



Universiteit
Leiden
The Netherlands

The principle of sincere cooperation as institutional bridge between competition and data protection law?

Beems, R.B.

Citation

Beems, R. B. (2025). The principle of sincere cooperation as institutional bridge between competition and data protection law? *Market And Competition Law Review*, 9(2), 149-176.
doi:10.34632/mclawreview.2025.17994

Version: Publisher's Version
License: [Creative Commons CC BY 4.0 license](#)
Downloaded from: <https://hdl.handle.net/1887/4296356>

Note: To cite this publication please use the final published version (if applicable).

The Principle of Sincere Cooperation as Institutional Bridge between Competition and Data Protection Law?*

*Belle Beems***

ABSTRACT: In digital markets, personal data is increasingly monetized. As a result, the areas of competition and data protection law collide and the competences of enforcers of these fields of law (i.e. competition and data protection authorities) also overlap. These overlapping competences are not problematic per se but trigger a need for cross-disciplinary cooperation between data protection and competition authorities. Despite this need for cooperation, the EU framework does not provide any specific rules on the interaction between competition and data protection authorities and the CJEU derives certain obligations to cooperate from the principle of sincere cooperation. This paper assesses whether this approach is apt to facilitate cooperation between competition and data protection authorities in the EU. To this end, the paper studies the need for cooperation, the (lack of) existing frameworks for cooperation and the relevance of the principle of sincere cooperation. Furthermore, by identifying the main gaps and open questions associated with the institutional framework, the paper uncovers existing problems relating to cross-disciplinary cooperation between data protection and competition authorities. The absence of a forum for cooperation and the lack of a legal basis to share information are major problems posing obstacles to effective cross-disciplinary cooperation. The EU legislator should fill these gaps

* Date of reception: May 15, 2025; date of acceptance: June 13, 2025.

DOI: <https://doi.org/10.34632/mclawreview.2025.17994>.

** Belle Beems is an assistant professor at the Europa Institute of Leiden University. She previously worked as a PhD candidate at Radboud University, Faculty of Law, Department for International and European Law. This paper is based on her PhD research. See B. Beems, *The interaction between enforcers of competition law, the DMA, and the GDPR – An inquiry into the coherence of enforcement across legal domains*, forthcoming. I am grateful for the feedback of my PhD supervisors, prof. Johan van de Gronden, dr. Catalin Rusu and Anne Looijestijn-Clearie and for the useful input of the anonymous reviewer. The usual disclaimer applies. Montessorilaan 10, 6525 HR Nijmegen, The Netherlands. Belle.beems@ru.nl.

in the institutional framework by harmonizing the inter-jurisdictional interaction between competition and data protection authorities.

KEYWORDS: competition law; data protection law; the principle of sincere cooperation; norm overlaps; digital markets

1. Introduction

Over the past decade, a trend of increasing digitalization has challenged the regulatory framework of the EU. The rise of new business models has fostered a significant increase in the scale and scope of (personal) data processing which potentially affects fundamental rights, in particular the rights to privacy and data protection.¹ Apart from fundamental rights challenges, personal data processing has become increasingly relevant from a competitive perspective. Personal data has become an economic good that is traded on digital platforms, and transactions centres around the collection exchange and monetization of personal data.² Consequently, personal data has become a “competitive parameter” and can, thus, be relevant for a competition law assessment.³

The fact that personal data has become an ever more important competitive parameter has led to an overlap between the legal branches of competition law and the General Data Protection Regulation (henceforth: GDPR). This overlap triggers both substantive and institutional questions. From a substantive perspective, for example, the question of to what extent competition law can (or should) leave room for data protection considerations

¹ R. Augusto Castellanos Pfeiffer, “Digital economy, big data and competition law”, *Market Competition Law Review* 3, no. 1 (2019): 53; “Charter of Fundamental Rights of the European Union”. *Official Journal of the European Union* C83, vol. 53. Brussels: European Union; European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), *Official Journal of the European Union* L 119, May 4, 2016.

² S. Schneider et al., “Exploring design elements of personal data markets”, *Electronic Markets* 33 (2023).

³ Judgement of 4 July 2023, *Meta Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, para. 51 (henceforth: CJEU, *Meta Bundeskartellamt*). See, for a more elaborate analysis of the economics of this case, O. Budzinski, M. Grusevaja and V. Noskova, “The economics of the German investigation of Facebook’s data collection”, *Market and Competition Law Review* 5 (2021): 43.

is subject to heated debate.⁴ Institutionally, the overlap between the respective frameworks calls for cross-disciplinary cooperation between competition and data protection authorities. The institutional relevance of the growing intersection between competition and data protection law is acknowledged by both (legal) scholars and governmental actors. Already in 2017, the European Parliament adopted a resolution calling for “closer collaboration among regulators of conduct in the digital environment, so as to strengthen the synergies between regulatory frameworks for consumers and competition and data protection authorities”.⁵ Similarly, the European Commission (henceforth: Commission) highlights that “there is an increasing intersection and interplay between [competition law and data protection], and between the authorities enforcing them respectively”.⁶ In a recent position paper, the European Data Protection Board (henceforth: EDPB) highlights that “promoting synergies between personal data protection and competition authorities can improve the ability of both regimes to protect data subjects and users”.⁷

Despite the fact that the need for cooperation between competition and data protection authorities is broadly acknowledged, it remains uncertain whether EU law provides a framework to realize this cooperation in practice. In the *Meta Bundeskartellamt* case, the Court of Justice of the EU (henceforth: CJEU) explicitly stressed that “[n]either the GDPR nor any other instrument of EU law provides for specific rules on cooperation between national competition authorities and [data protection authorities]”. Despite the absence of such instruments, the CJEU has held that

⁴ See, e.g., V. Robertson and K. Majcher, “Protecting personal data and the environment: Doctrinal challenges for EU competition law in our day and age”, *European Law Review* 47 (2022): 622; Costa-Cabral and Lynskey, “Family ties”; N. Economides and I. Lianos, “Restrictions on privacy and exploitation in the digital economy: A market failure perspective”, *Journal of Competition Law & Economics* 17, no. 4 (2021): 765; A. Gorecka, *The interface between competition law and data privacy law* (Cham: Springer, 2024).

⁵ European Parliament, Resolution of 14 March 2017 on Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non-Discrimination, Security and Law-Enforcement (2016/2225(INI)), para. 9.

⁶ OECD, *The Intersection Between Competition and Data Privacy – Note by the European Union*, DAF/COMP/WD(2024)30 (Paris: OECD, June 6, 2024), 2.

⁷ European Data Protection Board (EDPB), *Position Paper on Interplay between Data Protection and Competition Law*, adopted January 16, 2025, para. 27. See also S. Vezzoso, “All happy families are alike: The EDPS’ bridges between competition and privacy”, *Market and Competition Law Review* 4, no. 1 (2020): 41.

data protection and competition authorities are under the obligation to cooperate by relying on the principle of *sincere cooperation*.⁸

The use of the principle of sincere cooperation as a basis for cooperative obligations is at the heart of this research. This paper assesses the extent to which the principle of sincere cooperation is apt to facilitate cooperation between competition and data protection authorities in the context of the EU and considers whether the principle is a reasonable alternative to more explicit and specific mechanisms of cooperation.

To this end, Section 2 sets the scene by explaining why cross-disciplinary cooperation between data protection and competition authorities is necessary. Next, Section 3 studies the (lack of) mechanisms for cross-disciplinary cooperation between competition and data protection authorities. Section 4 discusses the principle of sincere cooperation, particularly as a tool for cross-disciplinary cooperation. This section also uncovers the main gaps and open questions associated with the current institutional framework and puts forward recommendations to resolve existing issues. Section 5 concludes.

2. The need for cooperation

The GDPR and competition law are separate fields of law with their respective objectives, substantive rules and enforcement frameworks. Despite these differences, the two fields of law share some common characteristics or “family ties”.⁹ While an extensive discussion of the shared traits of competition law and the GDPR does not fall within the scope of this paper, this section aims to explain (i) why competition law and the GDPR increasingly intersect, (ii) how this results in overlapping competences of different enforcers, and (iii) why this triggers a need for cooperation between competition and data protection authorities.

2.1. Increasing overlaps between competition law and the GDPR

In the context of digital markets, competition law and the GDPR increasingly intersect. Various digital platforms offer their services free of charge for end users but create revenue by the monetization of personal data. Rather than aiming to set prices as high as possible to maximize profits,

⁸ CJEU, *Meta Bundeskartellamt*, para. 53.

⁹ Costa-Cabral and Lynskey, “Family ties”: 11.

platforms rely on various strategies of cross-subsidy across user groups.¹⁰ For instance, in the case of *indirect cross-subsidy*, the platform distributes its services at zero prices for one side of the platform because the other side pays for it.¹¹ Personalized advertisement by social media platforms constitutes a clear example of indirect cross-subsidy. Users of the social media network can rely on the service free of charge by “paying” with their personal data.¹² By collecting personal data of its users, a social media platform can create rather precise user profiles, including information about gender, age, location, education level and online shopping behaviour.¹³ The other side of the platform, i.e. advertisers, are willing to pay a monetary fee to access a specific user base or target group with certain characteristics.¹⁴ A shop owner in Amsterdam would, for example, be particularly interested in having their advertisement exposed to people residing in the same city.

Due to the monetization of personal data, competition law, data protection and privacy increasingly collide because personal data turns into a *competitive parameter*. In its revised Market Definition Notice, the Commission highlights that the parameters of competition may include “the product’s price, but also its degree of innovation and its quality in various aspects – such as [...] the] privacy protection afforded”.¹⁵ In the *Meta Bundeskartellamt* case, the CJEU emphasized that “[...] access to personal data and the fact that it is possible to process such data have become a significant parameter of competition between undertakings in the digital

¹⁰ F. Bostoen, “Online platforms and pricing: Adapting abuse of dominance assessments to the economic reality of free products”, *Computer Law & Security Review* 35 (2019): 263; J. Newman, “Antitrust in zero-price markets: Foundations”, *University of Pennsylvania Law Review* 164 (2015): 154.

¹¹ Newman, “Antitrust in zero-price markets”: 149-154.

¹² The analogy of personal data as method of payment is disputed. For further reading, see J. Haucap, “Competition and competition policy in a data-driven economy”, *Intereconomics* 4 (2019): 201; T. Schrepel, “Why you are not paying with your data”, *Le Concurrentialiste*, 2021, <https://leconcurrentialiste.com/why-you-are-not-paying-with-your-data/>.

¹³ S. Boerman, S. Kruikemeier and F. Zuiderveen Borgesius, “Online behavioural advertising: A literature review and research agenda”, *Journal of Advertising* 46 (2017): 363 and 367.

¹⁴ Newman, “Antitrust in zero-price markets”: 157; Furman J. et al., “Unlocking digital competition. Report of the Digital Competition Expert Panel”. 2019. https://assets.publishing.service.gov.uk/media/5c88150ee5274a230219c35f/unlocking_digital_competition_furman_review_web.pdf: 29.

¹⁵ European Commission. Commission Notice on the Definition of the Relevant Market for the Purposes of Union Competition Law. C/2024/1645. *Official Journal of the European Union*, 2024, para. 15 (henceforth: Relevant Markets Notice).

economy”.¹⁶ Moreover, the CJEU alludes to the fact that “personal data are of great importance in the context of the digital economy”.¹⁷

The acknowledgment of personal data as a parameter of competition bridges the areas of competition law and data protection law. In the past, the CJEU highlighted in the *Asnef-Equifax* case that “possible issues relating to the sensitivity of personal data are not, as such, a matter of competition law”.¹⁸ Yet, in *Meta Bundeskartellamt* the CJEU stressed that, given the fact that personal data has become a competitive parameter, “excluding the rules on the protection of personal data from the legal framework to be taken into consideration by competition authorities when examining an abuse of a dominant position” would disregard the economic reality and undermine the effectiveness of competition law within the European Union.¹⁹

Does this mean that the *Asnef-Equifax* and the *Meta Bundeskartellamt* cases cannot be reconciled? In my view, this question warrants a negative answer. Although the CJEU stresses that data protection considerations *as such* are not a matter of competition law, it does not exclude the possibility of considering data protection considerations as a parameter of competition. Indeed, in *Meta Bundeskartellamt* the CJEU opens the door for data protection considerations because personal data constitutes a competitive parameter. Insofar as data protection considerations can be considered as a competitive parameter, and in particular as part of the quality of a service, these considerations become relevant for a competition law analysis.²⁰ In this case, data protection considerations are not integrated in a competition law assessment *as such* but are instead regarded as part of the quality of a service. In other words, data protection has become a “normative yardstick for the assessment of quality”.²¹ Therefore, both judgments are not irreconcilable.

¹⁶ CJEU, *Meta Bundeskartellamt*, para. 51.

¹⁷ CJEU, *Meta Bundeskartellamt*, para. 49.

¹⁸ Judgment of the Court of 23 November 2006, *Ansnef-Equifax*, C-238/05, ECLI:EU:C:2006:734, para. 63.

¹⁹ CJEU, *Meta Bundeskartellamt*, para. 51.

²⁰ V. Robertson and K. Majcher, “Protecting personal data,” 637.

²¹ F. Costa-Cabral and O. Lynskey, “The internal and external constraint of data protection on competition law in the EU”, 2015, https://eprints.lse.ac.uk/64887/1/Lynskey_Internal%20and%20External%20Constraints%20of%20Data%20Protection%20_Author_2015.pdf.15.

In sum, in *Meta Bundeskartellamt* the CJEU clearly endorses the bridge between competition law and the GDPR by allowing competition authorities to integrate or “internalize” data protection considerations.²²

2.2. The interaction between competition and data protection law

The fact that the CJEU allows competition authorities to take into account data protection considerations potentially results in overlapping competences of the respective authorities, because the GDPR could be considered by both a competition and data protection authority (henceforth: DPA).

The CJEU makes it explicit that a competition authority cannot “replace” a data protection supervisor.²³ The competition authority “neither monitors nor enforces” the application of the GDPR “for the purposes referred to in Article 51(1) GDPR, namely in order to protect the fundamental rights and freedoms of natural persons in relation to processing or to facilitate the free flow of personal data within the European Union”.²⁴ Moreover, the competition authority merely notes the non-compliance of a data processing operation with the GDPR for the sole purpose of establishing an abuse of a dominant position. Furthermore, it can only put the abuse to an end by relying on a legal basis derived from competition law and does not carry out any of the tasks or powers listed in Articles 57 and 58 GDPR.

Although competition authorities cannot act as data protection supervisors, the CJEU allows them to assess non-compliance with the GDPR for the purpose of a competition law assessment, as competition authorities can “internalize” or integrate data protection considerations. As a result, data protection authorities are no longer the only authority able to assess compliance and, consequently, the respective fields overlap and cannot always be considered entirely separately.²⁵ The overlap between competition law and the GDPR transcends the traditional boundaries between legal branches and is, thus, *cross-disciplinary*.

²² Yakovleva, Geursen and Arnbak, “Kaleidoscopic data-related enforcement”: 1465.

²³ CJEU, *Meta Bundeskartellamt*, para. 49.

²⁴ CJEU, *Meta Bundeskartellamt*, para. 49.

²⁵ European Data Protection Board (EDPB), *Position Paper on Interplay between Data Protection and Competition Law*, adopted January 16, 2025, para. 1.

2.3. *The need for cooperation*

Overlapping competences of data protection and competition authorities are not necessarily problematic. The areas of competition and data protection law can be applied complementarily, thereby strengthening synergies.²⁶ By integrating both fields, a broader range of concerns can be addressed. Both fields of law, for example, contribute to ensuring that data is collected and used in a way that benefits citizens.²⁷ The use of the GDPR as a normative yardstick to assess quality is a clear and concrete example of such potential synergies.²⁸

However, and notwithstanding the potential benefits of the integration of the competition law and data protection framework, overlapping norms carry a degree of risk. *Firstly*, while overlapping norms have the potential to protect complementary objectives, parallel or consecutive consequences can also lead to clashes, divergent approaches by different regulators and tensions in enforcement.²⁹ Consequently, isolated approaches can be detrimental to the coherent application of the respective frameworks. *Secondly*, uncoordinated approaches can result in an undue consumption of enforcers' resources.³⁰ Authorities do not have unlimited resources, and uncoordinated parallel proceedings into a single conduct are not the most efficient way to spend limited financial and human resources.

The risks associated with overlapping competences can be mitigated by well-functioning mechanisms of cooperation.³¹ It is thus unsurprising that both the Commission and the EDPB acknowledge the need for cooperation. Synergies between the legal fields can only be realized if authorities

²⁶ I. Graef, "Blurring boundaries of consumer welfare: How to create synergies between competition, consumer, and data protection law in digital market". 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881969.

²⁷ OECD, *The intersection between competition and data privacy – Note by the European Union*, DAF/COMP/WD(2024)30 (Paris: OECD, June 6, 2024), para. 3.

²⁸ Robertson and Majcher, "Protecting personal data": 644.

²⁹ OECD, *The intersection between competition and data privacy – Note by the European Union*, DAF/COMP/WD(2024)30 (Paris: OECD, June 6, 2024), para. 2; in *Meta Bundeskartellamt*, the CJEU acknowledges that the "examination by a competition authority of an undertaking's conduct in the light of the provisions of the GDPR may entail the risk of divergences between that authority and the supervisory authorities in the interpretation of that regulation". See: CJEU, *Meta Bundeskartellamt*, para. 55.

³⁰ I. Graef, "Regulating digital platforms: Streamlining the interaction between the Digital Markets Act and national competition regimes", in I. Graef and B. van der Sloot (eds.), *The legal consistency of technology regulation* (Oxford: Hart Publishing, 2024), 158.

³¹ Yakovleva, Geursen and Arnbak, "Kaleidoscopic data-related enforcement": 1467 and 1479.

engage in cooperative efforts and exercise their respective competences in a manner that is both complementary and coherent.³²

In the EU, both competition law and the GDPR are enforced in a multi-level legal order. This means that competence overlap can be both cross-disciplinary (i.e., transcending one legal branch and entailing cooperation between enforcers of different areas of the law, in this case competition and data protection authorities) and *multi-jurisdictional*. Multi-jurisdictional overlaps relate to the competences of authorities across multiple jurisdictions or legal orders and are created by the different institutional design of competition law and the GDPR.

While EU competition law was initially enforced centrally by the Commission, Regulation 1/2003 fostered a shift towards partially decentralized enforcement.³³ Nowadays, competition law is enforced in a multi-level governance or multi-level administration model.³⁴ The framework is enforced by the Commission and national competition authorities (henceforth: NCAs).³⁵ Considering the position of NCAs, competition law is modelled on a *country of destination model*, meaning that NCAs of the Member States where the regulated service is offered have the competence to address infringements that occur within the national territory or that (may) produce effects therein.³⁶ Furthermore, while the Commission focuses on enforcement of EU competition law, NCAs also enforce their national competition laws.

³² European Data Protection Board (EDPB), *Position Paper on Interplay between Data Protection and Competition Law*, adopted January 16, 2025, para. 1; OECD, *The Intersection Between Competition and Data Privacy – Note by the European Union*, DAF/COMP/WD(2024)30 (Paris: OECD, June 6, 2024), para. 3.

³³ Article 89 EC Treaty (Treaty of Rome); G. Monti, “Independence, interdependence and legitimacy: The EU Commission, national competition authorities, and the European Competition Network”, 2014, <https://cadmus.eui.eu/handle/1814/29218>, 1.

³⁴ F. Cengiz, “Multi-level governance in competition policy”, *European Law Review* 35 (2010): 660.

³⁵ Council Regulation (EC) No. 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty. *Official Journal of the European Union*, L 1/1, 4 January 2003; Directive (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. *Official Journal of the European Union*, L 11/3, 14 January 2019.

³⁶ A. De Streele and G. Monti, “Improving EU institutional design to better supervise digital platforms”, CERRE Report, 2022. <https://cerre.eu/publications/improving-eu-institutional-design/>, 18.

The enforcement of the GDPR is far more decentralized. National data protection authorities take the lead in the enforcement of the GDPR.³⁷ For cross-border cases, the GDPR introduces a system for allocating competences in order to streamline cooperation between data protection authorities.³⁸ In case of cross-border processing, the authority of a data processor's main or single establishment shall be competent to act as the lead supervisory authority. Consequently, it models its case allocation framework for cross-border cases on a *country of origin* model aiming to prevent parallel procedures and providing a tool for case allocation among DPAs.³⁹

The country of origin model in the GDPR is not absolute.⁴⁰ For instance, other authorities than the lead supervisory authority can conduct independent supervisory activities in exceptional cases and the GDPR's consistency mechanism requires the lead supervisory authority to involve other DPAs. Article 60 GDPR establishes that the lead supervisory authority shall cooperate with the other supervisory authorities concerned and shall endeavour to seek consensus.⁴¹ To achieve this consensus, data

³⁷ Article 51 GDPR.

³⁸ According to Article 4(23) GDPR, *cross-border processing* means either “processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State” or “processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to affect data subjects in more than one Member State”.

³⁹ De Streel and Monti, “Improving EU institutional design”: 18; A. Galetta and P. De Hert, “The proceduralisation of data protection remedies under EU data protection law: Towards a more effective and data-subject-oriented remedial system”, *Review of European Administrative Law* 8 (2015): 125-144.

⁴⁰ This is contrary to the initial proposal. In the initial Proposal for the GDPR, the one-stop-shop mechanism was more absolute. According to Article 51(2) of this Proposal, in case of cross-border processing, “the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or processor in all Member States”. See Proposal of 25 January 2012 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)11 final.

⁴¹ According to Article 4(22) GDPR, “supervisory authority concerned” means a supervisory authority which is concerned by the processing of data because (a) the controller or processor is established on the territory of the Member State that is the supervisory authority, (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing, or (c) a complaint has been lodged with that supervisory authority.

protection authorities can mutually assist each other and may exchange information.⁴²

Additionally, the GDPR establishes a *consistency mechanism*. Article 60(3) GDPR provides that the lead supervisory authority shall communicate a draft decision to the other supervisory authorities concerned.⁴³ These authorities can submit relevant and reasoned opinions to the draft decision within four weeks. The lead supervisory authority may revise its draft decision by following these reasoned opinions.⁴⁴ Alternatively, if the lead supervisory authority refrains from following the objections, the matter will be submitted to the dispute resolution mechanism.⁴⁵ Article 63 GDPR provides a consistency mechanism aiming to safeguard the GDPR's consistent application throughout the EU. If the different DPAs concerned cannot reach consensus, the European Data Protection Board⁴⁶ may intervene by adopting a binding decision concerning all matters addressed in the relevant and reasoned objections.⁴⁷ Importantly, the GDPR's institutional framework for cooperation is currently under revision.⁴⁸

The fact that competition law relies on a country of destination model, while GDPR is shaped along the lines of a country of origin model, triggers a need for cross-disciplinary and multi-jurisdictional cooperation. The necessity of this form of cooperation is clearly reflected in the *Meta Bundeskartellamt* case. In this case, the German NCA integrates GDPR considerations in its assessment of an abuse of a dominant position. In *Meta Bundeskartellamt*, the CJEU stresses that where an NCA considers it necessary to rule on the compliance or non-compliance with the GDPR, the competition authority and supervisory authority concerned or, *where*

⁴² See e.g. Article 61 GDPR.

⁴³ Supervisory authority concerned means a supervisory authority which is concerned by the processing of personal data because (a) the controller or processor is established on the territory of that authority, (b) data subjects residing in the territory of that DPA are (likely to) be substantially affected by processing, or (c) a complaint has been lodged with that supervisory authority. See Article 4(22) GDPR.

⁴⁴ Article 60(5) GDPR.

⁴⁵ Article 63 GDPR.

⁴⁶ The European Data Protection Board is composed of the heads of the Member States' data protection authorities. The Commission may participate in the activities and meetings of the Board without a voting right. See Article 68 GDPR.

⁴⁷ Article 65 GDPR; This decision is adopted by a two-third majority of the members of the European Data Protection Board.

⁴⁸ European Commission. Proposal for a Regulation laying down additional procedural rules relating to the enforcement of the General Data Protection Regulation (GDPR). 4 July 2023.

appropriate, the competent lead supervisory authority must cooperate with each other in order to ensure the consistent application of the GDPR. Since the NCA is not necessarily located in the same Member State as the lead supervisory authority or the supervisory authority concerned, a need for cross-disciplinary and inter-jurisdictional cooperation arises.

3. The (lack of) cooperation mechanisms

As explained in the previous Sections, the fact that the GDPR and competition law increasingly collide, combined with the different institutional frameworks of the respective fields of law, triggers a need for *cross-disciplinary* cooperation between authorities. This Section explores to what extent the current institutional framework provides for mechanisms to facilitate this complex form of cooperation. There are significant differences in place between mono- and multi-jurisdictional cooperation. Therefore, both types of cooperation are addressed in turn. The analysis starts with an overview of (the lack of) multi-jurisdictional mechanisms. Next, a discussion on cooperation between data protection authorities and competition authorities in the cases of The Netherlands and Germany will illustrate the fact that cross-disciplinary cooperation mechanisms in the national context can be much more elaborate and better developed.

3.1. Multi-jurisdictional cooperation

EU law does not provide for a cooperation mechanism facilitating the interaction between competition and data protection authorities established in different jurisdictions. In the *Meta Bundeskartellamt* case, the CJEU highlights the need for this form of cooperation. However, at the same time, the CJEU stresses that “neither the GDPR nor any other instrument of EU law provides for specific rules on cooperation between an NCA and the relevant national supervisory authority concerned or the lead supervisory authority”.⁴⁹ The CJEU resolves this gap in the institutional framework by deriving certain duties to cooperate from the general principle of sincere cooperation.⁵⁰ The use of the principle of sincere cooperation as a tool to facilitate cross-disciplinary and inter-jurisdictional cooperation is further discussed in Section 4.

⁴⁹ CJEU, *Meta Bundeskartellamt*, para. 43.

⁵⁰ CJEU, *Meta Bundeskartellamt*, para. 53.

3.2. Mono-jurisdictional cooperation in Germany and The Netherlands

While the EU institutional framework does not provide explicit mechanisms for cooperation between competition and data protection authorities, the national institutional frameworks of several Member States do address this type of cooperation. The Netherlands and Germany constitute clear examples of jurisdictions in which the issue of cross-disciplinary cooperation between competition and data protection authorities is addressed explicitly.

In The Netherlands, institutional laws establish a rather elaborate framework for cooperation between the Dutch competition and data protection authorities. The framework for cooperation between the Dutch competition authority (*Autoriteit Consument en Markt*, henceforth: ACM) and the Dutch data protection supervisor (*Autoriteit Persoonsgegevens*, henceforth: AP) is laid down in the *Samenwerkingsprotocol tussen de Autoriteit Consument en Markt en Autoriteit Persoonsgegevens* (Cooperation Protocol ACM and AP, henceforth: Cooperation Protocol). The Cooperation Protocol aims to set out general principles for cooperation and to establish arrangements on the exchange of information between the AP and the ACM, and to lay down general principles for handling matters where the tasks assigned to the respective authorities are related or overlapping.⁵¹ Thanks to the Cooperation Protocol, cooperative arrangements do not have to be made on an *ad hoc* basis. Moreover, its public availability guarantees transparency as to the cooperation between the ACM and the AP.⁵²

Article 8 Cooperation Protocol establishes that authorities shall realize an “efficient and careful exchange of information” and emphasizes that authorities can share information about relevant developments relating to their respective tasks. This information may relate to intra-disciplinary cooperation in international fora insofar as the exchange of information is not prevented by the confidentiality principle. Additionally, the ACM and the AP can share alerts relating to harmful conduct covered by the exclusive area of competence of the other authority. Apart from sharing “general information”, Article 7 Cooperation Protocol elaborates on the

⁵¹ Article 2 Autoriteit Persoonsgegevens (AP) and Autoriteit Consument & Markt (ACM), *Samenwerkingsprotocol tussen de Autoriteit Persoonsgegevens en de Autoriteit Consument & Markt* (Den Haag, 2020), <https://zoek.officielebekendmakingen.nl/stcr-2020-36741.html> (henceforth: Cooperation Protocol).

⁵² Preamble Cooperation Protocol.

authorities' competence to share sensitive information. In order to share this sensitive information, authorities need a legal basis.⁵³ The competence of the AP and the ACM to share information is grounded in Dutch formal law.⁵⁴ The Cooperation Protocol further elaborates on this legal basis and introduces certain safeguards. Article 7(3) Cooperation Protocol, for example, establishes that the exchanged information cannot be used for purposes other than that for which it was provided.

Apart from providing a framework for the exchange of information, the Cooperation Protocol considers practical aspects of cooperation between the AP and the ACM. For instance, Article 4 Cooperation Protocol sets out that both organizations must designate first points of contact for the other supervisor. Moreover, authorities have to consult at least once a year, but more frequently if needed. Consultation can take place at the managerial or staff level.⁵⁵

The ACM published several documents on the cooperation between the AP and the ACM highlighting the importance of bilateral arrangements and structural cooperation between the two authorities.⁵⁶ Yet, practical experiences with cooperation are not unequivocally positive. Challenges, including capacity problems and a reluctance to share (confidential) information hampered effective enforcement. However, and despite these difficulties, in the Dutch context cooperation appeared negotiable and solvable at the working level.⁵⁷ Consequently, the overall trend in cooperation seems positive. Despite the positive attitude, the ACM proposes certain

⁵³ G. Zwenne, W. Steenbruggen and M. Reker, "Rechtsbescherming bij het gebruik van big data door toezichthouders: een verkenning", *Tijdschrift voor Toezicht* 7 (2016): 29-45; F. Sickinghe, "Fusie NMa, OPTA en Consumentenautoriteit. Kwaliteitsoffer voor kostenbesparingen?", *Mediaforum* 7/8 (2011): 204; P. Kuipers and P. Gaasbeek, "ACM en Informatieverstrekking – Een Weerbaarstige Materie", *Sanctierecht & Compliance* 5/6 (2013): 210-225. See also Court of First Instance Rotterdam, 24 December 2024, Case ROT 21/4781 and 21/4782, *Apple v. ACM*, para. 10.3. In this case, the District Court Rotterdam ruled that the exchange of information between two Dutch supervisory authorities met this requirement, since there was a Cooperation Protocol based on a legal basis in Dutch formal law.

⁵⁴ Article 19(2) Dutch GDPR Implementation Act and Article 7(2)(a) Establishment Act ACM. See Nederland. *Implementatiewet Algemene Verordening Gegevensbescherming* (AVG). Stb. 2018, 91. In werking getreden 25 mei 2018 and Nederland. *Instellingswet Autoriteit Consument & Markt* (ACM). Stb. 2013, 107.

⁵⁵ Article 5 Cooperation Protocol.

⁵⁶ ACM Besluit 21 maart 2023, ACM/UIT/594498. <https://www.acm.nl/system/files/documents/woo-besluit-over-samenwerkingsprotocol-acm-en-ap.pdf>, accessed 24 March 2025.

⁵⁷ ACM, Verslag 13 February 2020, https://www.acm.nl/system/files/documents/vergaderverslag-13-2-2020_0.pdf, accessed 24 March 2025.

potential improvements, including the structural embedding of “linking pins” in the respective organizations. On top of this, further investments could be made in structural contact, investing in each other’s work, personal relationships and joint events.⁵⁸

In Germany, the legal framework for cooperation between data protection and competition authorities is less elaborate. The legal framework is limited to legal provisions allowing for the exchange of information. According to Section 50f GWB, the *Bundeskartellamt*, the Federal Commissioner for Data Protection and the *Land* Commissioners for data protection are permitted to exchange information.⁵⁹ Yet, cooperation between German competition and data protection authorities occurs frequently in practice. For instance, in the *Meta Bundeskartellamt* case, the German NCA consulted with the Federal Commissioner for Data Protection and the regional DPA of Hamburg to inform them about their enforcement actions. The *Bundeskartellamt*, amongst others, confirmed that the DPAs mentioned were not conducting parallel procedures. Cooperation between German authorities is not limited to the *Meta Bundeskartellamt* case. The German competition authority has reported cooperation in multiple cases.⁶⁰

Apart from bilateral cooperation between data protection and competition authorities, several multilateral initiatives may facilitate cooperation between competition and data protection authorities in the national context. In The Netherlands, both the ACM and the AP are part of the *Samenwerkingsplatform Digitale Toezichthouders* (Digital Cooperation Platform, henceforth: SDT) and the *Markttoezichthoudersberaad* (Market Supervisory Council, henceforth MTB).⁶¹ In Germany, both competition and data protection authorities participate in the Digital Cluster Bonn.⁶²

⁵⁸ ACM, Verslag 13 February 2020, https://www.acm.nl/system/files/documents/vergaderverslag-13-2-2020_0.pdf, accessed 24 March 2025.

⁵⁹ In Germany, the enforcement of data protection law is the shared responsibility of the federal and *land* authorities. See Section 8 and 9 Section 8 and 40 German Federal Data Protection Act.

⁶⁰ OECD. *The Intersection Between Competition and Data Privacy – Note by Germany*. DAF/COMP/WD(2024)42. Paris: OECD, 2024, para. 14; *Bundeskartellamt*. “Bundeskartellamt reviews Apple’s tracking rules for third-party apps”, June 14, 2022. Accessed March 12, 2025. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/PressBelle.beems@ru.nlemitteilungen/2022/14_06_2022_Apple.html.

⁶¹ Autoriteit Persoonsgegevens. “Samenwerking”. Accessed March 25, 2025. <https://www.autoriteitpersoonsgegevens.nl/over-de-autoriteit-persoonsgegevens/samenwerking>.

⁶² Digital Cluster Bonn. “Sechs Bundesbehörden Arbeiten Bei der Digitalisierung Enger Zusammen.” January 15, 2024. Accessed March 25, 2025. https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2024/15_01_2024_Digital_Cluster.html.

4. Cooperation on the basis of the principle of sincere cooperation

The previous section discussed mono- and multi-jurisdictional mechanisms of cooperation between competition and data protection authorities. It became apparent that while mono-jurisdictional mechanisms at the national level are rather elaborate, the framework for multi-jurisdictional cooperation is far less developed. Yet, in the *Meta Bundeskartellamt* case, the CJEU explicitly acknowledges the need for cooperation between competition and data protection authorities in this multi-jurisdictional setting.⁶³ The CJEU resolves the absence of explicit mechanisms for cooperation by invoking the general principle of sincere cooperation. In order to understand this approach, this Section starts with an analysis of the principle of sincere cooperation. Next, the relevance of the principle for cooperation between data protection and competition authorities established in different Member States will be addressed.

4.1. The principle of sincere cooperation

The principle of sincere cooperation, which is laid down in Article 4(3) TEU, establishes that the EU and the Member States shall, “in full mutual respect, assist each other in carrying out tasks which flow from the Treaties”.⁶⁴ The provision further establishes that Member States shall “take any appropriate measure, general or particular, to ensure fulfilment of the objectives arising out of the Treaties or resulting from acts of the institutions of the Union” and that “Member States shall facilitate the achievement of the Union’s tasks and refrain from any measure which would jeopardise the Union’s objectives”. Article 13(2) TEU concerns the loyalty between EU institutions and sets out that “[e]ach institution shall act within the limits of the powers conferred on it” and that “[t]he institutions shall practice in mutual cooperation”.⁶⁵

This principle of sincere cooperation has multiple dimensions. The horizontal dimension entails the cooperation between authorities established at the same level, i.e., between different EU institutions or between

⁶³ CJEU *Meta Bundeskartellamt*, para. 54.

⁶⁴ The principle of sincere cooperation is also being referred to as the principle of *loyal* cooperation. The terminology is not consistent. This paper uses the term sincere cooperation. See also Y. Jorens et al., “Analytical report for the European Commission on mutual assistance and sincere cooperation: An inquiry into the cooperation to enforce the Coordination Regulation to combat fraud and error”, 2017, <https://ec.europa.eu/social/BlobServlet?docId=19403&langId=en>.

⁶⁵ The obligations based on loyalty that apply between different Union institutions are also referred to as *institutional loyalty*. See Klamert, *The principle of loyalty in EU law*, 22 and 28.

different national authorities. Apart from this horizontal dimension, the principle of sincere cooperation applies vertically and addresses the position of Member States *vis-à-vis* EU institutions.⁶⁶ This vertical dimension can also be reversed: the principle of sincere cooperation can also impose obligations on EU institutions *vis-à-vis* national authorities.⁶⁷

The horizontal dimension of the principle of sincere cooperation has played a significant role in the decentralized enforcement framework of the EU.⁶⁸ National authorities play a key role in the enforcement of multiple EU laws, including EU competition law and the GDPR. Given the importance of national enforcement actions, a certain degree of loyalty is necessary to maintain the “federal” balance in the EU.⁶⁹

Furthermore, it is well established that the principle of sincere cooperation can also impose obligations on EU institutions, including the Commission.⁷⁰ The reciprocal nature of the principle is clearly reflected in Article 4 TEU, which refers to *mutual* respect. Yet, most cases on the reverse vertical application of the principle of sincere cooperation do not concern the Commission’s relationship with other executive authorities. The *Zwartveld* case, for instance, concerns the Commission’s cooperation with the national judiciary and in the *IMO case* the CJEU imposes a duty

⁶⁶ The vertical dimension of loyalty “finds its limits with purely political matters”. Member States are, for example, not required to cooperate in the Council. See Klamert, *The principle of loyalty in EU Law*, 24.

⁶⁷ M. Klamert, “Article 4 TEU”. In M. Kellerbauer, M. Klamert, and J. Tomkin (eds.). *The EU Treaties and the Charter of Fundamental Rights: A commentary* (Oxford: Oxford University Press, 2019), 123-145.

⁶⁸ For a discussion on the relevance of the principle of sincere cooperation for the European Competition Network, see C. Massa, “New CPC Regulation and ECN+ Directive: The powers of national authorities in the fields of consumer protection and antitrust”, *Market and Competition Law Review* 4, no. 2 (2020): 132-133.

⁶⁹ B. Guastaferro. “Sincere cooperation and respect for national identities: the unitary and the pluralist twists of the European integration process”. *Neo-Federalism Working Paper Series*, 2015. https://www.federalism.eu/assets/2017/07/wp_2_15.pdf, 3-4.

⁷⁰ De Baere and Roes stress that “[c]rucially, the duty of loyal cooperation not only imposes obligations on the Member States but also on the Union institutions”. Klamert puts forward that “[t]he CJEU] emphasized what is now explicitly stated in Article 4(3) TEU, namely that loyalty rests on mutual duties, which bind not only the Member States but also the Union institutions”. Lenaerts, Van Uffel and Corthaut put forward that “[t]he principle of sincere cooperation also holds good for the Union institutions, which must cooperate in good faith with the Member States”. See: G. De Baere and T. Roes, “EU loyalty as good faith”, *International & Comparative Law Quarterly* 64 (2015): 835; M. Klamert, *The principle of loyalty in EU Law* (Oxford: Oxford University Press, 2014); K. Lenaerts, P. Van Nuffel and T. Corthaut, T., *EU constitutional law* (Oxford: Oxford University Press, 2021), para. 16.0003.

of best effort upon the Commission *vis-à-vis* the Hellenic Republic.⁷¹ The reverse vertical application of the principle of sincere cooperation leads to open questions if the Commission were to integrate GDPR considerations into its competition law analyses. This issue is further discussed in Section 5.3.

4.2. The principle of sincere cooperation as a tool to facilitate the interaction between competition and data protection authorities

The principle of sincere cooperation shapes the cooperation between competition and data protection authorities in the EU. This is not a novelty: various intra-disciplinary cooperation mechanisms are grounded in this principle. The principle is, for example, the foundation for the European Competition Network, Regulation 1/2003 and the consistency mechanisms of the GDPR.⁷²

In *Meta Bundeskartellamt*, the CJEU relies on the principle of sincere cooperation to establish a duty for cross-disciplinary cooperation between data protection and competition authorities. The CJEU stresses that the authorities involved (i.e., the German competition authority and the German and Irish data protection authorities) are bound by the duty of sincere cooperation.⁷³ The CJEU reiterates the duties established in Article 4(3) TEU and further elaborates on the concrete duties of cooperation that can be derived from the principle. When internalizing GDPR considerations, NCAs are “required to consult and cooperate sincerely with the national supervisory authority concerned or with the lead supervisory authorities, all of which are then bound [...] to observe their respective powers and competences, in such a way as to ensure that the obligations arising from the GDPR and the objectives of that regulation are complied with while their effectiveness is safeguarded”.⁷⁴

⁷¹ In the *Delimitis* case, the CJEU also focused on cooperation with judicial authorities by stating that the Commission “is bound by a duty of sincere cooperation with the judicial authorities of the Member State, who are responsible for ensuring that [EU] law is applied in the legal order”. See Judgement of 28 February 1991, *Delimitis v. Henninger Bräu AG*, C-234/89, ECLI:EU:C:1991:9, para. 53; Order of 13 July 1990, *Zwartveld and Others*, C-2/88, ECLI:EU:C:1990:440, para. 18; Judgement of 12 February 2009, *Commission v. Hellenic Republic (IMO)*, C-45/07, ECLI:EU:C:2009:81, para. 25; Klamert, *The principle of loyalty in EU*, 240.

⁷² Whish and Bailey, for instance, refer to the European Competition Network as a manifestation of the principle of sincere cooperation. See R. Whish and D. Bailey, *Competition law*, 10th ed. (Oxford: Oxford University Press, 2021), 303.

⁷³ CJEU, *Meta Bundeskartellamt*, para. 53 and case law cited.

⁷⁴ CJEU, *Meta Bundeskartellamt*, para. 54.

The CJEU gives further shape to the general obligation to coordinate and cooperate in the judgment. It highlights that NCAs examining whether an undertaking's conduct is consistent with the provisions of the GDPR must "ascertain whether that or similar conduct has already been the subject of a decision" by a relevant DPA. If that is the case, the competition authority cannot depart from the decision, although it remains competent to draw its own conclusions as to the application of competition law.⁷⁵ In case of (i) doubts as to the scope of the assessment carried out by the DPA, (ii) where conduct is simultaneously investigated by a DPA or (iii) where the NCA considers the conduct in question as being not consistent with the GDPR, the competition authority must "seek cooperation to dispel its doubts or to determine whether it must wait for the [DPA] to take a decision before starting its own assessment".⁷⁶ In the *Meta Bundeskartellamt* case, the German *Bundeskartellamt* appears to have fulfilled its duty to cooperate as it contacted the *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (Federal Commissioner for Data Protection and Freedom of Information, Germany), the *Hamburgische Beauftragte für Datenschutz und Informationsfreiheit* (Commissioner for Data Protection and Freedom of Information, Hamburg, Germany) and the Irish Data Protection Commission.⁷⁷

The principle of sincere cooperation imposes obligations not only on competition authorities, but also on data protection authorities, which are under the obligation to respond to the request for information or cooperation within a reasonable period of time. DPAs must provide information capable of dispelling doubts or inform the NCA if it intends to initiate the cooperation procedure with other supervisory authorities.⁷⁸ In the absence of a reply within a reasonable time, the NCA may continue with its own investigation.

Lacking an explicit framework for cooperation, the CJEU relies on the principle of sincere cooperation to construe duties of cross-disciplinary cooperation. The fact that the CJEU openly affirms the need for this type of cooperation is to be applauded and marks an important step in the development of the discourse on cooperation between the enforcers of different

⁷⁵ CJEU, *Meta Bundeskartellamt*, para. 56.

⁷⁶ CJEU, *Meta Bundeskartellamt*, para. 57.

⁷⁷ The Irish authority would be the lead supervisory authority, as Meta has its European headquarters in Dublin. See, e.g., <https://www.meta.com/nl/en/legal/terms-of-sale/>, accessed 14 May 2025.

⁷⁸ CJEU, *Meta Bundeskartellamt*, para. 58.

legal branches. Yet, the solution is not without its flaws. The next Section will address the main open questions and gaps and aims to provide solutions to resolve these remaining issues.

5. Gaps, open questions and recommendations

The previous Section studied cross-disciplinary and multi-jurisdictional cooperation between data protection and competition authorities on the basis of the principle of sincere cooperation. Notwithstanding the importance of the CJEU paving the way for this type of cooperation, several open questions and gaps remain. This Section addresses three main complications, i.e., (i) whether an NCA can establish that a conduct is compliant with the GDPR, (ii) the fact that a general principle does not suffice to build a cooperative relationship, and (iii) the hypothetical problem that may arise if the Commission were to apply the theory of harm as established in *Meta Bundeskartellamt*.

5.1. What about compliance?

The *Meta Bundeskartellamt* judgement focuses on NCAs finding non-compliance with the GDPR.⁷⁹ However, the question of whether an NCA can find that specific conduct is *compliant* with the GDPR remains under-explored. Considering the tasks and competences of competition and data protection authorities, as well as the relationship between these enforcers, it is highly unlikely that a DPA would be bound by an NCA's conclusion of compliance with the GDPR. Indeed, the CJEU establishes that an NCA can rule on the GDPR “for the sole purpose of establishing an abuse of a dominant position”.⁸⁰ This indicates that a ruling of an NCA cannot limit the GDPR's competence to establish non-compliance with the GDPR.

Yet, the scenario in which a competition authority explicitly rules that a particular conduct complies with the GDPR, while a DPA regards the same conduct as a violation of the same regulation, is undesirable. Against this background, it is not appropriate that an NCA establishes that conduct is compliant with the GDPR. In my view, this limitation can be inferred from the principle of sincere cooperation and therefore already applies in practice. However, to enhance legal certainty, it would be beneficial to

⁷⁹ K. Majcher, “Interaction between EU competition law and data protection in digital markets: Striving for coherence”, in P. Parcu, G. Monti and M. Mariniello (eds.), *Research handbook on competition and technology*, (Cheltenham: Edward Elgar Publishing, 2024), 202-220.

⁸⁰ CJEU, *Meta Bundeskartellamt*, para. 49

explicitly establish this limitation. This approach would mirror Article 10 of Regulation 1/2003 and the *Tele2Polska* case, which provided that NCAs cannot decide on the inapplicability of EU competition law.⁸¹

5.2. A general principle is not enough

A second issue relates to the fact that a general principle (i.e., the principle of sincere cooperation) is not sufficient to facilitate a system of effective cooperation between authorities. Despite the fact that the CJEU gives further effect to the principle by deriving more concrete obligations to cooperate from the principle of sincere cooperation, (too) many open uncertainties persist. Notwithstanding the clear obligation to cooperate, the procedural details remain opaque. One of the most significant voids is the absence of a forum for cooperation. It is unclear in which forum authorities can realize their interaction. This also raises questions as to the practical details of cooperation. For instance, it remains unclear whether authorities should interact at the managerial level or whether interaction between officials or case handlers would suffice.

Another major gap concerns the absence of competence or legal basis for exchanging confidential information. In order to share such information, authorities must have a legal basis. Currently, no such basis exists for exchanging information between data protection and competition authorities in a multi-jurisdictional setting. While there is a clear obligation to coordinate, authorities are not entitled to exchange confidential information. The implications of these gaps were clearly illustrated by the *Google Fitbit* case, in which the EDPB stressed its willingness to advise the Commission on the implications of a merger for the protection of personal data.⁸² However, the Commission was rather reluctant to exchange evidence in cooperation with the EDP and Vestager emphasized that – in cooperation with privacy regulators – she “would not discuss specific cases because we would invite people who may not be privy to” confidential reviews of a merger.⁸³

⁸¹ Judgement of the Court of 3 May 2011, *Tele2Polska sp. z o.o. v. President of the Office of Electronic Communications*, C-375/09, ECLI:EU:C:2011:270.

⁸² European Data Protection Board. *Statement on the implications of mergers*. 19 February 2020. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf. Accessed May 14, 2025.

⁸³ A. White and H. Ali, *Google-Fitbit probe isn't for data watchdogs, Vestager says*. Bloomberg, February 25, 2020.

The EU legislator should take legislative action to address these gaps in the current framework. The principle for sincere cooperation offers a strong foundation for cooperation, but – on its own – is not sufficient to build a cooperative relationship between competition and data protection authorities. Moreover, the absence of a legal basis for exchanging (confidential) information poses a serious obstacle to effective cooperation. Given the multi-jurisdictional and cross-border nature of this issue, the EU legislator is best placed to take action, preferably by introducing secondary EU legislation harmonizing inter-jurisdictional cooperation between data protection and competition authorities. Such cooperation can hardly be arranged at the national level, as this would require 27 bilateral agreements between authorities – an unfeasible solution. Therefore, top-down action by the EU legislator is needed.

The EU legislator should adopt a directive which could be based on Article 103 TFEU, as well as Articles 16 and 114 TFEU. Rather than reinventing the wheel, the EU legislator could draw inspiration from existing frameworks for cross-disciplinary cooperation. Notably, Article 38(1) and (5) Digital Markets Act provides valuable guidance that could be applied by analogy.⁸⁴ These provisions allow for the exchange of (confidential) information for the purpose of coordination of enforcement. Beyond offering a legal basis for the sharing of information, the harmonized framework could introduce single points of contact in data protection and competition authorities.⁸⁵ Dedicated teams responsible for cross-disciplinary cooperation would facilitate an easier interaction between authorities. The dedicated teams could also receive targeted training on the relevant legal landscape and cross-disciplinary developments.⁸⁶

5.3. *The hypothetical problem: cooperation with the Commission*

An additional problem may arise if the Commission were to adopt the *Meta Bundeskartellamt* theory of harm. Although the *Meta Bundeskartellamt*

⁸⁴ European Union. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). *Official Journal of the European Union* L 265, September 12, 2022, 1-66.

⁸⁵ Such a single point of contact would not be a novelty. In the context of cooperation between the Dutch DPA and NCA, Article 4 Cooperation Protocol sets out that both authorities should establish a first point of contact.

⁸⁶ European Data Protection Board (EDPB), *Position paper on interplay between data protection and competition law*, adopted January 16, 2025, para. 24.

case concerned German competition law and the German authority refrained from applying EU competition law, the CJEU included Article 102 TFEU in the assessment by referring to “the examination seeking to establish whether there is an abuse of a dominant position within the meaning of Article 102 TFEU”.⁸⁷ Since the CJEU transposed the *Meta Bundeskartellamt* theory of harm to EU competition law, the Commission could potentially integrate data protection considerations into a competition law assessment.⁸⁸ If the Commission were to adopt this approach in the future, an awkward institutional situation may arise.

If an NCA integrates GDPR considerations, it has to ascertain whether it must wait for the DPA to dispel uncertainties.⁸⁹ Consequently, a competition law procedure can temporarily be suspended (e.g., due to an ongoing investigation by a DPA). Thus, executive action by a DPA can temporarily suspend a competition authority’s ability to proceed with its own procedure.⁹⁰

If the cooperative obligations of *Meta Bundeskartellamt* are transposed to the Commission, the Commission’s application of Article 102 TFEU could be suspended by a GDPR procedure at the national level. This would mean that the Commission (i.e., the Guardian of the Treaty) would be limited in the application of EU primary law by a national authority’s application of EU secondary law. Considering the Commission’s position, as well as the hierarchy of EU laws, this would be highly atypical. Admittedly, it is still uncertain whether the CJEU would derive similar obligations to cooperate from the principle of sincere cooperation in the context of the relationship between the Commission and a DPA. The principle of sincere

⁸⁷ CJEU, *Meta Bundeskartellamt*, para. 56. The fact that the German competition authority refrained from applying Article 102 TFEU amounts to a potential violation of Article 3(1) Regulation 1/2003. This issue does not fall within the scope of this paper. For further reading, see W. Wils, “The obligation for the competition authorities of the EU Member States to apply EU antitrust law and the Facebook decision of the Bundeskartellamt”, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3424592.

⁸⁸ The Commission has acknowledged the relevance of privacy as competitive parameter. In para. 15 of the Relevant Markets Notice, the Commission lists the level of privacy protection afforded as a parameter of competition for defining the relevant market.

⁸⁹ CJEU, *Meta Bundeskartellamt*, para. 57-59.

⁹⁰ This can potentially seriously delay competition law procedures. To prevent such delays, data protection authorities can waive the obligations to wait. According to Picht, the principle of sincere cooperation may even require such waiver. See P. Picht, “CJEU on Facebook: GDPR processing justifications and application competence”, 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4521320, 2. CJEU, *Meta Bundeskartellamt*, para. 59.

cooperation applies to the Commission – as also explained in Section 4.1. However, given the limited experience with the application of the principle of sincere cooperation to the Commission's relationship with national executive actors, the reach and implications of the principle are not clear. The CJEU should provide further clarity in this regard.

Considering the institutional framework, Article 40(1) GDPR could provide a potential solution. This provision allows the Commission to seek advice from the EDPB. Rather than consulting with national authorities, the Commission could approach the EDPB directly. Admittedly, the current institutional framework makes it rather difficult to adopt this solution, as it is hard to reconcile with the position of the lead supervisory authority. Moreover, and as addressed earlier, the lack of a legal basis for exchanging confidential information creates another barrier. It is important to address these issues in future EU legislation, ideally during the legislative procedure for the upcoming GDPR procedural regulation.⁹¹

6. Conclusion

This paper studied the cross-disciplinary cooperation between competition and data protection authorities. Currently, the EU framework does not provide explicit mechanisms to govern the interaction between these authorities.⁹² At the Member State level, for example in the Netherlands and Germany, more elaborate mechanisms are in place. While these tools are important for the national context, they cannot facilitate effective inter-jurisdictional cooperation in cross-border cases. Yet, the current institutional framework requires cooperation between data protection and competition authorities across different Member States – particularly given the fact that competition law is enforced according to a country of destination model, whereas the GDPR is modelled on a country-of-origin model.

The fact that the CJEU acknowledges the need for cross-disciplinary cooperation is a welcome development and marks an important step in the development of mechanisms to enable this (complex) form of cooperation.⁹³ Yet, although the principle of sincere cooperation can serve as

⁹¹ European Commission, *Proposal for a Regulation Laying Down Additional Procedural Rules Relating to the Enforcement of the General Data Protection Regulation* (GDPR). 4 July 2023. https://commission.europa.eu/publications/proposal-regulation-laying-down-additional-procedural-rules-relating-enforcement-gdpr_en.

⁹² CJEU, *Meta Bundeskartellamt*, para. 43.

⁹³ See, e.g., CJEU, *Meta Bundeskartellamt*, para. 43.

a foundation for cooperation, the principle alone does not suffice to build a cooperative relationship. Further (institutional) arrangements and procedural guarantees are required. As discussed in this article, due to the general nature of the principle of sincere cooperation, (too) many open questions remain. The absence of a designated forum for cooperation and the lack of clearly defined procedural details will hamper effective cooperation. Furthermore, and arguably even more critically, the absence of a framework for exchanging (confidential) information presents an insurmountable obstacle to effective cooperation and coordination. Apart from these gaps in the institutional framework, the hypothetical situation in which the Commission would apply the *Meta Bundeskartellamt* theory of harm can give rise to further institutional problems. The principle of sincere cooperation applies to the Commission, but it is uncertain which concrete duties *vis-à-vis* national data protection authorities can be derived from this principle. The relationship between the Commission and national data protection authorities thus needs to be reconsidered and the CJEU should provide further clarity on the application of the principle of sincere cooperation in this specific context.

Consequently, the principle of sincere cooperation provides a useful foundation to realize effective cooperation but cannot substitute more explicit and specific mechanisms. Against this background, the EU legislator should take action by harmonizing the cooperation between competition and data protection authorities in a cross-border context. It is particularly important to establish a forum for cooperation and to provide a legal basis for exchanging confidential information to coordinate enforcement actions.

6. Bibliography

- Boerman, S., Kruikemeier, S., and Zuiderveen, Borgesius F. "Online behavioural advertising: A literature review and research agenda". *Journal of Advertising* 46 (2017).
- Bostoen, F. "Online platforms and pricing: Adapting abuse of dominance assessments to the economic reality of free products". *Computer Law & Security Review* 35 (2019).
- Budzinski, O., Grusevaja M. and Noskova V. "The economics of the German investigation of Facebook's data collection". *Market and Competition Law Review* 5 (2021).
- Castellanos Pfeiffer, R. A. "Digital economy, big data and competition law". *Market Competition Law Review* 3, no. 1 (2019).
- Cengiz, F. "Multi-level governance in competition policy". *European Law Review* 35 (2010).

- Costa-Cabral, F. and Lynskey, O. "The internal and external constraint of data protection on competition law in the EU". 2015, https://eprints.lse.ac.uk/64887/1/Lynskey_Internal%20and%20External%20Constraints%20of%20Data%20Protection%20_Author_2015.pdf.
- Costa-Cabral, F. and Lynskey, O. "Family ties: The intersection between data protection and competition law in the EU". *Common Market Law Review* 54 (2018).
- De Baere, G. and Roes, T. "EU loyalty as good faith". *International & Comparative Law Quarterly* 64 (2015): 829-849.
- De Streel, A. and Monti, G. "Improving EU institutional design to better supervise digital platforms". CERRE Report, 2022. <https://cerre.eu/publications/improving-eu-institutional-design/>.
- Economides, N. and Lianos, I. "Restrictions on privacy and exploitation in the digital economy: A market failure perspective". *Journal of Competition Law & Economics* 17, no. 4 (2021).
- Furman J. et al. "Unlocking digital competition. Report of the Digital Competition Expert Panel". 2019. https://assets.publishing.service.gov.uk/media/5c88150ee5274a230219c35f/unlocking_digital_competition_furman_review_web.pdf.
- Galetta, A. and De Hert, P. "The proceduralisation of data protection remedies under EU Data protection law: Towards a more effective and data-subject-oriented remedial system". *Review of European Administrative Law* 8 (2015): 125-144.
- Gorecka, A. *The interface between competition law and data privacy law*. Springer, 2024.
- Graef, I. "Blurring boundaries of consumer welfare: How to create synergies between competition, consumer, and data protection law in digital market". 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881969.
- Graef, I. "Regulating digital platforms: Streamlining the interaction between the Digital Markets Act and national competition regimes". In I. Graef and B. van der Sloot (eds.). *The legal consistency of technology regulation*, 156-176. Oxford: Hart Publishing, 2024.
- Guastaferro, B. "Sincere cooperation and respect for national identities: The unitary and the pluralist twists of the European integration process". Neo-Federalism Working Paper Series, 2015. https://www.federalism.eu/assets/2017/07/wp_2_15.pdf.
- Haucap, J. "Competition and competition policy in a data-driven economy". *Intereconomics* 4 (2019).
- Jorens, Y. et al. "Analytical report for the European Commission on mutual assistance and sincere cooperation: An inquiry into the cooperation to enforce the Coordination Regulation to combat fraud and error". 2017, <https://ec.europa.eu/social/BlobServlet?docId=19403&langId=en>.
- Klamert, M. *The principle of loyalty in EU law*. Oxford: Oxford University Press, 2014.

- Klamert, M. "Article 4 TEU". In M. Kellerbauer, M. Klamert, and J. Tomkin (eds.). *The EU Treaties and the Charter of Fundamental Rights: A commentary*, 123-145. Oxford: Oxford University Press, 2019.
- Kuipers, P. and Gaasbeek, P. "ACM en Informatieverstreking – een Weerbarstige Materie". *Sanctierecht & Compliance* 5/6 (2013): 210-225.
- Lenaerts, K., Van Nuffel, P. and Corthaut, T. *EU constitutional law*. Oxford: Oxford University Press, 2021.
- Majcher, K. "Interaction between EU competition law and data protection in digital markets: Striving for coherence". In P. Parcu, G. Monti, and M. Mariniello (eds.). *Research handbook on competition and technology*, 202-220. Cheltenham: Edward Elgar Publishing, 2024.
- Monti, G. "Independence, interdependence and legitimacy: The EU Commission, national competition authorities, and the European Competition Network". 2014, <https://cadmus.eui.eu/handle/1814/29218>.
- Massa, C. "New CPC Regulation and ECN+ Directive: The powers of national authorities in the fields of consumer protection and antitrust". *Market and Competition Law Review* 4, no. 2 (2020).
- Newman, J. "Antitrust in zero-price markets: Foundations". *University of Pennsylvania Law Review* 164 (2015).
- Picht, P. "CJEU on Facebook: GDPR processing justifications and application competence". 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4521320.
- Robertson, V. and Majcher, K. "Protecting personal data and the environment: Doctrinal challenges for EU competition law in our day and age". *European Law Review* 47 (2022).
- Schneider S. *et al.* "Exploring design elements of personal data markets". *Electronic Markets* 33 (2023).
- Sickinghe, F. "Fusie NMa, OPTA en Consumentenautoriteit. Kwaliteitsoffer voor kostenbesparingen?". *Mediaforum* 7/8 (2011): 203-217.
- Schrepel, T. "Why you are not paying with your data". *Le Concurrentialiste*, 2021, <https://leconcurrentialiste.com/why-you-are-not-paying-with-your-data/>.
- Vezzoso, S. "All happy families are alike: The EDPS' bridges between competition and privacy". *Market and Competition Law Review* 4, no. 1 (2020).
- Whish, R. and Bailey, D. *Competition law*, 10th ed. Oxford: Oxford University Press, 2021.
- White, A. and Ali, H. "Google-Fitbit probe isn't for data watchdogs, Vestager says". Bloomberg, February 25, 2020.
- Wils, W. "The obligation for the competition authorities of the EU Member States to apply EU antitrust law and the Facebook decision of the Bundeskartellamt". https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3424592.

Zwenne, G., Steenbruggen, W. and Reker, M. "Rechtsbescherming bij het gebruik van big data door toezichthouders: Een verkenning". *Tijdschrift voor Toezicht* 7 (2016): 29-45.

