


Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?

Filipe Brito Bastos* and Przemysław Pałka** 

*NOVA School of Law and CEDIS, Lisbon, Portugal, email: filipe.bastos@novalaw.unl.pt

**Jagiellonian University, Krakow, Poland, email: przemyslaw1.palka@uj.edu.pl (corresponding author)

Protection of personal data as a fundamental right – GDPR’s enforcement dilemma in cross-border cases – “One-stop-shop” model’s inadequacies highlighted – Distinction: regular cross-border enforcement versus cases of common European concern – Proposal: centralised enforcement mechanism for cases of common European concern – Union supervisory authority as a solution – Insufficiencies of the harmonisation proposal of the European Commission – Centralisation’s advantages: uniform enforcement, better coordination, and curbing forum shopping – Implications: fundamental rights protection and EU’s constitutional obligations – Constructive critique of the one-stop-shop model, not a dismissal – European constitutional law mandates effective data protection enforcement.

INTRODUCTION

The right to the protection of personal data is the only fundamental right in the Charter that specifically demands the setting up of specialised administrative authorities.¹ Hence, not only is the existence of the data protection supervisory agencies required by the EU’s constitutional law, but also their ability to effectively control the potential infringers is a matter of the data subjects’ fundamental rights. Conversely, if their institutional or

¹Art. 8(3) Charter, reading ‘Compliance with these rules shall be subject to control by an independent authority’.

European Constitutional Law Review, 19: 487–517, 2023

© The Author(s), 2023. Published by Cambridge University Press on behalf of the University of Amsterdam. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

doi:10.1017/S1574019623000202

procedural setup renders data protection authorities unable to effectively enforce the General Data Protection Regulation,² this presents not merely a problem of administrative underperformance but a deficit of protection of a fundamental right.

This article addresses the challenge of the General Data Protection Regulation's suboptimal enforcement in cross-border cases from the point of view of the EU's constitutional law. There is a growing consensus among personal data protection law experts that the status quo should be assessed negatively.³ The Regulation has been applicable since 25 May 2018,⁴ yet an average EU resident still has data about her activities shared with, or used by, advertising companies 376 times a day.⁵ Moreover, a substantial number of cross-border enforcement cases remain unresolved.⁶ We argue that this deficiency of fundamental rights protection stems from the specific oversight model adopted by the General Data Protection Regulation.⁷

The second section of this article begins by recalling the governance model of the General Data Protection Regulation and pointing out its shortcomings. Currently, enforcement of the Regulation is decentralised and lies solely in the hands of national supervisory authorities. For all cases of cross-border enforcement, the Regulation adopted the so-called 'one-stop-shop' model.⁸ Under that model, there is always one national authority – admittedly bound by a duty to cooperate with

²Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, or GDPR).

³See G. Gentile and O. Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR', 71 *International and Comparative Law Quarterly* (2022) p. 799; see also the European Data Protection Supervisor's Conference Report summarising the discussions of 'The future of data protection: Effective enforcement in the digital world' conference held in Brussels on 16-17 June 2022, p. 13-14, 20-21, 24-25, 27-28, 33-34, 53-54, 60-64, available at https://www.edpsconference2022.eu/sites/default/files/2022-11/22-11-10-EDPS-Conference-Report-2022_EN.pdf, visited 29 September 2023.

⁴Art. 99 GDPR.

⁵See Irish Council for Civil Liberties, 'The Biggest Data Breach: ICCL Report on the Scale of Real-Time Bidding Data Broadcasts in the US and Europe' (16 May 2022), p. 2, available at <https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/>, visited 29 September 2023.

⁶See Irish Council for Civil Liberties, 'Europe's Enforcement Paralysis: ICCL's 2021 Report on the Enforcement Capacity of Data Protection Authorities', p. 4, available at <https://www.iccl.ie/digital-data/2021-gdpr-report/>, visited 29 September 2023.

⁷See below, section titled 'The one-stop-shop and its drawbacks'.

⁸Recitals (127) and (128) GDPR.

others⁹ – competent to conduct the proceedings and issue a decision.¹⁰ In some cases, even if the model could be made more effective on the margins,¹¹ this is a valid choice. However, not all cross-border enforcement is the same. We propose to distinguish the regular cross-border enforcement of the General Data Protection Regulation from what we call the cases of common European concern.¹² The latter would comprise situations where an act of data processing puts in jeopardy the fundamental rights of the residents of the entire Union and, due to the high number of persons or jurisdictions involved, the significantly risky nature of processing at hand, or the complexity of the interpretative questions raised, cannot be effectively overseen by the national authorities acting within the one-stop-shop model. To ensure fundamental rights protection in such cases, we argue, the Union needs a different approach.

As the third section explains, we posit that the flaws resulting from the administrative structure of the one-stop-shop model, which are particularly severe in cases of common European concern, cannot be solved with the harmonisation of procedural provisions, as the European Commission has recently proposed. Instead, we argue, the EU should adopt a centralised enforcement model for the cases of common European concern and delegate their oversight to a newly empowered Union supervisory authority.¹³ Centralisation would tap into the unique institutional advantages of the Union administration by ensuring that the law is interpreted and enforced equally in all member states, and by preventing mishaps and delays resulting from poor coordination between national authorities. In addition, centralisation would curb the negative effects of forum shopping by the most notorious third-country data controllers, such as the influence of national enforcement strategies on the Union-wide case outcomes or the unfair distributive consequences of the one-stop-shop model.

As we argue in the fourth section, there are concrete implications to the fact that centralised enforcement might be the only viable option to effectively protect

⁹Arts. 60-63 GDPR.

¹⁰In some cases, subject to revision by the European Data Protection Board, *see* Arts. 63-67 GDPR.

¹¹*See* Gentile and Lynskey, *supra* n. 3, p. 823-828; *see also* the European Data Protection Board ‘Statement on Enforcement Cooperation’ adopted in Vienna on 28 April 2022, available at https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf, visited 29 September 2023.

¹²*See* below, section titled ‘Distinguishing the cases of common European concern’.

¹³This could mean either the creation of a whole new administrative agency or designating an already existing one – like the European Data Protection Supervisor or the European Data Protection Board – as the Union supervisory authority. For a discussion of various possibilities, *see* below, section titled ‘Centralisation, independence, and the limits to delegation’.

the fundamental rights of data subjects. Given the EU's positive obligations to protect the fundamental right to data protection, and given that the availability of an independent data protection authority constitutes part of that right, centralising enforcement for some cases is arguably not only a sound political choice but a move required by the EU's constitutional law.

Two caveats are in order. First, the proposal to create the Union supervisory authority solely competent to oversee the cases of common European concern should not be read as an attack on the one-stop-shop model altogether. The authors agree that, in many simple cross-border cases, this is the most effective approach, and refer to some ideas on how it could be improved without a general overhaul.¹⁴ Second, the idea to centralise the enforcement of the General Data Protection Regulation in (some) cross-border cases was timidly, though repeatedly, flagged by various speakers at the European Data Protection Supervisor's conference in June 2022.¹⁵ The authors do not claim the authorship of the idea. Rather, as a follow-up, they decided to scrutinise it from the point of view of European constitutional law, demonstrating how not only is such a development consistent with the Treaties but also, effectively, required by them.

THE ONE-STOP-SHOP AND ITS DRAWBACKS

The General Data Protection Regulation is the EU's horizontal regulation governing the processing of personal data of EU residents (data subjects) by both private and public actors (data controllers).¹⁶ It aims to, simultaneously, guarantee the protection of fundamental rights and facilitate the free movement of personal data within the EU.¹⁷ To this end, the General Data Protection Regulation obliges data controllers to abide by several principles,¹⁸ secure a legal basis for each act of processing,¹⁹ and fulfil numerous regulatory requirements,²⁰ while endowing data subjects with various rights.²¹ Albeit creating a complex system of substantive rules, the General Data Protection Regulation has been clearly and

¹⁴See below, section titled 'Harmonization of procedure?'

¹⁵See Conference Report, *supra* n. 3, p. 23, 25, 33, 37, 42, 56, 60-64, 69-71.

¹⁶Arts. 1(1), 2(1), 3(1)-(2) GDPR.

¹⁷*Ibid.*, Art. 1(2)-(3).

¹⁸*Ibid.*, Art. 5.

¹⁹*Ibid.*, Art. 6.

²⁰*Ibid.*, Arts. 7-9, 24-39, 44-49.

²¹*Ibid.*, Arts. 12-22.

succinctly presented in the scholarly literature.²² The enforcement of the Regulation is to be guaranteed by the national supervisory authorities.²³

There are three defining administrative features of the General Data Protection Regulation's current enforcement model: (i) its decentralised character; (ii) its cooperative character; and (iii) the dominant role it accords to the 'lead supervisory authority' in cases of cross-border data processing. First, regarding the decentralised character, enforcement is undertaken by a plurality of national supervisory authorities, each acting within the territory of its own member state.²⁴ Second, given the cooperative character of enforcement, the national authorities are required to mutually assist each other, e.g. by exchanging information or carrying out inspections on each other's behalf.²⁵

Further, third, under the General Data Protection Regulation's one-stop-shop system, the lead authority, i.e. the national authority 'of the main establishment or of the single establishment of the controller or processor', is solely competent to exercise supervisory powers over a controller.²⁶ Such powers are, however, exercised in consultation and cooperation with the national authorities from other member states whose residents are affected by the data processing in question (i.e. the 'concerned supervisory authorities').²⁷ While the lead authority enjoys exclusive power to decide whether to initiate investigations and to take decisions vis-à-vis controllers, it must also circulate draft decisions, e.g. imposing fines, to the concerned authorities. The role of the latter in that context is limited to raising 'relevant and reasoned objections' to the draft decision.²⁸ The lead authority is, however, not obliged to decide in accordance with such objections. It is only obliged to bring the matter to the European Data Protection Board (the Board) so that the Board may issue a binding decision to settle the specific points of disagreement between the lead and concerned authorities.²⁹ It should be emphasised that despite holding the power to take binding decisions – as it recently did in an investigation

²²See, e.g. N. Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law', 10 *Law, Innovation and Technology* (2018) p. 40; C.J. Hoofnagle et al., 'The European Union General Data Protection Regulation: What It Is and What It Means', 28 *Information & Communications Technology Law* (2019) p. 65; B. Petkova, 'Privacy as Europe's First Amendment', 25 *European Law Journal* (2019) p. 140; T. Streinz, 'The Evolution of European Data Law', in P. Craig and G. de Búrca (eds.), *The Evolution of EU Law*, 3rd edn. (Oxford University Press 2021) p. 902; K. Yeung and L.A. Bygrave, 'Demystifying the Modernized European Data Protection Regime: Cross-disciplinary Insights from Legal and Regulatory Governance Scholarship', 16 *Regulation & Governance* (2022) p. 137.

²³Arts. 51-59 GDPR.

²⁴Ibid., Arts. 51, 56, 57 and 58.

²⁵Ibid., Art. 61.

²⁶Ibid., Art. 56(1).

²⁷Ibid., Art. 60(1). See also ECJ 15 June 2021, Case C-645/19, *Facebook Ireland*, para. 53.

²⁸Art. 60(4) GDPR.

²⁹Ibid., Art. 65(1)(a).

concerning Meta³⁰ – the Board’s involvement does not represent any deviation from the fundamentally decentralised character of General Data Protection Regulation enforcement. Indeed, the Board’s intervention is not to enforce the General Data Protection Regulation as a Union supervisory authority but rather to assist its true enforcers, the national supervisory authorities. Crucially, national authorities are bound by the Board’s decisions, but the Board itself is bound by what the national authorities ask it to rule upon. It is always the lead supervisory authority requesting the Board for a decision that, by defining the scope of the disagreement between itself and the concerned authorities, effectively defines the extent of the Board’s role in the procedure.

As the one-stop-shop model of enforcement only applies in cases of cross-border processing of personal data, it is important to clarify what this notion entails. Cross-border processing occurs when a data controller established in one member state operates in several jurisdictions or when a controller established outside of the Union offers goods or services to the Union residents in several member states or monitors their behaviour.³¹ We illustrate this in the table below.

	Data controller established in a member state	Data controller established outside of the EU
Data controller processing data of residents of one member state	Purely national processing (case A)	National processing by a controller from outside of the EU (case B)
Data controller processing data of residents of several member states	Cross-border processing by a controller based in the EU (case C)	Cross-border processing by a controller from outside the EU (case D)

Hence, if a Romanian pizzeria serves consumers only in Romania, this is a case of purely national processing, and a Romanian authority will be competent to oversee its activities (case A). If a company from a third country, like Mexico, directs an app predominantly to residents of one member state, like Spain, it should establish a representative in Spain and will be overseen by the Spanish authority (case B).³² If a company based in a member state, like Sweden, offers a streaming service to residents of several member states, it will be monitored by the authority of the member state where it is based, i.e. the Swedish authority (case C).

³⁰See Decision *In the matter of Meta Platforms Ireland Ltd (previously known as Facebook Ireland Ltd)*, DPC Inquiry Reference: IN-20-8-1, dated 12 May 2023, https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf, visited 29 September 2023.

³¹Art. 3(2) GDPR.

³²See Article 29 Working Party, *Guidelines for Identifying a Controller or Processor’s Lead Supervisory Authority*, 16/EN WP 244 rev.01, adopted on 13 December 2016, as last revised and adopted on 5 April 2017, p. 3-5.

However, companies from third countries that offer their services throughout the Union (case D) pose entirely distinct problems. Data controllers established outside of the EU must designate a representative ‘in *one* of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are’.³³ Though this is a problem that the General Data Protection Regulation has attempted to solve, the provision makes it possible for controllers to forum shop for the national authorities that will be responsible for their supervision. Put differently, companies from third countries – paradigmatically, the US ‘Big Tech’ companies like Google, Meta, and Amazon but also corporations from China, offering services like TikTok – are free to choose their own supervisor quite liberally, for as long as they are able to demonstrate that decisions about processing are indeed taken in that jurisdiction.³⁴ This is what aggravates the problems raised by cases of common European concern.

The generic shortcomings of the one-stop-shop model

Admittedly, there might be many cross-border cases where the one-stop-shop model functions or could function well. For example, in its public-oriented communications,³⁵ the European Data Protection Board describes a situation where three residents of Italy believe their rights were violated by a data controller in Sweden and, thanks to the one-stop-shop, can lodge a complaint in Italian, with the Italian supervisory authority. Then, the authority can contact its counterpart in Sweden, who (as the lead authority) will investigate and determine whether the General Data Protection Regulation has, in fact, been infringed. This scenario, arguably, is a win-win-win situation for the data subjects (who can communicate, in their own language, with the authority familiar to them), supervisory authorities (who each investigate controllers located in their own jurisdiction), and data controllers (who communicate with only one supervisory authority, in their own language, following a familiar procedure).

However, the reality of enforcement is often far more complex. In fact, the one-stop-shop system has been widely criticised. In a powerful recent critique, Gentile and Lynskey have described the one-stop-shop model as ‘deficient by design’.³⁶ They contend that, despite containing the most comprehensive and stringent substantive rules in the world, the General Data Protection Regulation

³³Art. 27 GDPR (emphasis added, spelling original).

³⁴Article 29 Working Party *Guidelines*, *supra* n. 32, p. 7.

³⁵See the European Data Protection Board ‘One-Stop-Shop’ leaflet, 29 June 2021, available at https://edpb.europa.eu/our-work-tools/our-documents/one-stop-shop-leaflet_en, visited 29 September 2023.

³⁶See generally Gentile and Lynskey, *supra* n. 3.

also institutes an enforcement model that is ill-suited to ensure effective compliance with data protection law.³⁷

Though the Treaties contain no precise definition of what constitutes effective enforcement of EU law, one may infer one possible test from the Court's case law. Among others, effectiveness requires public authorities to resort to 'the least distortive means of achieving their policy objectives'.³⁸ One should, therefore, question whether the three defining administrative features of the General Data Protection Regulation cause, or are unable to prevent, distortion in achieving the objective of protecting 'fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'.³⁹ The four points of critique raised by Gentile and Lynskey, in fact, all concern precisely the three administrative features that we highlight – the decentralised structure of enforcement, its cooperative nature, and the dominant role of the lead authority.⁴⁰ Despite looming reforms in terms of enforcement, these four weaknesses are unlikely to be overcome anytime soon.

It is the decentralisation that enables the distortion of enforcement by national particularities, both in terms of applicable laws and in terms of political and economic contexts. One problem that Gentile and Lynskey point out concerns 'insufficient procedural fairness guarantees' that hamper the procedural rights of the parties to the proceedings and might even lead to the exclusion of some data subjects from the process.⁴¹ A second problem that Gentile and Lynskey note is that the 'preponderant influence of national, rather than European, priorities and regulatory approaches in the transnational [General Data Protection Regulation] enforcement by [national supervisory authorities]'⁴² might lead to divergent application of law depending on who the lead authority is. Ultimately, this threatens a basic tenant of the rule of law, i.e. equality before the law, as the data protection rights of individuals may enjoy vastly different levels of protection in different member states.

Another problem concerns the tension between decentralisation and the requirement that supervisory authorities cooperate. Due to 'procedural ambiguities and divergences in the cooperation procedure',⁴³ Gentile and Lynskey write, 'disparities between national procedural rules have become a

³⁷Ibid., p. 799.

³⁸See P. Nicolaidis and M. Geilmann, 'What is Effective Implementation of EU Law?', 19 *Maastricht Journal of European and Comparative Law* (2012) p. 383 at p. 398.

³⁹Art. 1(2) GDPR.

⁴⁰Note that, to better explain the overlap between our views and those of the two authors, we do not mention the four problems raised by Gentile and Lynskey in the original order.

⁴¹See Gentile and Lynskey, *supra* n. 3, p. 813.

⁴²Ibid., at p. 806.

⁴³Ibid., at p. 806.

source of friction and delay'.⁴⁴ Put differently, as is common in the EU's administrative system, the General Data Protection Regulation's administrative procedures represent 'incomplete' procedures.⁴⁵ The Regulation specifies only part of the decision-making procedures that the supervisory authorities must follow. In most instances, it is the relevant authority's national administrative law that will apply. As member states' laws differ, e.g. on the notion of 'draft decision', on the scope of procedural rights and on the timing for their exercise, the lead and concerned authorities involved in the same decision-making process grapple with the lack of a shared procedural framework. This generates legal uncertainty and makes it more unpredictable for data subjects to know whether and how their rights will be protected, which in turn may discourage taking steps to protect themselves.

Finally, Gentile and Lynskey identify the problems emerging from the dominant role of lead authorities. Given that they solely enjoy the prerogative in critical steps of enforcement procedures, e.g. in shaping initial inquiries into General Data Protection Regulation infringements, concerned authorities have only a limited ability to protect data subjects within their jurisdiction.⁴⁶ In July 2023, the European Commission published a proposal for a regulation meant to harmonise the procedural rules that national supervisory authorities should follow while enforcing the data protection law.⁴⁷ The regulation aims to improve cooperation and effectiveness of enforcement. As is elaborated below, the proposal represents a missed opportunity. It does not, in any way, call the one-stop-shop model into question. Despite some positive steps, the proposal does not completely resolve any of the model's fundamental weaknesses, such as those noted by Gentile and Lynskey; in fact, the proposal risks making some of them even worse. The reasons are elaborated on below in the section titled 'Harmonisation of procedure?', which considers procedural harmonisation as a potential strategy to improve the enforcement of the General Data Protection Regulation.

Distinguishing the cases of common European concern

The critique offered by Gentile and Lynskey is both novel and powerful. However, in our view, the gravity of the concerns raised and, thereby, the desirable solution

⁴⁴Ibid., at p. 807.

⁴⁵See D. Pretis, 'Procedimenti amministrativi nazionali e procedimenti amministrativi europei', in G. Falcon (ed.), *Il procedimento amministrativo nei diritti europei e nel diritto comunitario* (CEDAM 2008) p. 49, p. 68.

⁴⁶See Gentile and Lynskey, *supra* n. 3, p. 810.

⁴⁷Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679 (COM/2023/348 final) (henceforth, the Proposed Regulation).

to the one-stop-shop's 'deficiency by design' will not be the same in every case of cross-border enforcement. Arguably, the situation of the data subjects and the national authorities is very different in cases of simple, regular cross-border enforcement (when two or three authorities need to communicate regarding a straightforward matter) and in cases of complex, Union-wide proceedings (where essentially all the supervisory authorities are entitled to be 'concerned', and the decision to be made is controversial on substance).

For this reason, we propose to distinguish between the standard cases of cross-border enforcement and what we call the 'cases of common European concern'. How to distinguish them? The best way to explain what we mean by the cases of common European concern, and to see why the problems with the one-stop-shop are different in these cases than in standard cases of cross-border enforcement, is to compare paradigmatic examples of each.

First, let one imagine a model, simple case of cross-border enforcement. There might be a pizzeria in Hungary that serves customers just across the border in Austria and ends up using data collected for the purpose of performing the contract to send commercial communications to its former clients. A resident of Austria, who does not speak Hungarian, and might not know how to file a complaint in Hungary, can complain to the Austrian supervisory authority, which then contacts the Hungarian authority, which can investigate (including by collecting evidence within its own jurisdiction) and issue a decision. The matter at hand is rather simple (it involves minimal legal questions requiring interpretation and limited discretion) and concerns only one data subject, represented by one lead authority and one concerned authority.

Would such a case, given the limitations of the one-stop-shop, present a danger to the fundamental rights of the Austrian customers? It might. The lead authority might be slow to act; national enforcement strategies can deem such cases a low priority, different procedural rules might lead to misunderstandings, etc. There may be room for improving the law in ways that render the proceedings more effective. However, in our view, such simple, cross-border cases do not challenge the very concept of the one-stop-shop.

Second, let one consider a case recently making the headlines, namely that of the Irish supervisory authority fining Meta Inc (formerly Facebook Inc) €390m,⁴⁸ following a complaint brought by Max Schrems's organisation noyb on behalf of an Austrian and a Belgian user, for relying on the wrong legalising basis, namely the necessity for the performance of the contract, to process data for the purposes

⁴⁸See Decision *In the matter of Meta Platforms Ireland Ltd (previously known as Facebook Ireland Ltd)*, *supra* n. 30.

of personalised advertising.⁴⁹ Detailed press coverage allows one to learn a lot about the specifics of the case. It was filed in January 2019⁵⁰ (so it took four years to issue the first decision), and the Irish authority (acting as the lead authority since Facebook has its European establishment in Ireland) has been overruled by the European Data Protection Board through the Article 65 procedure.⁵¹ Initially, the Irish authority wanted to side with Facebook's interpretation (and find no General Data Protection Regulation violation), then it proposed a much lower fine (between €28m and 36m), only for the Board to take a completely different view.

This is an example of what we call a case of common European concern. First, even though it was filed by data subjects from two specific member states, its outcome affects the fundamental rights of all the millions of Union residents using Meta's products, like Facebook or Instagram, who reside in all member states. In this sense, every single supervisory authority has a title to act as a concerned authority; and if every authority in the Union is concerned, the entire Union is concerned. Second, the matter at hand involves a legal issue requiring complex interpretation open to good-faith disagreement. Though it constitutes a clear pro-privacy move, the Board's ultimate decision was not the only possible interpretation, as demonstrated by the draft decision of the Irish authority and Meta's definite willingness to appeal. In such cases, the divergence in national enforcement strategies, given the lead authority's privileged position, can negatively affect the fundamental rights of data subjects all across the Union. Third, Meta is a third-country data controller generating significant profit. Its business model has been forged in a non-European environment,⁵² and it specifically and with free will chose Ireland as its place of establishment. This presents a risk of home bias, given the possible convergence of interests between the controller (looking for a lenient authority) and the member state willing to attract companies of this nature.

Moving from these paradigmatic examples to a clear-cut legal test presents a challenge. In our view, though this might initially seem a circular definition, the

⁴⁹See noyb, 'Meta Prohibited from Use of Personal Data for Advertising' (4 January 2023), available at <https://noyb.eu/en/breaking-meta-prohibited-use-personal-data-advertising>, visited 29 September 2023.

⁵⁰See noyb, 'Forced Consent & Consent Bypass' (undated), available at <https://noyb.eu/en/project/forced-consent-dpas-austria-belgium-france-germany-and-ireland>, visited 29 September 2023.

⁵¹See European Data Protection Board, Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR) adopted on 13 April 2023.

⁵²For the differences in approach to personal data protection in the US, see P. Schwartz and D. Solove, 'Reconciling Personal Information in the United States and European Union', 102 *California Law Review* (2014) p. 877.

best way to understand the cases of common European concern is as cases in which the fundamental rights of the Union's residents, in the view of the central European supervisory authority (whose establishment we advocate), would be best protected at the Union level and not a national level within the one-stop-shop-model. Such an understanding contains a clear, albeit general, threshold for assessment (effectiveness of protection of fundamental rights) while leaving a significant amount of discretion to the central supervisory authority. Let us elaborate on why such an approach promises to be the most effective.

One could imagine the core of the specific legal test for distinguishing between regular cross-border cases and the cases of common European concern involving a combination of the following factors: (i) the number of member states and/or the Union residents whose fundamental rights are affected; (ii) the gravity of the threat to the fundamental rights; (iii) the complexity of the case which, if high, presents a risk that the one-stop-shop model would render the proceedings excessively long or invite the national enforcement priorities to significantly influence the outcome; (iv) the origin of the data controller. Admittedly, within this frame, several possible tests could be proposed. For example, one could imagine a simple test stating that if data processing concerns the residents in every member state, such a case is of common concern. However, this would risk being simultaneously over- and underinclusive. On the one hand, every single website collecting any personal data⁵³ Union-wide – regardless of the level of risk for fundamental rights – should be seen as of common concern. Suddenly, Cambridge University Press, politico.eu, chess.com, and a myriad of others, would have to be supervised centrally, even though the types of processing these controllers engage in are neither specifically risky nor present complicated interpretative questions. On the other hand, a start-up engaging in potentially very dangerous data processing, e.g. involving new applications of facial recognition – one that could, in the near future, put the rights of the entire Union's residents at risk – would not be considered of common concern as long as it limits its processing to just a handful of member states.

What defines the cases of common European concern is precisely the unpredictability of their nature and their systemic impact on fundamental rights. The private sector is creative and innovative, also in the ways in which data can be used or misused. For this reason, we posit, the central supervisory authority should have a default competence – e.g. cases that involve three-quarters of the member states, or at least ten million users in at least six member states, etc. – while retaining the ability to take over enforcement of cases it considers best protected on the Union level, and delegate back to the national authorities the

⁵³See N. Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law', *10 Law, Innovation and Technology* (2018) p. 40.

cases it considers best protected on the national level. The usefulness of this approach will become even more apparent when discussing the shortcomings of the one-stop-shop model in cases of common European concern.

The shortcomings of the one-stop-shop in cases of common European concern

The one-stop-shop model is decentralised, through and through, and applies indistinctly to any case involving cross-border data processing. Unlike in other areas of Union law, the enforcement of the General Data Protection Regulation does not require certain kinds of cases, i.e. those with Union-wide implications, to be overseen at the Union level. A comparison with competition law may prove illuminating. If a multinational IT company from a third country, like Google or TikTok, established its European branch in Czechia and later planned to merge with a large Union-based company in the same sector, then the merger would be considered a 'concentration with a Union dimension'.⁵⁴ Unless the impact of a merger is confined to a single member state, the European Commission acts as a 'one-stop shop' with the exclusive power to decide on whether the merger should be authorised.⁵⁵ In contrast, even if its operations affect the fundamental right to data protection of millions of residents in every EU member state, the same multinational IT company would be exclusively supervised by an altogether different 'one-stop-shop' – the Czech lead authority, albeit in cooperation with other concerned authorities. Controllers originating from third countries may pick a national authority to handle what are, in effect, Union-wide fundamental rights questions. Some key problems that emerge from cases of common European concern result from this setup. It will be conceded that data protection law is not the only field under Union law where firms are effectively 'clients' of administrative agencies, with the liberty to choose their own 'provider' authority.⁵⁶ In many decentralised networks similar to the General Data Protection Regulation's system, and depending on their goals, 'regulatees may exploit the opportunities resulting from multiple regulators' and select the best, the most sympathetic, or even the least efficient administration.⁵⁷

There are numerous examples of procedures similar to the General Data Protection Regulation's one-stop-shop model. The regulation of veterinary medicines is just one of many. When a company wishes to market a medicine

⁵⁴See Art. 1 of Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (hereinafter the Merger Regulation).

⁵⁵See Recital (8) Merger Regulation.

⁵⁶Cf B.G. Mattarella, 'Il rapporto autorità-libertà e il diritto amministrativo europeo', 4 *Rivista trimestrale di diritto pubblico* (2006) p. 909 at p. 919.

⁵⁷E. Chiti, 'The Governance of Compliance', in M. Cremona (ed.), *Compliance and the Enforcement of EU Law* (Oxford University Press 2012) p. 31 at p. 41-42.

in several member states, one of their respective national authorities will act as a 'reference' authority. That authority prepares an assessment report on the medicine and circulates it to the remaining authorities. If the remaining authorities do not raise any objections, the drug must be authorised in all the relevant member states. If they do, a new procedure is initiated to settle the disagreement and, if necessary, the European Commission itself will take the final decision.⁵⁸

However, decentralised regulatory networks such as this also present crucial differences from the General Data Protection Regulation's one-stop-shop model. First, while the reference authority competent to authorise a veterinary drug will be 'the competent authority in the member state chosen by the applicant',⁵⁹ the range of that choice is necessarily limited to one of the regulators of the member states where the medicine will actually be marketed, and where it may raise public health concerns. In contrast, the sole test under the General Data Protection Regulation (if the data controller processes data of residents of the entire Union) is the state where corporations have chosen to set up their own 'main establishment', i.e. where decisions about processing are made. Second, unlike pharmaceutical regulators, which regulate specific classes of products, lead authorities under the General Data Protection Regulation do not supervise specific services involving the processing of personal data but the entire data processing activity of a controller. Lastly, the very nature and purpose of administrative powers differ. In other domains, regulators' powers are predominantly preventive and aim at protecting from future harm certain public interests, such as public health, which are abstract interests rather than specific individual rights. Under the General Data Protection Regulation, the powers of supervisory authorities are predominantly reactive and aim at offering remedies to individuals whose fundamental rights have been infringed or at imposing corrective measures to put an end to infringements.

Put differently, the General Data Protection Regulation allows forum shopping in ways that simply do not exist in other regulatory regimes. In the cases of common European concern, the controller may artificially choose the regulator of a member state where only a small proportion of affected fundamental rights holders live. The controller's power to make that choice is no less than a power to decide which authority the controller would like to be sanctioned by, or to whose corrective powers it would like to be subject to, in case it ends up violating fundamental rights.

The fact that third-country multinationals may choose the jurisdiction in which they desire to be policed accentuates the weaknesses of the one-stop-shop

⁵⁸Arts. 49 and 54 of Regulation (EU) 2019/6 of the European Parliament and of the Council of 11 December 2018 on veterinary medicinal products and repealing Directive 2001/82/EC.

⁵⁹*Ibid.*, Art. 49.

model. The combination of decentralised enforcement and dominance of the lead authorities, on the one hand, with the ability to forum shop for a preferred supervisory authority, on the other, risks serious distortion to the aim of protecting data subjects' fundamental rights. Put differently, that combination structurally undermines the one-stop-shop to secure effectiveness in the enforcement of the General Data Protection Regulation.

It may be noted that three problems are specifically exacerbated in the cases of common European concern. The first is that the one-stop-shop compromises the principle of equality.⁶⁰ As such cases present a threat to the fundamental rights of individuals in every EU member state, they present, in fact, Union-wide threats to such rights which, to be effectively tackled, require a Union-wide response. However, the one-stop-shop leads to the fragmentation of enforcement into a multitude of national jurisdictions. This makes it possible for individuals located throughout the Union, faced with exactly the same threat to their fundamental rights, to be protected differently – or not at all – depending on the resolve or resources of their respective national authorities to defend their rights when objecting to lead authority's decisions that will profoundly affect them. This represents an obvious problem from the perspective of equal treatment of data subjects. Yet, the very fact that significantly different enforcement practices may exist throughout the Union also generates a problem from the perspective of the principle of legal certainty, another constitutional principle of Union law. According to the Court's case law, 'the principle of legal certainty requires that rules of law be clear and precise and predictable in their effect, so that interested parties can ascertain their position in situations and legal relationships governed by EU law'.⁶¹ Individuals may understandably feel discouraged from requesting the protection of their rights if they cannot anticipate how the General Data Protection Regulation will be enforced in the midst of a myriad of different national enforcement approaches.

Yet another problem in cases of common European concern emerges from the structural incentive to overburden certain national authorities. As companies in the same sector are unlikely to forum shop for wildly different reasons, the one-stop-shop makes it possible for cases of common European concern to accumulate in the hands of the same lead authorities. The freedom to forum shop embedded in the General Data Protection Regulation thus enables extensive backlogs. It is no secret that the extremely competitive Irish tax system, as well as the fact that Ireland is an English-speaking country where US-based law firms can be directly involved in compliance, have been some of the key motivations for giants such as

⁶⁰Art. 20 Charter.

⁶¹ECJ 3 December 2019, Case C-482/17, *Czech Republic v European Parliament and Council*, para. 148.

Google, Meta, Apple, Microsoft, Twitter and TikTok to choose the Irish authority.⁶² It should also be no surprise that, as of 2021, more than 97% of major General Data Protection Regulation cases referred to the Irish authority remained unresolved.⁶³ One could argue that such backlogs could be solved by drastically increasing the resources of the most challenged authorities so that they could enforce the Regulation more actively. To put things in perspective, the yearly budget of the Irish authority was €19.1m in 2021,⁶⁴ whereas Meta alone, in the same year, spent US\$9.8 billion on administrative and legal operations.⁶⁵ Yet, it is difficult to miss the deep redistributive dilemmas here. The lead authority in cross-border cases, of common concern or otherwise, also exercises its powers as a purely national authority, in purely national cases. Using its resources to supervise a flood of cases involving some of the most powerful companies in the world, to act as a *de facto* EU-wide regulator, necessarily means using fewer of that authority's resources to protect the fundamental rights of the member state's residents in purely national cases. The one-stop-shop, in short, is structurally vulnerable to the overburdening of the same lead authorities with the responsibility to deal with Union-wide threats to fundamental rights, to the detriment of more delimited threats originating in the territory of their own member state.

Finally, the one-stop-shop carries a serious risk of a domestic bias. This is close to the point made by Gentile and Lynskey, already alluded to above, that effective enforcement of the General Data Protection Regulation risks being hampered by a 'preponderant influence of national, rather than European, priorities'. Such a bias is not a phenomenon specific to the enforcement of data protection law. The absence of centralised enforcement in EU-wide issues often risks parochial business or political pressures distorting the Union's regulatory objectives. Prior to the Eurozone crisis, such pressures reflected in a pervasive problem of national banking supervisors proving excessively permissive with respect to national credit institutions considered 'national champions', which ended up harming financial stability in the EU.⁶⁶ Accusations of a similar bias have been levelled against the Irish authority, as suspicions mount that the Irish economy's reliance on Big Tech, and the Data

⁶²See for instance 'The Irish Times View on Corporate Tax Yield from Big Tech: A Risky Bet' (30 January 2022), available at <https://www.irishtimes.com/opinion/editorial/the-irish-times-view-on-corporate-tax-yield-from-big-tech-a-risky-bet-1.4789249>, visited 29 September 2023.

⁶³See Irish Council for Civil Liberties, *supra* n. 6, p. 4.

⁶⁴*Ibid.*, p. 9.

⁶⁵See 'Meta Reports Fourth Quarter and Full Year 2021 Results', available at <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx>, visited 29 September 2023.

⁶⁶E. Wymeersch, 'The European Banking Union, a First Analysis', *Financial Law Institute Working Paper Series* WP 2012-07, p. 2-3, available at <https://ssrn.com/abstract=2171785>, visited 29 September 2023.

Protection Commission's singularly Big Tech-friendly approach to enforcement, when compared to every remaining authority, might not be unrelated.⁶⁷

STRENGTHENING FUNDAMENTAL RIGHTS IN THE CASES OF COMMON EUROPEAN CONCERN

Given the enforcement deficits of the status quo under the General Data Protection Regulation, different proposals have been made to better address cross-border cases. The first proposed approach has been to enact EU legislation harmonising the rules governing the administrative procedures that the national supervisory authorities must follow while enforcing the Regulation. This is the approach favoured by the European Commission, which has recently proposed a regulation to harmonise provisions governing administrative procedures for the enforcement of the General Data Protection Regulation. A second proposed approach, however, was signalled repeatedly at the European Data Protection Supervisor's Conference in June 2022, a year prior to the publication of the Commission's Proposed Regulation. That proposal was to centralise the enforcement powers in some cases at the Union level. While both approaches have their merits, the first would likely leave many of the drawbacks discussed above unresolved – indeed, despite some positive steps, the Commission's Proposed Regulation may even worsen some of them. We discuss these two alternative approaches in the following sections.

Harmonisation of procedure?

In April 2022, the European Data Protection Board adopted a statement on cooperation between supervisory authorities on the enforcement of the General Data Protection Regulation.⁶⁸ The statement set out the Board's intention to 'identify a list of procedural aspects that could be further harmonised in EU law to maximise the positive impact of GDPR cooperation',⁶⁹ as such harmonisation 'could bridge differences in the [authorities'] conduct of (cross-border) proceedings to increase efficiency'.⁷⁰ This 'wish-list', as termed by the media,⁷¹ was sent to the

⁶⁷Ireland Frets as Criticism over Big Tech Links Goes Mainstream', *Politico.eu*, 16 December 2021, available at <https://www.politico.eu/article/ireland-frets-criticism-over-big-tech-links-goes-mainstream/>, visited 29 September 2023.

⁶⁸See Board Statement, *supra* n. 11.

⁶⁹*Ibid.*, p. 2.

⁷⁰*Ibid.*

⁷¹See 'EU's Data Protection Authorities Call for Streamlining of Procedural Aspects', *Euractiv*, 12 October 2022, available at <https://www.euractiv.com/section/data-protection/news/eus-data-protection-authorities-call-for-streamlining-of-procedural-aspects/>, visited 29 September 2023.

European Commission and published in October 2022.⁷² In a nutshell, the absence of clear common standards in administrative procedure was felt to ‘hinder the full effectiveness of the GDPR’s cooperation and consistency mechanism’.⁷³ The list covered matters ranging from the status and rights of complainants to amicable dispute settlement and deadlines for decisions to be taken.

The Commission took note. The Board’s ‘wish-list’ is reflected in the Commission’s proposal for the harmonisation of procedures in General Data Protection Regulation enforcement, which was published in July 2023.⁷⁴

In essence, the Proposed Regulation pursues three aims.⁷⁵ The first is to clarify the legal position of complainants. To this end, among others, the Proposed Regulation establishes uniform formal requirements for complaints, sets out complainants’ procedural rights, including the right to be heard, and regulates the possibility of amicable settlements between complainants and the parties subject to investigation. The second aim is to strengthen and standardise the procedural rights of parties under investigation. To that end, the Proposed Regulation introduces common provisions, e.g. on the right of said parties to access the administrative case file concerning the investigation. The third aim is to reinforce the cooperation between the lead authority and concerned authorities. To that end, the Proposed Regulation regulates with greater detail and clarity aspects relating to the earlier stages of the investigation, including the possibility for an urgent decision by the Board to settle disputes concerning the scope of the investigation in complaint-based cases.⁷⁶

An effort to harmonise procedural rules, such as the one embodied by the Proposed Regulation, has several advantages. From a political standpoint, harmonisation is consistent with recent efforts of the EU legislator – for instance, in the reformed European Competition Network⁷⁷ – to ensure uniformity of Union law by standardising enforcement powers of national authorities rather than, more controversially, centralising such powers in the Union administration. From a practical standpoint, harmonisation avoids reopening the General Data Protection Regulation for reform, which the Board itself considers ‘premature’,⁷⁸ or overhauling

⁷²European Data Protection Board Letter of 10 October 2022, available at https://edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf, visited 29 September 2023.

⁷³Ibid., p. 1.

⁷⁴Proposed Regulation, *supra* n. 47.

⁷⁵See the Proposed Regulation’s Explanatory Memorandum, at p. 2-4.

⁷⁶Art. 10(6) Proposed Regulation.

⁷⁷Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market.

⁷⁸Ibid.

the Regulation's system of cooperative decentralised enforcement. Lastly, harmonisation can doubtless serve as a useful tool to remedy many of the discrepancies between national practices that hamper adequate cooperation and hence the enforcement of Union law.

The Proposed Regulation certainly displays such advantages. It also takes several positive steps that are likely to improve cooperation and procedural protection under the one-stop-shop mechanism. And yet, the Proposed Regulation falls short of remedying the fundamental weaknesses of the one-stop-shop model – particularly so in terms of the weaknesses that become apparent in cases of common European concern.

First, in terms of procedural rights, there is no doubt that the Proposed Regulation clarifies several issues and generates some uniformity in the protection of procedural rights throughout the Union. For instance, the Proposed Regulation regulates the timing of the exercise of the right to be heard by lead supervisory authorities and the Board⁷⁹ or the scope of the contents that must be available to parties under investigation who exercise their right of access to the case file.⁸⁰ One particularly positive step is that complainants will enjoy the right to be heard without distinction as to whether their interests are personally impacted by decisions to reject a complaint (i.e. civil society actors representing data subjects have the right to be heard in the same terms as a data subject who filed a complaint to obtain a remedy).⁸¹ This is by no means a given, as the Charter and the European Court of Justice's case law only entitle a person to be heard before a decision 'which would *affect* him or her *adversely* is taken'.⁸²

And yet, it is striking how the procedural rights of parties under investigation, and especially of complainants, are placed at the discretion – at the goodwill – of lead supervisory authorities. Complainants, for example, will enjoy the right to access administrative case files but only if the lead supervisory authority '*considers* that it is *necessary*' (emphasis added) to share documents contained in them for complainants to be able to make their views known effectively.⁸³ A lead authority that revises a draft decision after receiving other authorities' objections will be required to observe the right to be heard. That is, of course, if the lead authority decides that a hearing is convenient – when, according to the Proposed

⁷⁹Arts. 11, 14, 15 and 17 Proposed Regulation.

⁸⁰*Ibid.*, Art. 19.

⁸¹*Ibid.*, Art. 11.

⁸²See Art. 41(2)(a) Charter. One should note that, even though the Art. 41 Charter itself does not apply to national administrative procedures, the ECJ has made it clear that the rights enshrined in it constitute general principles of law that must be respected by Union as well as national authorities: see ECJ 24 November 2020, Joined Cases C-225/19 and C-226/19, *R.N.N.S.*, at paras. 33-34 (emphasis added).

⁸³Art. 15(3) of the Proposed Regulation.

Regulation, it ‘*considers that the revised draft decision . . . raises elements on which the parties under investigation should have the opportunity to make their views known*’ (emphasis added).⁸⁴ Moreover, in the absence of any minimum delay, the Proposed Regulation will give the lead authority full discretion to define the time limit within which complainants and parties under investigation may state their views, which is inadequate to ensure sufficient time for them to prepare their case.⁸⁵

Second, one must acknowledge that the Proposed Regulation contains some common, pre-established standards that are likely to generate legal certainty for individuals, firms, and supervisory authorities themselves. And yet, no harmonisation can ever be so extensive as to entirely remove discrepancies between national rules which inevitably hinder effective cooperation. Indeed, administrative procedures not only involve rules about the procedural rights of complainants, the handling of complaints, amicable settlement, the scope of case files, or the calculation of deadlines – all of which are included in the Proposed Regulation and certainly represent a useful step towards greater effectiveness of General Data Protection Regulation enforcement – for authorities involved in (simpler) cross-border cases.⁸⁶ Administrative procedures also involve detailed rules on issues as diverse as quorum, conflicts of interest, preparation of decisions, the burden of proof, the internal distribution of caseload or cooperation with authorities operating in distinct sectors. No provisions on these issues appear in the Proposed Regulation. Moreover, administrative procedures involve the use of legal concepts, such as ‘resolved case’, ‘draft decision’, or ‘interested party’, that are occasionally defined in the legislation but usually are only a matter of national doctrinal consensus.⁸⁷ The Proposal only covers discrepancies in procedural rules and legal concepts that have proven detrimental to General Data Protection Regulation enforcement *thus far* – only five years since such enforcement began. One simply cannot anticipate the number or severity of other discrepancies that might only become visible in the future. Suffice it to give one simple example. The Proposed Regulation clarifies that the complainant must be informed of the judicial remedies available to him or her when a supervisory authority decides to fully or partially reject a complaint.⁸⁸ Yet the appropriate judicial remedies may differ significantly between member states when the administration refuses a request to make a decision. Remedies may range from judicial annulment of the

⁸⁴Ibid., Art. 17(1).

⁸⁵Ibid., Arts. 12 and 17(2).

⁸⁶Ibid., Arts. 4, 5, 11, 13, 19 and 29.

⁸⁷This kind of concept has raised significant practical problems in the enforcement of the GDPR: see Gentile and Lynskey, *supra* n. 3, at p. 806-808.

⁸⁸Art. 13 Proposed Regulation.

refusal decision to judicial injunctions for the administration to decide as requested.

To the best of our knowledge, no piece of Union sectoral legislation exists that exhaustively regulates every aspect of national administrative procedures. Moreover, it should be recalled that the Union's competences in harmonising national administrative procedures are limited. Such competences may only be strictly accessory to the substantive harmonisation of the policy fields they address (e.g. harmonising rules for the marketing of medicines may involve not only uniform safety requirements but also uniform licensing procedures). The further harmonisation goes, the more it verges on the complete replacement of administrative procedural laws (at least in one policy field). Such harmonisation would lack any legal basis. Article 197 TFEU, though providing that effective enforcement is a matter of common interest to the member states, explicitly rules out harmonisation legislation; Article 298 authorises the Union to legislate general procedural provisions but only to regulate procedures of the Union's own administration.⁸⁹

Lastly, even if the Proposed Regulation somewhat patches up the General Data Protection Regulation's gaps in procedural protection or generates a degree of similarity in national legal standards, it is unable to solve other deficiencies that necessarily arise from the one-stop-shop model. These deficiencies lie in how the model's structural administrative features – decentralised governance and dominance of the lead supervisory authority – lead to the unequal treatment of data subjects, forum shopping, the overburdening and over-empowering of the lead supervisory authority, and risks of domestic bias.

None of these problems can be remedied by simply establishing common procedural provisions. All of them lead to the failure of the General Data Protection Regulation's enforcement model in cases of common European concern. In fact, despite some likely benefits in simpler cross-border cases, the Proposed Regulation not only fails to recognise that large, systemic, serious cross-border cases need a different approach to enforcement, it also even appears to worsen some of the one-stop-shop's shortcomings that it aims to improve.

The Proposed Regulation intends to strengthen the influence of all concerned supervisory authorities in cross-border enforcement procedures.⁹⁰ Ensuring that they are informed and can comment on the initial stages of investigations is certainly a useful step. However, the overall dominance of lead supervisory authorities is not only not mitigated, but indeed entrenched. First, the much-vaunted protection of procedural rights will, as explained above, remain a matter

⁸⁹For many, see J. Schwarze, 'European Administrative Law in the Light of the Treaty of Lisbon', 18 *European Public* (2012) p. 285.

⁹⁰See Recital (12) Proposed Regulation.

for the lead authority's discretionary prerogatives after all. Second, the concerned authorities' relevant and reasoned objections are significantly more restricted in their scope in comparison to how they are framed in the General Data Protection Regulation. For instance, concerned authorities may only relate their objections to factual elements already contained in the draft decision – i.e. they may not object by adding factual elements of their own – and they may not change the scope of the allegations in the lead authority's investigation by raising points amounting to the identification of additional allegations.⁹¹ The Proposed Regulation's Explanatory Memorandum even states that the mechanism of objections is to be used only 'sparingly'.⁹² Lastly, despite providing that the Board will enjoy the power to issue an urgent binding decision in cases where national authorities disagree on the scope of an investigation, the Proposed Regulation significantly restricts that power. The Board can only exercise that power in investigation proceedings initiated with complaints, and – at least according to the Preamble – it may not do so to expand the scope of an investigation on its own initiative.⁹³

The case for centralisation

Alongside procedural harmonisation, a second possible remedy has been proposed to mend the one-stop-shop model. The remedy was suggested repeatedly at the 2022 European Data Protection Supervisor's conference on the topic of enforcement and concerns the option of centralising enforcement. It was even mentioned in the speech made by the European Data Protection Supervisor himself, who advocated for a 'pan-European model' of enforcement.⁹⁴

Centralised enforcement would mean that *some* cases of cross-border data processing – those that we here designate as cases of common European concern – would be removed from the scope of the existing one-stop-shop model and would thus not be supervised by national lead authorities, in consultation with concerned authorities. Such cases would rather be exclusively handled by a Union authority (newly created or designated from within the existing ones, like the European Data Protection Board or the European Data Protection Supervisor). For example, an Irish university processing students' and employees' data would still be supervised by the Irish national authority, while a social media platform

⁹¹Ibid., Art. 18.

⁹²This limitation stems from the Commission's concern that a swift resolution of the administrative procedure is necessary to provide data subjects with a remedy. *See* Recital (28) Proposed Regulation.

⁹³Recital (16) Proposed Regulation.

⁹⁴W. Wiewiórowski, 'EDPS Speech at the "Future of Data Protection: Effective Enforcement in the Digital World" Conference, 16 & 17 June 2022', available at https://edps.europa.eu/system/files/2022-06/2022-06-17-edps-conference-speech_en.pdf, visited 29 September 2023.

like Facebook, targeting all the residents of the Union, would be supervised not by the Irish authority but by the – newly empowered – central authority.

Centralising the enforcement of data protection law can tap into the unique institutional advantages of the Union administration. As Zgliniski explains, ‘different institutions are good at making different kinds of decisions [so that] when allocating the authority to decide it is crucial that we take these relative strengths and weaknesses into account’.⁹⁵ The institutional advantages of the Union administration prove especially relevant in the enforcement of data protection law to address the failures of the one-stop-shop in cases of common European concern.

Centralised enforcement is better at ensuring that Union law is interpreted and enforced equally throughout the Union. Unlike national authorities,⁹⁶ the Union administration’s jurisdiction is not confined by member states’ borders and instead covers the sum of their territories. This minimises the risk of different national enforcement strategies influencing the decisions and thereby presenting the threat of unequal treatment of the citizens of the Union.

Centralised enforcement prevents mishaps and delays that often result from poor coordination between authorities in decentralised enforcement models. This was one of the reasons why the regulation of financial markets shifted towards a more centralised model, with the European Supervisory Authorities playing a powerful, albeit subsidiary, role. Indeed, the recitals of the regulation instituting the European Security and Markets Authority, when justifying its creation, bear striking resemblance to the criticism of the one-stop-shop model under the General Data Protection Regulation. The regulation intended to remedy a status quo ‘where there is insufficient cooperation and information exchange between national supervisors’ and ‘where joint action by national authorities requires complicated arrangements to take account of the patchwork of regulatory and supervisory requirements’.⁹⁷

⁹⁵See J. Zgliniski, *Europe’s Passive Virtues: Deference to National Authorities in EU Free Movement Law* (Oxford University Press 2020) p. 162.

⁹⁶For a recent example, see the *Facebook Ireland* ruling, *supra* n. 27, at paras. 47 and 77. The principle of territoriality has shaped the powers of data protection authorities even since before the GDPR. See ECJ 1 October 2015, Case C-230/14, *Weltimmo*, ECLI:EU:C:2015:639, paras. 50 and 56, where the ECJ stated that the territorial legal limits of national authorities’ powers derive from the ‘territorial sovereignty’ of the member states.

⁹⁷Regulation (EU) No. 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), Recital (8).

CONSTITUTIONAL FRAMEWORK FOR THE CENTRALISATION OF THE GENERAL DATA PROTECTION REGULATION'S ENFORCEMENT

In most areas of the law, centralised enforcement is simply a matter of political debate as to its advantages and, ultimately, of political choice. We submit, however, that the administrative enforcement of data protection law is constitutionally distinctive from other policy areas.

Article 16 TFEU, the legal basis for the General Data Protection Regulation,⁹⁸ as well as Article 8 of the Charter, listing the components of the fundamental right to data protection, state that 'compliance' with rules concerning data subjects' rights 'shall be subject to the control of independent authorities'. Both provisions imply that, if it constitutes the only viable solution to ensure effective 'control', centralising enforcement in data protection is not merely desirable, but constitutionally required. They further imply that, because it must be ensured by 'independent' authorities, effective enforcement cannot be entrusted to one of the bodies qualified in the Treaties as EU institutions, like the European Commission. Instead, it must be entrusted to a Union agency – a Union body created by secondary legislation – in terms that necessarily derogate from the constitutional limitations on the delegation of vast powers to Union agencies that apply in any other policy areas. The two points are elaborated upon below.

Centralisation and the ability to effectively 'control'

Remarkably, the right to the protection of personal data is the *only* fundamental right in the Charter that specifically demands the setting up of specialised administrative authorities. Article 8 requires data protection rights to be 'subject to control' by supervisory authorities.⁹⁹ The very existence of such authorities, the Court stresses, constitutes 'an essential component of the protection of individuals with regard to the processing of personal data' – such authorities are 'the guardians of those fundamental rights and freedoms'.¹⁰⁰ Accordingly, given that it is 'intended to ensure the effectiveness and reliability of the monitoring of

⁹⁸See the Preamble to the GDPR.

⁹⁹Indeed, some fundamental rights commentators list the existence of such authorities as constitutive of the right to the protection of personal data, alongside substantive principles such as purpose limitation or fairness. See M. Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU's Constitutional Reasoning', 20 *German Law Journal* (2019) p. 864 at p. 880-881.

¹⁰⁰ECJ 9 March 2010, Case C-518/07, *European Commission v Federal Republic of Germany*, at paras. 22-23.

compliance’, the guarantee of an independent supervisory authority ‘must be interpreted in the light of that aim’.¹⁰¹

The effectiveness of data protection authorities’ powers is, therefore, inextricably linked with the effectiveness of the right to data protection itself. If the supervisory authorities tasked with ‘control’ of compliance with data protection rights lack adequate means to actually fulfil that task – i.e. if the administrative governance of data protection is structurally unable to ensure the effectiveness of those rights – that represents a problem of far more than mere administrative underperformance. It is a problem of a deficit of protection of a fundamental right. It is a violation of a fundamental right by omission rather than by contravention.

Fundamental rights do not merely impose negative obligations – i.e. a prohibition for public authorities, such as Union agencies or national legislatures, to act in a manner that disturbs or harms said rights. Fundamental rights also impose positive obligations, or ‘duties to protect’ (*Schutzpflichten*), i.e. a command to actively take the measures necessary for the right of an individual to be effectively protected against other individuals or companies. The right to life does not simply prohibit the state from killing an individual; it also requires the state to effectively safeguard human life, including preventing, investigating and sanctioning murder.¹⁰² The existence of such positive obligations has been recognised by the Court, e.g. in the context of general and indiscriminate retention of traffic and location data to prevent, investigate and prosecute criminal offences, when balancing the need to protect the physical and mental integrity of individuals, or the rights of minors, with the rights to privacy and inviolability of communications.¹⁰³

Positive obligations are especially important in scenarios where an uneven balance of power exists between private parties. In such cases, the state is under a duty to legislate in such a manner as to protect, e.g. the rights of an employee vis-à-vis the employer.¹⁰⁴ The right of individuals to data protection is another prime example of a fundamental right commonly violated by other private parties in respect of whom they find themselves vulnerable, namely data controllers.

The positive obligations attached to the fundamental right to data protection are not only found in Article 8 of the Charter¹⁰⁵ but in Article 16 TFEU, which

¹⁰¹ECJ 26 July 2017, Opinion 1/15, para. 229.

¹⁰²See ECtHR 14 June 2011, No. 19776/04, *Ciechońska v Poland* and 17 July 2014, 47848/08, *Centre for Legal Resources and Câmpeanu v Romania*.

¹⁰³ECJ 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, at para. 126 ff. and 5 April 2022, Case C-140/20, *G.D.*, at paras. 49-50.

¹⁰⁴See Opinion of AG Trstenjak of 8 September 2011, in Case C-282/10, *Dominguez*, at paras. 86 and 118.

¹⁰⁵It should be recalled that, according to Art. 51(1) of the Charter, the Charter cannot, as such, form the legal basis for Union competences.

unequivocally creates a competence for the Union legislature to regulate and protect that right. In fact, the basic content of such obligations is plain. Article 16 includes, among others, the requirement addressed to the Union legislature that it creates, or ensures that the member states create, independent supervisory authorities. Article 16 TFEU (and Article 8 of the Charter) entail a requirement, addressed to supervisory authorities, that they ensure compliance with data protection rights. If one takes the general interpretive criterion of *effet utile* seriously – ‘the principle that provisions of EU law should be given full effect, practical effect, or their useful effect’¹⁰⁶ – then Article 16 must also imply a requirement, addressed to the Union legislature, that supervisory authorities, by their legal powers, procedures and institutional setup, have a real ability to ensure effective compliance.

It has been suggested that, when establishing whether positive fundamental rights obligations are complied with, the Court could draw inspiration from the case law of the European Court of Human Rights. The Strasbourg Court accords states with a broad margin of appreciation, i.e. of discretion when choosing the concrete means to the end of protecting fundamental rights.¹⁰⁷ Indeed, this should also be the approach when establishing what measures the Union legislature could take to ensure the protection of personal data.

However, if in certain categories of cases only centralised enforcement can ensure the effectiveness of such protection, then the margin of discretion of the Union concerns not whether it may choose to centralise, but how it may choose to centralise. If the one-stop-shop enforcement system is inherently flawed in the cases of the common European concern because of its decentralised structure, then the political discretion of the Union legislature is only circumscribed to a choice between potential alternative models of centralised enforcement that are fit for the purpose of data protection.

Centralisation, independence, and the limits to delegation

Unlike with other administrative authorities, the Union Treaties are uniquely specific as to the institutional characteristics that data protection authorities must have. Under Article 8(3) of the Charter and Article 16 TFEU, these supervisory authorities are required not only to effectively ‘control compliance’ but also to be

¹⁰⁶G. Beck, *The Legal Reasoning of the Court of Justice of the EU* (Hart Publishing 2012) p. 210-211. For an example in the case law, see ECJ 7 March 2018, Case C-31/17, *Cristal Union*, ECLI:EU:C:2018:168, para. 41.

¹⁰⁷See M. Beijer, ‘Active Guidance of Fundamental Rights Protection by the Court of Justice of the European Union: Exploring the Possibilities of a Positive Obligations Doctrine’, 8 *Review of European Administrative Law* (2015) p. 127 and M. Klatt, ‘Positive Obligations under the European Convention on Human Rights’, 71 *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* (2011) p. 691.

‘independent’. Two fundamental conclusions follow from the two requirements. First, as none of the Union Institutions established in the Treaties – such as the Commission or the Council – qualify as ‘independent’, centralised enforcement must fall to a Union authority established in secondary legislation. Second, and crucially, the two requirements combined imply that the powers of a Union-level supervisory authority derogate from the general constitutional limitations to the extent of Union agencies’ power – namely, the *Meroni* doctrine.¹⁰⁸

Regarding ‘independence’, when establishing the central supervisory authority, the Union must ensure that it is free from external or political pressure but retains liberty as to how to guarantee that. In practice, this could mean either the creation of an entirely new agency, or delegation of the new powers to one of the existing authorities, like the European Data Protection Supervisor or the European Data Protection Board. Constitutionally, each of these choices seems of equal validity. However, one should ponder whether the protection of fundamental rights would be better served by the doubling of enforcers (as the creation of a completely new one would entail) or rather by tapping into the already existing expertise of the Board or the Supervisor.

Such assessments remain beyond the scope of our argument; however, we suggest that they must be taken into account when establishing the Union’s central supervisory authority. In any event, one must point out that centralised enforcement for cases of common European concern, in parallel with decentralised enforcement in the remaining cases, does not compromise the independence of the supervisory authorities at either level. The supervisor is designated and operates separately from any other body, national or European. The Board is composed of representatives of all national data protection authorities, and its decisions already reflect deliberation by consensus rather than by the dominance of individual authorities. The Board’s independence is reinforced by the independence of the data protection authorities (much as the independence of the European Central Bank is reinforced by the independence of national central banks). Lastly, the independence of national data protection authorities may even be reinforced by centralised enforcement. As the General Data Protection Regulation recognises, the sufficiency of ‘human, technical and financial resources’ is a vital prerequisite for data protection authorities to function in an independent fashion.¹⁰⁹ By transferring jurisdiction over large, European cases from national authorities to a Union authority, the former can free up resources that they can use in smaller domestic or moderately cross-border cases.

¹⁰⁸ECJ 13 June 1958, Case 9/56, *Meroni*. On the constitutional boundaries that the *Meroni* doctrine sets for the empowerment of Union agencies, see generally M. Chamon, *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration* (Oxford University Press 2016) Chapter IV.

¹⁰⁹See Art. 52(4) GDPR.

Regarding the limitations of the Union's agencies' power, the matter seems constitutionally more nuanced. At its core, *Meroni* aims to preserve the powers of Union institutions and the balance that the Treaties establish between them. As Union agencies are typically not mentioned in the Treaties, *Meroni* bans the granting to Union agencies of powers implying such a 'wide margin of discretion' that it would bring about 'a transfer of responsibility' from the Union legislator to a Union agency.¹¹⁰ Crucially, however, the *Meroni* limits apply to 'cases where autonomous powers have been conferred on an Agency by the EU legislature'.¹¹¹ The Court has, for instance, denied the Single Resolution Board to have been granted 'autonomous powers', given that its measures required the assent of the Council and the Commission.¹¹²

Presumably, if it were to act as effectively as its national counterparts, a Union data protection authority would require powers similar to those currently enjoyed by national supervisory authorities. Many such powers involve a broad margin of discretion – a margin of autonomy to assess, on a case-by-case basis, what decisions and choices most adequately serve the policy objectives of data protection law. Supervisory authorities exercise discretion, for example, when they 'order the controller or processor to bring processing operations into compliance with the provisions of [the General Data Protection Regulation], where appropriate, in a specified manner and within a specified period'.¹¹³

Nevertheless, *Meroni* does not forbid equally broad discretionary powers from being delegated to a Union data protection authority. First, even though the *Meroni* limits have traditionally been subject to a rather conservative reading, as banning any delegation of discretion, more recent literature has demonstrated that it allows some degree of administrative discretion, i.e. a margin of autonomy in deciding how to implement policy choices, as opposed to making such choices.¹¹⁴ How broad that margin may exactly be, and how the line between political and administrative discretion can be drawn, remains to be established.

¹¹⁰ECJ 22 January 2014, Case C-270/12, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union (ESMA)*, at para. 42.

¹¹¹GC 1 June 2022, Case T-510/17, *Del Valle*, para. 208.

¹¹²*Ibid.*, para. 219.

¹¹³Art. 58(2)(d) GDPR.

¹¹⁴Some consider that the *ESMA* ruling, while not explicitly abandoning *Meroni*, constitutes a new delegation doctrine: M. Scholten and M. van Rijsbergen, 15 *German Law Journal* (2014) p. 1223 at p. 1249-1250. Others consider that the *ESMA* ruling simply proved what had been a possible interpretation of *Meroni* all along – that the Union may institute agencies which exercise a margin of administrative discretion, i.e. a margin of choice in how to implement policy priorities, as opposed to political and legislative discretion, i.e. a margin of choice as to what said priorities should be: see M. Simoncini, *Administrative Regulation Beyond the Non-Delegation Doctrine* (Hart Publishing 2018).

Second, and more importantly, we submit that delegation of administrative decision-making powers to a Union supervisory simply does not come under the scope of the *Meroni* doctrine. The very rationale for the doctrine, i.e. preventing a ‘transfer of responsibility’ away from Union institutions to the benefit of authorities absent from the Treaties, does not apply. Article 16(2) TFEU does foresee the existence of ‘independent authorities’ devoted to the ‘control’ of compliance data subjects’ rights. On the one hand, the provision means that, unlike Union agencies in other policy areas, the legislative creation of a specialised Union-level authority is not only mentioned, not only allowed, but indeed required by the Treaties. The constitutional status of a Union authority is thus less like agencies that were birthed by purely legislative choice and more like the European Central Bank. It is true that the Treaties directly create the European Central Bank, whereas they simply require the creation of a Union data protection authority. Yet both authorities are similar in that the Treaties do foresee their existence, independence from other actors, and intended mandate. Precisely because the Treaties provide that it may be vested with ‘specific tasks’ of banking supervision (Article 127(6) TFEU), the European Central Bank was, within the Single Supervisory Mechanism, endowed with extensive and independently exercised discretionary powers of a sort which would have been constitutionally impossible with agencies like the Single Resolution Board.¹¹⁵ Similarly, precisely because its mandate and independence from other authorities are foreseen in the Treaties, a Union-level data protection authority can be delegated with extensive discretionary powers, without the involvement of Union institutions, which would be unthinkable with other agencies.

On the other hand, the constitutional requirement of independence entails that a Union data protection agency must be able to exercise ‘autonomous powers’ – precisely the sort of powers that *Meroni* aims to limit. This precludes in data protection the use of ‘endorsement’ mechanisms, such as the ones existing in bank resolution or financial or pharmaceutical regulation.¹¹⁶ Such mechanisms are introduced in order to preserve the powers of Union institutions and therefore comply with *Meroni*. When Union agencies have the power to make complex technical and economic assessments, their measures often require the approval – often, in practice, the rubberstamping – of the Commission or the Council.

¹¹⁵See e.g. N. Moloney, ‘European Banking Union: Assessing its Risks and Resilience’, 51 *Common Market Law Review* (2014) p. 1609; and P. Weismann, ‘The ECB’s Supervisory Board under the Single Supervisory Mechanism (SSM): A Comparison with European Agencies’, 24 *European Public Law* (2018) p. 311 at p. 315-317.

¹¹⁶These agencies are known as ‘quasi-regulatory’ EU agencies. For an overview, see P. Craig, *EU Administrative Law* (Oxford University Press 2018) p. 164.

Whereas in other policy areas the introduction of an endorsement mechanism is necessary to ensure conformity with Union Treaties, such a mechanism would necessarily lead to the violation of Article 16(2) TFEU and Article 8(3) of the Charter. If their powers are too rigidly delimited, supervisory authorities cannot ‘control’ compliance; if their powers cannot be exercised without subsequent approval by Union institutions, these authorities cannot be ‘independent’.¹¹⁷ Accordingly, if the Treaty and the Charter are to be respected, then data protection authorities must be endowed with appropriate discretionary powers as well as the ability to exercise said powers on their own. This applies to a Union-level supervisory authority as well.

CONCLUSION

Personal data protection is a fundamental right protected by the Charter, with all its consequences. As it exists to implement the requirements of that fundamental right,¹¹⁸ the General Data Protection Regulation is different in nature from other Union legislation. Its enforcement hence differs from the enforcement of regulations in other policy areas. Ensuring its effectiveness is as crucial to fulfilling the positive obligation to protect fundamental rights as the adoption of substantive rules.

In this article, we have claimed that some of the instances of cross-border personal data processing – those that we label the cases of common European concern – are constitutionally required to be supervised by a Union supervisory authority. This is because the protection of fundamental rights in such cases can be effectively ensured only by centralised enforcement and not by the decentralised one-stop-shop model, structurally prone to create backlogs and invite national strategies to hamper the rights of the residents of the entire Union. We have put forward the arguments supporting this proposition and discussed various constitutional frameworks that need to be considered when engaging in the creation of the central supervisory authority. We have made the case that harmonisation of procedural provisions, despite some likely benefits in smaller cases, will not be an adequate remedy for the one-stop-shop model’s weaknesses.

Centralisation of enforcement should not be taboo. In fact, the trend in many areas of Union law has been to increasingly empower the Union’s own enforcement

¹¹⁷Indeed, as Union case law states, ‘independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task’: see ECJ 9 March 2010, Case C-518/07, *European Commission v Federal Republic of Germany*, para. 30.

¹¹⁸Explicitly in this sense, see ECJ 12 January 2023, Case C-154/21, *RW*, at para. 44.

authorities.¹¹⁹ We understand the possible hesitance of some actors to ‘reopen’ the General Data Protection Regulation or to fundamentally change the status quo of the one-stop-shop. However, when dealing with matters of constitutional gravity, we owe an obligation to act bravely not only to the law but, most importantly, to the people whose rights the law promises to protect. In cases of common European concern, we might face choices on how exactly to centralise enforcement. Yet, the affirmative answer to the ‘whether?’ question is provided by the Treaties.

Acknowledgements. The co-authors wish to thank the two anonymous peer reviewers for their attentive reading and helpful critique. The co-authors remain exclusively responsible for any flaw or mistake found in the paper. Pałka’s acknowledgement: The research leading to these results has received funding from the Norwegian Financial Mechanism 2014-2021, project No. 2020/37/K/HS5/02769, titled ‘Private Law of Data: Concepts, Practices, Principles & Politics’. The Open Access for this publication was funded by the Faculty of Law and Administration of the Jagiellonian University granted within the Priority Research Area FutureSoc under the program “Excellence Initiative – Research University” at the Jagiellonian University in Krakow.

Filipe Brito Bastos is assistant professor at NOVA School of Law and affiliated researcher at CEDIS, in Lisbon, Portugal.

Przemysław Pałka is assistant professor at the Jagiellonian University in Krakow, Poland, and affiliated fellow of the Information Society Project at Yale Law School.

The two authors contributed equally.



¹¹⁹M. Scholten, ‘Mind the Trend! Enforcement of EU Law Has Been Moving to “Brussels”’, 24 *Journal of European Public Policy* (2017) p. 1348 at p. 1354.