exception to being the rule. This procedure places an extraordinary burden on all NSAs. Docksey has highlighted the challenges in the handling of reasoned objections in the Twitter case, where 'the LSA was obliged to respond to them in detail and finally the matter had to be addressed by the Board'.[74] Moreover, given that the LSA may need to reconcile potentially conflicting objections of SACs, the prospect of the consistency mechanism being invoked is heightened. Therefore, what could be a single decisional process in situations where cooperation functions effectively risks becoming a protracted multi-jurisdictional and multi-tiered process.[75] Such a scenario seems destined to favour organisations with deep-pockets and experience of complex multi-jurisdictional litigation.

In sum, the consequences of the absence of equality among NSAs are stark: such lack of equality delegitimises the legislative choice to neuter the more stringent NSAs in favour of a more Europeanised approach to enforcement; it has placed significant resource burdens on NSAs; and, ultimately, has impeded NSAs from becoming agents of European rather than national law. These implications are further exacerbated by gaps in the procedural fairness guarantees found in the cooperation and consistency mechanisms.

[73] During Council negotiations there was an attempt to limit the definition of SAC which was rejected by Member States on this ground. See Council of the EU, 'GDPR – the one stop shop mechanism', 5627/1/15 REV1, (11 February 2015) 2.

[74] Docksey (n 64) 234.

[75] A good example of this is the Whatsapp investigation initiated by the Irish DPC in 2018 following complaints and which led to the second consistency decision of the EDPB (Mustert (n 65)). Both the EDPB decision and the Irish DPC have been appealed before the General Court and Irish High Court respectively (see Case T-709/21, *WhatsApp Ireland v EDPB*, pending and C Taylor and A O'Faolain, 'WhatsApp challenges DPC's €225 million fine' (*Irish Times*, 16 September 2021)).

C. Insufficient Procedural Fairness Guarantees

The diagonal composite administrative proceedings created by the GDPR raise the prospect of myriad procedural fairness challenges. Procedural fairness is essential in any legal system because it enhances the legitimacy of and trust towards public authorities while ensuring fair decision-making.[76] It does so, among others, by favouring democratic participation in decision-making procedures and by guaranteeing the neutrality of public authorities towards the parties to a dispute.[77] Procedural fairness ultimately contributes to judgments and settlements which favour compliance with the law.[78] It is therefore not surprising that procedural fairness guarantees underpin the text of several constitutions and fundamental rights treaties, including the EU Charter of Fundamental Rights.[79]

The OSS and the consistency mechanism involve an intrinsic contradiction in terms of procedural fairness: while they sought to introduce stricter rules on cooperation among NSAs with the objective of facilitating effective decision-making under the GDPR, they also feature significant gaps in terms of procedural rights. For instance, a crucial aspect of procedural fairness is that decisions should be issued in a reasonable time.[80] Considerations of timeliness are built into the OSS mechanism. For instance, Article 65(1) GDPR provides that where a LSA does not request or follow the opinion of the EDPB, SACs or the Commission may communicate the matter to the Board, thus immediately triggering the consistency mechanism. Yet although the OSS mechanism was designed to enhance efficiency by arriving at a single supervisory decision through a quicker administrative procedure, the reality of its operation has been described differently: 'serious cross-border cases involving all DPAs hang in the mill of a bureaucratic procedure for years and absorb the strength and the poor resources of the authorities'.[81] This type of paralysis is not unique to data protection law and is an inherent risk in European procedures involving Member States' representatives.[82] The EDPB rules of procedure have been amended to expedite the initiation of the consistency mechanism by allowing the EDPB Chair to initiate the dispute

[76] K van den Bos et al, 'When Do We Need Procedural Fairness? The Role of Trust in Authority' (1998) 75(6) Journal of Personality and Social Psychology 1149, 1455.

[77] J Brockner 'Making Sense of Procedural Fairness: How High Procedural Fairness Can Reduce or Heighten the Influence of Outcome Favourability' The Academy of Management Review (January 2002) 58.

[78] RT Tyler, 'Procedural Fairness and Compliance with the Law' (1997) Revue Suisse D'Economie Politique et de Statistique, 219–40.

[79] In particular, the 'Justice' title of the EU Charter.

[80] J Flattery, 'Balancing Efficiency and Justice in EU Competition Law: Elements of Procedural Fairness and Their Impact on the Right to a Fair Hearing' (2010) 7(1) The Competition Law Review 53, 79.

[81] Statement of 7/07/20, Missed Opportunity to take action (Hamburg DPC). See also N Kobie, 'Germany says GDPR could collapse as Ireland dallies on big fines' (*Wired*, 27 April 2020) <https://www.wired.co.uk/article/gdpr-fines-google-facebook>.

[82] Busuioc (n 70) 111, 120.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

resolutions procedure.[83] Other issues, such as the sometimes-lengthy wait before a LSA is designated, could similarly be more quickly resolved.[84]

A further aspect of procedural fairness is that no one should be tried or punished twice for the same offence, a principle enshrined in Article 50 of the EU Charter.[85] This provision is central to ensuring due process guarantees under the GDPR considering the possibility of overlapping fines and proceedings of a criminal nature within the EU territory. As established in *Facebook Belgium*, the general rule is that data protection proceedings will be managed by the LSA, the competence of SACs being the exception.[86] Yet where SACs trigger the urgency procedures foreseen, the risk of parallel data protection proceedings across the Member States becomes more tangible.

An exhaustive identification and treatment of the potential procedural fairness issues of composite data protection proceedings is beyond the scope of this article. Instead, it focusses on the most immediate challenges that the OSS and the consistency mechanism engender. First, these proceedings entail the de facto exclusion of data subjects from the cooperation and consistency procedure. Secondly, the interaction between these composite proceedings and Articles 78 and 79 GDPR sits uncomfortably with the EU Charter right to an effective remedy. In practice, the role of the individual in these procedures seems to be lost behind the curtain of administrative cooperation. These concerns will be addressed in turn.

1. Composite proceedings may entail the de facto procedural exclusion of data subjects

Procedural fairness demands participation of the parties involved in a dispute in the decision-making procedure. The GDPR provides individuals with a right to lodge a complaint with a supervisory authority, in particular in the Member State of their habitual residence, place of work or the place of the alleged infringement.[87] Where the complaint concerns cross-border data processing, the NSA which receives the complaint must inform the LSA without delay and the LSA must determine (again, without delay) whether it wishes to handle the complaint and therefore engage the OSS procedure. As discussed above, the national procedural rules of the LSA apply from the point at which it assumes responsibility for the complaint.[88] The status of

[83] Such amendment to the EDPB rules avoids delays and acknowledges that the EDPB 'is best placed to start the dispute resolution procedure itself'. P Van Eecke and A Šimkus, 'Article 64. Opinion of the Board' in C Kuner, LA Bygrave and C Docksey (eds), 'The EU General Data Protection Regulation (GDPR): A Commentary – 2021 Update' (OUP 2021) 224, 225–6.

[84] BEUC (n 45) 13.

[85] 'No one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law.'

[86] *Facebook Ireland Ltd* (n 27) para 56.

[87] Art 77(1) GDPR.

[88] EDPB Guidelines on Article 60 considers that national procedural autonomy applies to such administrative procedures. EDPB Guidelines on Article 60 (n 39); see paras 32–35 and 110.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

complainants and other parties to the proceedings (including those under investigation) are therefore determined by the national law of the LSA. Hofmann observes that:

> when the lead authority will open an investigation against a data controller, the complainant has no enforceable rights to participate since procedures before a lead authority are, in this system, conducted like investigations upon another authority's initiative.[89]

As a matter of fact, the rights foreseen by the GDPR for data subjects in this context are limited. For instance, complainants are only notified of a decision once it is adopted in accordance with the national laws of the State where they lodged the complaint.[90] Their prior involvement is ostensibly limited to furnishing their local NSA—a SAC in the cooperation procedure—with relevant information that might be passed on to the LSA.

Given the ultimate objective of GDPR investigations—to ensure violations of rules protecting personal data are effectively identified and redressed—the exclusion of complainants is striking, particularly given that it is their fundamental rights under Articles 7 and 8 of the EU Charter that are at stake. This exclusion also sits uneasily with procedural fairness rights, in particular the right to be heard and the rights of defence. These two entitlements are enshrined in a series of Charter provisions[91] and are essential to ensure 'democratic input' by way of involvement of data subjects in the enforcement of the GDPR. Without the possibility for complainants to be heard, the chance to obtain an effective remedy for violations of the GDPR may be hindered. Where complainants are unable to explain their perspectives and to react to the evidence submitted by controllers and processors in the context of investigations, complainants may end up receiving a remedy which does not adequately address the GDPR violations. This result would run counter to Article 19(1)TEU, which provides that Member States shall provide remedies sufficient to ensure effective legal protection in the fields covered by Union law. This norm is a direct expression of the rule of law in the EU, one of its founding values.[92]

The EDPB Guidelines on Article 60 GDPR seek to alleviate some of the procedural fairness concerns that stem from this exclusion. For instance, they provide that the LSA should ensure that the draft decision it produces is fully compliant with the domestic law provisions regarding the right of the parties to the proceedings to be heard. Moreover, the LSA should specify the steps taken to ensure compliance with that right in the text of the draft decision.[93] With specific reference to the right to good administration in Article 41 EU Charter, the Guidelines also provide that the decision issued as a result of the

[89] Hofmann (n 13) 23. [90] Art 60(7) GDPR. [91] Arts 41, 47, 48 of the EU Charter.
[92] Case C-64/16 *Associação Sindical dos Juízes Portugueses* EU:C:2018:117, para 32.
[93] EDPB, 'Article 60 Guidelines' (n 39) para 105.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

cooperation mechanism should include a description of relevant facts, sound reasoning and a proper legal assessment to enable relevant parties to assess whether they wish to challenge the decision before a Court.[94] The Guidelines also emphasise that good administration requires the LSA and other NSAs to deal with complaints in a reasonable time.[95] The EDPB emphasises the overarching obligation of NSAs to exercise their discretionary powers 'impartially, fairly and within a reasonable time', in accordance with the provisions of GDPR and with appropriate procedural safeguards found in EU and Member State laws.[96]

While these Guidelines offer some reassurance to the parties to composite proceedings, they do not possess legally binding effect and may thus be disregarded by their addressees.[97] Gaps in legal protection for affected parties in LSA proceedings are therefore likely to persist. Most notably, there is no guaranteed right for the complainant to participate in the proceedings before the LSA. The EDPB Guidelines seem to suggest that this deficiency can be remedied by taking utmost account of the views of the SACs, as representatives of the parties involved. Yet this solution remains less compelling when the role of the SAC is minimised, as discussed above, or its objections are disregarded by the LSA, triggering the consistency mechanism.[98]

Similarly, gaps can be identified in the procedural fairness guarantees for data subjects in the consistency procedure. Although the EDPB is bound by EU administrative law and must respect the right to good administration,[99] neither complainants, data controllers nor processors have a right to be heard in the EDPB procedure.[100] This procedural exclusion is not necessarily problematic if the EDPB's decision is based only on matters arising before the LSA where the parties had the opportunity to be heard. However, as just noted, this is not always the case. This lack of representation before the EDPB is further exacerbated by the limited standing for non-privileged applicants before EU courts. Procedural fairness is expressed via the right to obtain a judicial remedy in case of violation of the law. The decisions and acts issued by the EDPB can be challenged before the EU courts, and both individuals and NSAs would qualify as non-privileged applicants under Article 263 TFEU. When EDPB decisions clearly state their addressees, then standing for those addressees would be easily fulfilled under Article 263(4) TFEU. Yet if the complainants, controllers or processors are not the addressees of the EDPB's acts, they may encounter significant hurdles in

[94] ibid, para 111. [95] ibid, para 123. [96] ibid, para 29.

[97] G Gentile, 'To Be or Not to Be (Legally Binding)? Judicial Review of EU Soft Law after *BT* and *Fédération Bancaire Française*' (2021) 70 Revista de Derecho Comunitario Europeo, 981.

[98] See the 'equality' section above. [99] Art 41 EU Charter.

[100] In Case T-709/21, *WhatsApp Ireland* (n 75), WhatsApp appeals the EDPB decision, inter alia, on the grounds that the EDPB infringed its Article 41 EU Charter by disregarding WhatsApp's right to be heard and by failing to carefully and impartially examine the evidence and provide reasons.

accessing the review of the EU judicature as they must prove the demanding requirements of individual and direct concern under the *Plaumann* formula.[101]

2. *An effective remedy under Article 78 GDPR?*

The handling of the dismissal of complaints foreseen by the cooperation mechanism provides for multiple decisions to be issued by the various authorities involved.[102] In particular, the LSA must notify the controller and processor while the SACs must inform the complainants residing in their territories. This system was designed to seek maximum proximity between complainant data subjects and their NSAs, with amendments made to the Commission proposal during the legislative process to ensure this.[103] They were, as Advocate General Bobek put it, 'specifically intended to avoid data subjects having to "tour" the courtrooms of the European Union in order to bring proceedings against inactive supervisory authorities'.[104] However, there are several controversial implications stemming from this rule.

Although the OSS creates a single point of contact for controllers and processors, the desire to allow complainants to engage with their local NSAs creates a web of parallel procedural processes.[105] Friction between administrations becomes a tangible scenario and may ultimately undermine legal certainty.[106] Additionally, and more worryingly, Article 60(9) GDPR entails a gap in legal protection. The complainant may have an interest in challenging the decision of the LSA which rejects or dismisses the complaints or where the LSA fails to act. Even where a complaint is upheld fully or partially, the complainant might have an interest in challenging the corrective measure adopted by the LSA.[107] However, according to Article 78 GDPR, an action against a NSA shall be brought before the court of the Member State where the NSA is established. It may be difficult for an unsatisfied complainant to bring a claim before the courts of the jurisdiction within which the LSA operates. This hurdle is discussed in the EDPB guidelines on Article 60 GDPR, but no solution is presented.[108]

[101] See Case C-25/62 *Plaumann* v *Commission* of the EEC EU:C:1963:17. *Prima facie*, it appears hard to establish standing in light of the EU case law. As demonstrated in cases such as *Piraiki-Patraiki*, (Case C-11/82 EU:C:1985:18, [1985] ECR 207) the individual concern requirement regards classes of individuals who can be distinguished in an absolute way. When a group of individuals could be joined by others in the future and do not relate to completed, past fact situations, the individual concern requirement would not be fulfilled. Classes of data subjects may be affected by the same challenges to prove standing.

[102] Art 60(9) GDPR.

[103] Council of the EU. 'GDPR - The One-Stop-Shop Mechanism' (n 73).

[104] *Facebook Ireland Ltd*, Opinion of AG Bobek, (n 10) para 105.

[105] The splintering of the notification duty across multiple jurisdictions may result 'in the possibility of several inter-related decisions under Member State and EU law'. Hofmann (n 13) 23.

[106] For instance, delays necessarily ensue where a LSA re-verifies the admissibility of complaints that were deemed admissible by the complainants' local NSA. BEUC (n 45) 11.

[107] See below.

[108] EDPB Guidelines on Article 60 (n 39) para 213ff.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

In this context, there is also a risk that the decision notified to the complainant might simply be a formulaic response to the complaint, with the substance of the decision found in the decision addressed to the controller by the LSA. In such circumstances, it is unclear whether a data subject would have to bring proceedings before the courts of the LSA's Member State to obtain effective redress. These hurdles in accessing a court raise equality concerns. As Hofmann observes:

> Essentially, procedural rights of those individuals, who are not capable of mounting a complaint outside of their home jurisdiction will be disadvantaged, possibly thereby in violation of the prohibition of discrimination on the basis of nationality or origin protected under Article 21 CFR.[109]

A further, final procedural fairness issue arising from Article 60(9) GDPR is linked to horizontal divergence: a complainant who received a decision from their NSA may want to challenge that act before national courts.[110] The courts hearing the challenge to the decision may annul that decision in full or in part. As a result, divergent findings in different jurisdictions and ultimately fragmented enforcement of the GDPR would arise.[111] Yet a requirement of procedural fairness is legal certainty in so far as it contributes to the predictability of decisions.[112] It has been suggested that the establishment of a common register with the EDPB might mitigate this risk. However, this measure would merely render transparent conflicting findings.[113] Moreover, where the dispute resolution mechanism is invoked and the LSA communicates the final decision to the controller or processor, both the final decision of the LSA and the decision of the EDPB are subject to potential challenge.[114] From a strategic perspective, this risks unnecessarily depleting the resources of NSAs and the EDPB, defending decisions on multiple fronts, and stands to benefit data controllers with deep pockets, such as Big Tech companies. As Mustert notes, it is questionable how a LSA which does not agree with the findings of the EDPB consistency decision will defend these findings before a national court when its decision giving them effect is challenged.[115]

In conclusion, one may wonder whether Article 78 GDPR is compliant with the right to an effective remedy, one of the tenets of procedural fairness in Article 47 EU Charter and Article 19(1) TEU. Under a combined reading of these provisions, effective remedies should exist in the fields covered by EU

[109] Hofmann (n 13) 23 fn 91.
[110] This possibility is envisaged under art 78 GDPR and recital 129 GDPR.
[111] Foreseen by recital 144 GDPR. One may wonder whether this recital is compatible with art 41 EU Charter.
[112] C Sunstein, 'Two Conceptions of Procedural Fairness' (2006) 73(2) Social Research 619.
[113] Submission of Austrian Delegation to DAPIX, 5571/15.
[114] Recital 143 GDPR affirms that actions for annulment may be brought against the decisions of the EDPB before the CJEU by CSAs and natural and legal persons where they are directly and individually concerned by the decision.
[115] Mustert (n 65) 419–20.

law. The importance of the right to an effective remedy in the EU has been extensively explored in the literature,[116] suffice it to recall here that the possibility to obtain an effective remedy is of particular relevance for the EU due to its complex legal structure, which relies both on EU and national authorities for the implementation of EU law.[117] Indeed, where public authorities fail to comply with EU law, individuals should be entitled to access courts to vindicate the rights and legal interests stemming from EU law. However, the system of remedies available in the context of the OSS and consistency mechanisms falls short of providing effective remedies.

This is perhaps most starkly illustrated by the inclusion of Max Schrems as a named defendant in litigation initiated by the Irish NSA before the Irish Courts.[118] Although contested by the Irish NSA, the European Parliament considered that this litigation highlighted the difficulties experienced by data subjects in cross-border proceedings and created a chilling effect on their ability to defend their rights.[119] More mundane, yet nevertheless significant obstacles to an effective remedy include rules regarding admissibility, funding and legal aid, and a lack of transparency regarding the handling of complaints in cross-border situations.

It is therefore apparent that the breadth of the gaps in the procedural fairness guarantees stemming from the GDPR is remarkable. However, the effective enforcement of the GDPR suffers also because of the discretion exercised by NSAs, as the next section will illustrate.

D. NSAs' Discretion Impedes Effective Transnational Enforcement: Rule of Law Challenges

One of the founding values of the EU is the rule of law.[120] The rule of law has clearly acquired normative content in the EU through recent legislative measures[121] and the jurisprudence of the ECJ.[122] An expression of this is the principle of judicial independence, which guarantees that EU law should be applied effectively.[123] In EU law, the rule of law also requires respect for the principles of legality,[124] implying a transparent, accountable, democratic and

[116] E Sharpston, 'Effective Judicial Protection through Adequate Judicial Scrutiny—Some Reflections' (2013) 4(6) JECL&Pract 453; V Roeben, 'Judicial Protection as the Meta-norm in the EU Judicial Architecture' (2020) 12 HJRL 29.

[117] Case C-26/62, *Van Gend en Loos v Netherlands Inland Revenue Administration* [1963] ECR-1, Case C-6/64 *Costa v Enel* [1964] ECR-00585.

[118] See NOYB (n 50).

[119] (2020/2789(RSP)), 'European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 — *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ('Schrems II'), Case C-311/18', para H.

[120] See art 2 TEU.

[121] Regulation (EU) 2020/2092 on a general regime of conditionality for the protection of the Union budget, OJ L 433I

[122] See Cases C-156/21 *Hungary* v *European Parliament et al*., EU:C:2022:97, C-64/16 *Associação* (n 92); Case C-619/18, *Commission* v *Poland* EU:C:2019:531.

[123] Case C-619/18 *Commission* v *Poland* (n 122) para 47.

[124] Case C-496/99 P *Commission* v *CAS Succhi di Frutta*, EU:C:2004:236, para 63.

pluralistic law-making process, legal certainty,[125] and prohibition of arbitrariness of the executive powers.[126] These principles reflect the consolidated formal theories on the rule of law.[127]

Applying the formal rule of law conception—which focuses on the equal application of the law—to the OSS and consistency mechanisms, it follows that the NSAs should strive, collectively and individually, to enforce the GDPR in an equal manner in the context of transnational enforcement, without creating different treatments for data subjects, controllers and processors located in different jurisdictions. In a way, the cooperation and consistency mechanisms seek to enhance compliance with the rule of law when it comes to the GDPR by regulating the rules of the cooperation game among NSAs. Yet the achievement of the equal enforcement of the GDPR in transnational settings, and thus of the formal aspect of the rule of law, is seriously hindered by the national strategies adopted by NSAs, especially LSAs.

As Hijmans observes, the consistency mechanism requires the consistent application of the law, rather than consistent strategies.[128] Two main fault lines have emerged. The first concerns strategic or selective enforcement, including whether NSAs focus on particular sectors or data controllers. For instance, while many of the discussions of under-enforcement concern 'Big Tech', the Irish Commissioner has stated that such a selective focus is irrational as 'it discloses far too narrow a view of the problems at hand, the result of which would be to permit substantial amounts of unlawful processing to continue, unchecked'.[129]

A second emerging divergence in terms of enforcement approach regards the extent to which amicable or negotiated settlements between the NSA and the data controller or processor meet the GDPR's enforcement objectives. Practice suggests that NSAs have historically sought to reach amicable solutions in the context of complaints, a position seemingly endorsed by the EDPB.[130] Amicable solutions to complaints may have the strategic advantage of solving complaints more efficiently, while conserving the financial and human resources of NSAs. Moreover, the resolution of complaints via

[125] Joined Cases C-212/80 to 217/80, *Meridionale Industria Salumi and Others*, EU:C:1981:270, para 10.

[126] Cases C-46/87 and 227/88 *Hoechst* v *Commission*, EU:C:1989:337, para 19.

[127] See LL Fuller, *The Morality of Law* (Yale University Press 1964); J Raz, *The Authority of Law: Essays on Law and Morality* (Clarendon Press 1979) 214.

[128] See H Hijmans, How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner?'(2018) 1 EDPL 1.

[129] Letter from the Irish Data Protection Commissioner to the European Parliament (12 March 2020) available at <https://www.dataprotection.ie/sites/default/files/uploads/2021-03/DPCtoLibe12.03.21.pdf>.

[130] See European Parliament question: <https://www.europarl.europa.eu/doceo/document/E-9-2021-002629-ASW_EN.html>. However, the EDPB does not seem to view amicable dispute settlement as contrary to the GDPR: see <https://edpb.europa.eu/system/files/2022-01/20211118plenfinalminutes57thplenarymeeting_public.pdf>.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

amicable settlement would further prevent the need to resort to judicial proceedings. Some argue that more effective compliance with the GDPR can be ensured by regulators engaging responsively with organisations to influence the ethical culture and behaviour of those market operators, rather than relying on 'backward-looking' rules enforced by sanctions.[131] However, the risk of emphasising amicable resolution over other enforcement strategies is that fundamental rights may be imperilled while regulators embolden systematic infringers of the regulatory framework.[132]

The GDPR does not explicitly resolve these more strategic questions. It obliges NSAs to 'handle complaints … and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and outcome of the investigation'.[133] This has been interpreted by some NSAs to mean that they are not obliged to produce a decision in all circumstances and can instead resort to the amicable settlement of disputes[134] or even to switch to own initiative inquiries in the course of complaint-handling.[135] On this reading, it is possible that transnational complaints might not reach the stage of a draft decision, thereby short-circuiting the OSS system and cutting SACs out of the picture. Such actions also eliminate or reduce the possibility for complainants to contribute to the investigations, although their input might be beneficial, and hinders the complainant from seeking follow-on damages in private litigation.

However, this reading is contestable. Not only must the LSA communicate 'relevant information' to SACs without delay; the non-binding recital 131, which is the only GDPR provision to refer to the amicable settlement of disputes, applies where the local NSA acts instead of the LSA due to the complaint's domestic nature or impact. This calls into question whether such amicable settlements can be used where the OSS is engaged. This example suggests that some NSAs continue to act as agents of national law rather than agents of European law when they apply data protection law. As a result of these differing enforcement strategies, the GDPR is subject to differential enforcement, leading to an unequal application of the law. The formal rule of law is therefore at risk with differentiated enforcement benefitting non-compliant data controllers and processors.

If data controllers perceive certain jurisdictions to be more lenient than others, there is a real risk that they will set up their establishment in those jurisdictions to shield themselves from regulatory action by more stringent regulators, a possibility alluded to by Advocate General Bobek.[136] Regulators continue to jostle, as happened in *Facebook Belgium*, to claim

[131] C Hodges, 'Delivering Data Protection: Trust and Ethical Culture' (2018)1 EDPL 65, 70.
[132] See recital 131 GDPR. Oireachtas Joint Committee Report (n 37) 23.
[133] Art 57(1)(f) GDPR. See also recital 131 GDPR.
[134] Access Now and Data Protection Law Scholars Network (n 46) 27–32.
[135] EDPB (n 58) para 2.
[136] *Facebook Ireland Ltd*, Opinion of AG Bobek, (n 10) para 124.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

oversight competence for various matters since the GDPR's entry into force.[137] Nevertheless, whether motivated by GDPR enforcement, or broader commercial considerations such as favourable taxation regimes, it is clear that some jurisdictions—notably Ireland and Luxembourg—act as LSAs in a disproportionate number of proceedings.[138] Assuming that data controllers and data processors secure a regulatory benefit—in the form of weaker enforcement—from this arrangement, this leads to lower levels of fundamental rights protection (by neutering the more active NSAs);[139] weakens competition on the internal market by creating 'geographical advantages as well as disadvantages';[140] and imposes unequal costs for data protection compliance across the residents of the EU. One might wonder, for instance, why the residents of Luxembourg should foot the bill to ensure the effective data protection of the residents of Sweden or Slovakia.

This situation may also lead to NSAs seeking alternative routes beyond the OSS to secure effective data protection, particularly those where the rights of data subjects have historically been subject to higher protection. For instance, in *Facebook Belgium* the Belgian NSA wished to continue with judicial proceedings before a domestic court rather than going down the administrative route through the OSS mechanism. Although neither the Advocate General nor the Court accepted its pleas, it explicitly argued before the Court that judicial proceedings were necessary to remedy the deficiencies in the OSS mechanism and ensure effective protection for data subjects.[141] This plea suggests that the Belgian NSA doubted the effectiveness of the cooperation with the Irish NSA which would have acted as LSA in the context of OSS proceedings. Recourse to proceedings before national courts as an alternative to the OSS would potentially lead to litigation concerning the differing levels of protection of fundamental rights when protected both at EU and national level.[142] Practice indicates that NSAs are finding other ways to

[137] V Manancourt, 'Why Europe's Hands Are Tied on TikTok' (*Politico*, 2 September 2020) <https://www.politico.eu/article/tiktok-europe-privacy-gdpr-complexity-ties-hands/>. The Irish DPC has subsequently assumed the role of LSA: BBC, 'TikTok Faces Privacy Investigations by EU Watchdog' (15 September 2021) <https://www.bbc.co.uk/news/technology-58573049>.

[138] According to the Irish Council for Civil Liberties (ICCL), a small number of Member States (Ireland, Spain, Germany, Netherlands, France, Sweden, and Luxembourg) receive almost three quarters (72 per cent) of all cross-border complaints referred between DPA. ICCL, 'Europe's Enforcement Paralysis: ICCL's 2021 Report on the Enforcement Capacity of Data Protection Authorities' (2021) 4.

[139] It emphasised that under the OSS the LSA or any CSA could not eschew their responsibility to contribute to the provision of effective fundamental rights protection as, if this were to occur, it would lead to forum shopping by data controllers. *Facebook Belgium* (n 27) para 68.

[140] European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)) 21.

[141] *Facebook Ireland Ltd*, Opinion of AG Bobek, (n 10) para 20ff.

[142] See arts 52 and 53 of the EU Charter. In particular, art 53 of the EU Charter has been interpreted by the CJEU as giving prevalence to the EU level of protection when both EU and national fundamental rights are applicable (see C-399/11, *Melloni* EU:C:2013:107). However, other readings are possible. For instance de Witte and Spaventa suggest that this interpretation is

sidestep the OSS to guarantee fundamental rights protection. For instance, the French NSA has sanctioned Google for breach of the ePrivacy Directive rather than the GDPR, thereby avoiding the OSS, with the French *Conseil d'Etat* upholding this course of action.[143] In a similar vein, other regulatory agencies can sidestep the application of GDPR mechanisms by initiating legal proceedings where similar or identical factual circumstances give rise to an alleged infringement of a distinct area of law, such as consumer protection or competition law.[144]

In conclusion, the current application of the cooperation and consistency mechanisms appears challenging from the angle of the equal application of the law and risks stretching the limits of compliance with the rule of law, especially in its formal meaning. The following section considers how these problems with the transnational enforcement of the GDPR might best be addressed.

IV. ADDRESSING DEFICIENCIES TO SECURE EFFECTIVE TRANSNATIONAL ENFORCEMENT

This section identifies some of the options available to address the four deficiencies identified in the previous section: ambiguous and autonomous procedures; the lack of equality between NSAs; inadequate regard for procedural fairness; and divergent enforcement strategies by NSAs which risk breaching the equal application of the law and thus the rule of law. It is suggested that many of the deficiencies identified could be remedied from within the existing framework, by encouraging NSAs to act more cooperatively and the EDPB to act more robustly against the backdrop of general principles of EU law. Where such encouragement fails, enforcement action by the Commission, intervention by the Court of Justice, procedural harmonisation, or a combination of the three may be required.

contrary to the multilayered, pluralistic protection of fundamental rights in the EU and that the national standard should prevail where more protective (see B De Witte, 'Article 53' in S Peers et al (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014); E Spaventa, 'Should We "Harmonize" Fundamental Rights in the EU? Some Reflections about Minimum Standards and Fundamental Rights Protection in the EU Composite Constitutional System' (2018) 55(4) CMLR 997). National courts have problematised the existence of various overlapping fundamental rights by reaching contradicting results. For instance, the Spanish Tribunal Constitucional has transformed the interpretation (ie lowered in terms of protection) of the right to a fair trial after the decision of the CJEU in *Melloni*, while the German Federal Constitutional Court has adopted an unclear notion of harmonisation of EU law to justify cases in which a set of circumstances could be scrutinised under national (German Federal Constitutional Court/ 1 BvR 16/13 ('Right to be Forgotten I') or EU (German Federal Constitutional Court, 1 BvR 276/17 ('Right to be Forgotten II') fundamental rights.

[143] CNIL, 'Cookies: The Council of State Confirms the Sanction Imposed by the CNIL in 2020 on Google LLC and Google Ireland Limited' (28 January 2022) <https://www.cnil.fr/fr/node/122118>.

[144] Indeed, in the *Facebook Belgium* case the referring court had noted that the German Competition Authority (the Bundeskartellamt, or BKA) 'clearly considered itself to be competent, in spite of the "one-stop-shop" mechanism'. *Facebook Belgium* (n 27) para 40.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

A. Leveraging General Principles of EU Law to Align Procedures

Many of the shortcomings of the cooperation and consistency mechanisms do not stem from their design but from the failure of NSAs and the EDPB to implement these mechanisms appropriately. A shift in approach from key actors would therefore lead to significant improvements.

As NSAs act within the scope of EU law, they should comply with general principles of EU law, including the principle of sincere cooperation and, indirectly, the sub-principle of effectiveness. Article 4(3) TEU imposes a duty on national authorities to assist each other in carrying out the tasks stemming from the Treaties, and to 'take any appropriate measure […] to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union'. Moreover, Member States must facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives.[145] Therefore, the activities of NSAs in the context of the OSS and the consistency mechanism should be guided by the objective of attaining sincere cooperation in the EU legal landscape.

The principle of effectiveness may also be helpful in framing the enforcement duties of NSAs. This principle ensures that the enforcement of EU rights is not made impossible or excessively difficult.[146] It was developed, alongside the principle of equivalence, by the CJEU to act as an outer limit on the national procedural autonomy.[147] Under the principle of equivalence, the national courts are required to assess whether remedial rules used in the field of the GDPR are more stringent than those used for similar national claims—an example being rules on fines or on damages. While they are applied by national courts, both principles are subject to the exclusive interpretation by the Court of Justice, meaning that national courts should cooperate with the Luxembourg judges to set the standards of the effective enforcement of EU law, including the GDPR. Via judicial proceedings,[148] parties unsatisfied with the way in which NSAs have applied EU law may bring legal action against that authority. However, as discussed above, there are significant hurdles when it comes to the right to effective judicial protection following the initiation of the OSS.

Moreover, NSAs are also bound by the EU Charter, which should be respected in the context of national procedures applied in the fields of EU law.[149] For instance, one might argue that, in light of the criminal nature of the sanctions imposed for violation of the GDPR, the procedures of the LSA

[145] Art 4(3) TEU.
[146] Case C-33/76 *Rewe* v *Landwirtschaftskammer für das Saarland* EU:C:1976:188.
[147] Case C-224/97 *Ciola* EU:C:1999:212.
[148] See art 78 GDPR.
[149] According to art 51 of the Charter, the Charter applies to Member States when they are implementing EU law. The national procedures used in the scope of application of the GDPR would constitute an instance of implementation of EU law. See Case C-617/10 *Åkerberg Fransson* EU:C:2013:105.

must be quasi-judicial in nature.[150] According to Article 6 ECHR, in the light of which Article 47 of the EU Charter must be interpreted,[151] '[i]n the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law'. The guarantees of Article 6 ECHR have been applied in a more stringent way in relation to criminal rather than civil charges[152] with a view to ensuring an effective and fair judicial process.[153] Considering the severity of fines which could be imposed as a result of GDPR cross-border investigations, those sanctions may be seen as criminal, and thus the requirements of Article 6 ECHR would apply to the procedures before the NSAs. The applicability of Article 6 ECHR to NSAs reinforces the case that procedural fairness guarantees should be granted in the context of the OSS mechanism. It can be seen therefore that by simply respecting the general principles of EU law, NSAs can bring about a substantial improvement in the enforcement of the GDPR.

The EDPB also has a role to play, in particular in ensuring the equality of NSAs in the consistency mechanism. For instance, in the *Twitter* case, the EDPB could have required further investigation to remedy gaps in the draft decision.[154] Docksey surmises that this was probably deemed impractical given that it would effectively have required the entire procedure to start from the beginning.[155] While undoubtedly true, more robust handling by the EDPB of these early experiences would have sent a strong signal to LSAs about expectations in the context of the consistency mechanism. The EDPB Guidelines require a LSA to 'seek consensus regarding the scope of the procedure (ie the aspects of data processing under scrutiny) prior to initiating the procedure formally'.[156] Where such consensus building is absent or inadequate, it is therefore for the EDPB to be firm in its response and to relaunch proceedings if necessary. While this might be inefficient in the short term, it may pay longer-term dividends. However, as shall now be discussed, it may be that where such changes on the part of NSAs and the EDPB are not forthcoming, more significant intervention is required. This might come in the form of a corrective role for the Commission or intervention from the EU Courts, again neither of which would require reform of the existing framework.

[150] The less severe infringements could result in a fine of up to €10 million, or 2 per cent of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.

[151] See art 52 of the EU Charter.

[152] D Slater, S Thomas and D Waelbroeck, 'Competition Law Proceedings before the European Commission and the Right to a Fair Trial: No Need for Reform?' (2008) <https://www.coleurope.eu/sites/default/files/research-paper/gclc_wp_04-08.pdf> 3.

[153] According to the so-called *Engel* criteria, a criminal charge exists in the presence of the following criteria: the classification of the offence under domestic law; the nature of the offence; and the nature and severity of the penalty. See Judgement of the ECtHR of 8 June 1976, *Engel and others v the Netherlands*.

[154] EDPB (n 58) para 39; EDPB (n 67) para 9.

[155] Docksey (n 64) 233–4.

[156] EDPB (n 67) para 28.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

B. A Corrective Role for the Commission

The European Commission, as guardian of the Treaties, is responsible for ensuring that Member States do not violate their Treaty obligations.[157] Accordingly, Member States can be held responsible for the activities of their organs falling foul of EU law, including the violation of EU case law.[158] More generally, the Commission should seek the effective enforcement of EU law, including Article 16 TFEU. During the GDPR legislative negotiations, the consequences of a failure to cooperate between NSAs was queried.[159] This is answered in the GDPR itself: recital 135 GDPR provides that the consistency mechanism 'should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties'. Failure to comply with GDPR obligations, like failure to comply with any EU legislative instrument, can therefore lead to infringement proceedings against the relevant Member State under Article 258 TFEU. If, for instance, a LSA consistently interpreted a procedural concept such as 'draft decision' or 'without undue delay' in a way that hindered the effective involvement of other NSAs in the cooperation procedure or in contravention of the EDPB Guidelines, the Commission could initiate an infringement action against the Member State concerned.

It might be asked what the threshold for the initiation of such a procedure would be, in particular in light of the independence of NSAs, and how effective it might be in practice. Two reflections are relevant in this regard. First, the infringement procedure is renowned for its 'dialogical' nature: before bringing a Member State before the EU Courts, the Commission will find avenues for compromise and political dialogue with the Member States.[160] The initiation of this dialogue with a Member State concerning its NSA may be sufficient to correct violations of the GDPR where the resolution sought is of a technical nature (for instance, the amendment of a national procedural rule providing an excessively short time limit to challenge an NSA decision). Secondly, by analogy with recent case law on the breach of judicial independence by the Polish authorities, the Commission may decide to prosecute one-off cases of breach of the OSS or consistency mechanism where their implications would be considered of a systemic nature.[161] The requirement of impartiality stemming both from Articles 41 and 47 of the Charter should receive special attention with reference to NSAs. A finding against the Member State may lead to the

[157] Art 17 TEU.

[158] Art 258 TFEU.

[159] Council of the EU, 'Note from Austrian delegation to Working Group on Information Exchange and Data Protection (DAPIX)', 5571/15, 8. It queried: 'What are the legal consequences of breaches of obligations to cooperate by any lead DPA or DPA concerned? What are the legal consequences of breaches of the obligation to bring a case before the European Data Protection Board …?'.

[160] See arts 258 and 260 TFEU. See P Craig and G de Búrca, 'Enforcement Actions Against Member States' in P Craig and G de Búrca (eds), *EU Law: Text, Cases and Materials* (7th edn, OUP 2020) 503.

[161] *Commission* v *Poland* (n 122).

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

imposition of penalties against the Member State.[162] Proceedings before national courts for *Francovich* damages for the violation of EU law by national authorities would further strengthen the enforcement of the GDPR.[163]

C. Intervention from the EU Courts

The EU Courts will also have a role to play should the current transnational enforcement challenges persist. Respect for the EU Charter of Fundamental Rights, and in particular relevant rights in the Citizens' Rights and Justice Chapters, should be central to the case law on the GDPR:[164] the Court of Justice should be 'proactive' in putting flesh on the bones of these fundamental rights in the context of the GDPR. The interpretation of the GDPR should be guided by these fundamental rights with a view to ensuring the effective enjoyment of the data protection rights, thus going beyond the mere respect of procedural requirements and rather focusing on the possibility for data subjects to be granted the full extent of their entitlements. Principles of good administration and due process should acquire a central importance as they are key to ensuring the procedural fairness necessary to enhance the legitimacy of and trust in public authorities and the law. For instance, any guidance from the Court of Justice on the extent to which Articles 41 and 47 EU Charter apply to NSAs and the EDPB would be welcome.

In addition, via the combined reading of recital 13 GDPR, Articles 61(1) GDPR, 4(3) TEU and 41 of the EU Charter it may be possible to challenge the violation of the principle of sincere cooperation in the context of the OSS mechanism.[165] It should be recalled that recital 13 GDPR and Article 61(1) GDPR both demand that NSAs engage in sincere cooperation. The sincere cooperation requirement also stems from the right of good administration protected under Article 41 of the EU Charter. Moreover, the principle of sincere cooperation is laid down in Article 4(3) TEU, which has general application regardless of the division of competences among the EU and the Member States.[166] Potential violations of this principle could be raised in the context of national judicial proceedings under Article 78 GDPR and brought to the attention of the CJEU via a preliminary ruling, or via direct actions against the EDPB's decisions before the EU judicature. As mentioned, they could also be the object of an infringement procedure.

The EU judicature should also consider developing a principle of equality among the NSAs. This would tackle the over-representation of the LSA. In this sense, the CJEU has a crucial role to play in levelling up the currently deficient due process guarantees provided under the OSS and the consistency

[162] Art 260 TFEU. [163] Case C-6/90 *Francovich and Bonifaci* v *Italy* EU:C:1991:428.
[164] Arts 41, 47, 48, 49 and 50 of the EU Charter of Fundamental Rights.
[165] *Facebook Ireland Ltd* (n 27) para 53, where the CJEU teased out the requirement of sincere cooperation laid down in the GDPR.
[166] M Klammert, *The Principle of Loyalty in EU Law* (OUP 2014) 18.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

mechanisms. Indeed, it has already started to delineate the content of procedural rights in its GDPR decisions.[167]

Advocate General Bobek opined that the Court may be ready to go further and place these challenging demands on its shoulders. He observed that should the legislature's choice in enacting the GDPR be undermined—should 'the child turn out bad'—then the Court would not 'turn a blind eye to any gap which might thereby emerge in the protection of fundamental rights guaranteed by the Charter and their effective enforcement by the competent regulators'.[168] He also hinted at the options available to the CJEU: interpreting the OSS and consistency mechanisms in conformity with the EU Charter; or assessing the validity of the mechanisms in light of the EU Charter. This serves as a shot across the bow for recalcitrant NSAs and the EDPB itself: should the GDPR cooperation and consistency mechanisms not function, alternative options will need to be made available. These alternatives shall be considered briefly.

D. Reform of the Existing Rules

In case reliance on general principles of EU law proves insufficient to enhance the substantive and procedural consistency of the GDPR, procedural harmonisation could occur via EU secondary measures. The ReNEUAL 2.0 principles on good administration may offer the starting point for drafting legislation on the procedures governing transnational cooperation under the GDPR. A principle-based framework may nevertheless be considered partial and not sufficiently defined to address the gaps in GDPR enforcement. Therefore, it is suggested that EU secondary rules would offer a more appropriate outlet for regulating the procedural rules and rights in the context of the OSS and the consistency mechanism. There are examples of similar procedural approximations in the field of competition law.[169] So far, approximation has occurred through the EDPB guidelines.[170] However, the absence of binding effects for those instruments may hinder their enforcement and, as noted above, the guidelines only pertain to the aspects of GDPR enforcement provided for explicitly by the GDPR.[171] Other elements of national administrative procedures fall outside their scope and may thus hinder smooth cooperation among NSAs.

A question to address in this context is that of the legal basis for the EU to adopt such procedural rules. Although Article 16(2) TFEU does not refer

[167] See Cases C-362/14 *Schrems* I EU:C:2015:650, C-311/18 *Facebook Ireland and Schrems* EU:C:2020:559, C-73/16 *Puškár* EU:C:2017:725.

[168] *Facebook Ireland Ltd*, Opinion of AG Bobek, (n 10) para 128.

[169] Commission Regulation (EC) No 773/2004 of 7 April 2004 relating to the conduct of proceedings by the Commission pursuant to Arts 81 and 82 of the EC Treaty (Text with EEA relevance) OJ L 123, 18–24.

[170] See eg EDPB Guidelines on Article 60 (n 39).

[171] See eg Case C-911/19 *FBF* EU:C:2021:599, where the EBA guidelines were found to be non-legally binding.

https://doi.org/10.1017/S0020589322000355 Published online by Cambridge University Press

explicitly to procedural rules, this Article could constitute the legal basis to introduce procedures aimed at protecting individual rights connected to data processing. Another possible legal basis is the harmonisation clause included in Article 114 TFEU.

While it is beyond the scope of the present contribution to identify the precise content of these rules and to assess the viability of this prospect in light of prior EU experience of procedural harmonisation, two points bear noting. First, in terms of the content of these rules, it is critical that they enable complainants to engage effectively in NSA proceedings concerning cross-border processing operations. Consumer organisation BEUC, for example, suggests that complainants should be able to intervene throughout the GDPR administrative procedures, including concerning the allocation of complaints, rather than only at the end when a decision is reached.[172] Secondly, the limited EU experience of procedural harmonisation suggests that such harmonisation can be politically sensitive. Yet should subsidiarity so dictate, the harmonisation could cover the procedures applicable domestically when the cooperation and consistency mechanisms are engaged. Such harmonisation should also consider whether pan-European procedures should be introduced when it comes to national proceedings before NSAs and courts in the field of data protection. The existence of harmonised procedures in these two fields would further achieve the objectives of uniform application of the GDPR framework. While, historically, EU law has played a limited role in determining how EU law should be applied, EU legislative instruments—even those without an explicit procedural dimension—increasingly incorporate procedural requirements, going well beyond the old formula of 'effective, dissuasive and proportionate' sanctions. The GDPR itself is a case in point.[173]

A further potential reform concerns the possibility for the EDPB to act as central authority for the handling of cross-border complaints. By attributing this competence to the EDPB, some of the current deficiencies of GDPR enforcement in transnational settings would be addressed. The enforcement model existing in the EU competition law field could be taken as an example. However, this possibility risks significant complications. First, the centralisation of GDPR enforcement in the hands of a European body may meet resistance from the Member States as the reform would remove a significant part of EU data protection from NSAs. The political consensus needed to amend the relevant aspects of the GDPR might therefore not be forthcoming. Furthermore, other stakeholders such as civil society organisations might also be wary of such a move: placing such enforcement

[172] BEUC (n 45) 14.

[173] cf with arts 17ff of Directive (EC) 2006/54 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation, OJ L 204/23.

power in the hands of a single entity may, for instance, leave it more vulnerable to regulatory capture. Finally, any potential attribution of competence to the EDPB for cross-border complaints could hinder the proximity principle, according to which data subjects should be able to address national authorities to raise a complaint under the GDPR. Such reform would therefore require careful consideration, lest by addressing existing procedural justice deficiencies new problems would be created.

V. CONCLUSIONS

The insufficient enforcement of the GDPR is, by now, well-documented, with the responsibility for this under-enforcement often attributed to specific NSAs. This article has mapped the shortcomings of the GDPR's transnational public enforcement mechanisms in a more systematic manner, for it is only by accurately diagnosing the problems that effective solutions can be identified. The analysis exposes flaws that go beyond the inadequacy of a single NSA, pointing instead to more fundamental constitutional challenges, including: a lack of explicit equality between NSAs to the detriment of the system's legitimacy; procedural fairness deficiencies to the detriment of the rights to data protection, privacy and due process; and the unequal application of the law to the detriment of the rule of law.

Do these flaws stem from the very design of the relevant mechanisms or might they be addressed by a change in approach by NSAs and the EDPB? What is apparent is that the missing element in the current enforcement of the GDPR is a truly cooperative, European culture in the field of data protection. The GDPR has not thus far fully supported the emancipation of data protection from national particularism and policies. The preponderance of a national dimension in the enforcement of the GDPR emerges powerfully when considering the pitfalls resulting from the current functioning of the OSS and consistency mechanisms. While the NSAs are bound by a duty of loyal cooperation, the exhortation to engage in this spirit has so far fallen on deaf ears. Whether a legal obligation of loyal cooperation would be any more effective in this context remains doubtful.

In this instance, it would fall to the EU Institutions to step in. The Commission could bring infringement proceedings against Member States whose NSAs act in a way which is not fully compliant with the GDPR, while the CJEU could tease out in its case law the requirements stemming from the EU Charter and further clarify the relevant due process requirements. Harmonisation of procedural norms and reforms of existing rules remains a last resort option.