ZESZYT PRAWNICZY UAM
NR 15/2025
https://doi.org/10.14746/zpuam.2025.15.9

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

MARIANNA ZAWAL

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0000-4368-296X
marzaw20@st.amu.edu.pl

The Synergy Between European Union Data Protection and Digital Market Regulation

Abstract: This article examines the relationship between the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA), with a particular focus on how gatekeeper obligations affect the legal bases for personal data processing. While Article 6 GDPR provides several lawful grounds, such as consent, necessity for contract performance, and legitimate interests, Article 5(2) DMA significantly restricts gatekeepers' ability to rely on the latter two. The author highlights the increasing regulatory pressure to ensure that consent is freely given, especially in light of EDPB Opinion 08/2024 and the European Commission's April 2025 decision concerning the "consent or pay" model. The analysis reflects the EU's broader effort to reinforce fundamental rights and ensure genuine user autonomy in the context of digital platform regulation.

Keywords: General Data Protection Regulation, Digital Markets Act, consent, user autonomy

Introduction

In recent years, the pace of technological advancement has been unprecedented. When the General Data Protection Regulation (GDPR) entered into force, it was hailed as a groundbreaking step towards safeguarding personal data in the European Union.[1] However, the digital ecosystem has since evolved dramatically. Artificial Intelligence systems have matured from experimental prototypes to widely deployed tools embedded in consumer platforms, while dominant digital platforms—such as Google, Meta, and Amazon—have deepened their role as essential intermediaries in everyday life.

This rapid evolution has exposed the growing gap between law and technology. Although the GDPR introduced comprehensive rules on personal data processing, many of its provisions are ill-suited to addressing the complexities of data-driven business models, especially those built around profiling, behavioural advertising, and algorithmic decision-making. Moreover, the regulation did not anticipate the extent to which digital platforms would accumulate structural power—not merely as data controllers, but as de facto gatekeepers of access to digital markets and information flows.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, pp. 1–88), hereinafter: GDPR.

Recognising this regulatory lag, the European Union has undertaken a series of legislative initiatives aimed at recalibrating the digital legal order. Chief among them are the Digital Markets Act (DMA),[2] the Digital Services Act (DSA),[3] and the recently adopted AI Act.[4] These instruments signal a shift from traditional, reactive forms of data protection and competition enforcement to a more anticipatory and systemic approach. The DMA introduces *ex ante* obligations for designated gatekeepers, aiming to restore contestability and fairness in core platform services. At the same time, the DSA enhances accountability in online content moderation, while the AI Act seeks to govern algorithmic systems according to their societal risks.

This ambitious regulatory agenda has not gone unnoticed internationally. Leading figures in the current administration of the United States have accused the EU of disproportionately targeting American tech giants under the guise of digital regulation. This criticism reflects not only geopolitical tensions but also deeper disagreements about the scope and legitimacy of regulating data, competition, and innovation in digital markets.[5]

Against this background, this article examines the intersection of data protection and competition law in the regulation of gatekeepers, focusing on the evolving role of legal bases for data processing under the GDPR considering the DMA's provisions. It argues that the EU's efforts to impose structural obligations on dominant platforms are both necessary and normatively justified—but that their success depends on resolving underlying legal tensions, particularly regarding the role of user consent, data portability, and the allocation of enforcement competences.

1. The Role and Limits of Consent under the GDPR

Consent remains one of the most prominent legal bases for processing personal data under the GDPR, reflecting the foundational value of informational self-determination in European data protection law. It is often regarded as the most transparent and user-centric form of legitimising data processing, premised on the autonomy of

[2] 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) (OJ L 265, 12.10.2022, pp. 1–66), hereinafter: DMA.

[3] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, pp. 1–102), hereinafter: DSA.

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024), hereinafter: AI Act.

[5] Aleksandra Wójtowicz, "U.S. and EU Clash over Regulation of Digital Content Moderation," Polski Instytut Spraw Międzynarodowych, published 21 March 2025, https://pism.pl/publications/us-and-eu-clash-over-regulation-of-digital-content-moderation.

the data subject. Article 6(1)(a) GDPR recognises consent as a lawful basis, further elaborated in Article 4(11) and Recital 32, which emphasise the need for consent to be freely given, specific, informed, and unambiguous.

Yet, in practice, the deployment of consent by powerful digital platforms—especially those designated as "gatekeepers" under the DMA—has proven deeply problematic. These entities frequently operate in structurally imbalanced environments, where users are presented with take-it-or-leave-it choices, nudged by manipulative interface designs (so-called "dark patterns"), or deprived of viable alternatives. As a result, consent mechanisms risk becoming formalistic rather than meaningful, undermining the normative premise of voluntariness. Empirical and regulatory findings have confirmed that many gatekeepers have either circumvented the requirement for consent through reliance on alternative legal grounds, such as "legitimate interest," or implemented consent flows that fall short of the GDPR's stringent standard.

Moreover, the economic incentives propelling data-driven platform models create a systemic tension between the ideal of user control and the commercial logic of maximising data extraction. Gatekeepers have a structural interest in steering users toward consenting to broad, bundled processing purposes, often making withdrawal difficult or opaque. This has raised fundamental concerns about whether consent can function effectively in digital ecosystems dominated by a small number of entrenched intermediaries.

The shortcomings in enforcing meaningful consent under the GDPR—especially in environments shaped by data-driven gatekeepers—have underscored the limitations of traditional legal frameworks in addressing structural power asymmetries. Consent, while a cornerstone of the GDPR, has proven challenging to operationalise effectively in practice, particularly when deployed by entities exercising considerable market power.

The European Data Protection Board (EDPB), in its Guidelines 05/2020 on consent, elaborates that valid consent must be obtained through clear affirmative action, and that mechanisms such as pre-ticked boxes or user inactivity cannot be considered sufficient.[6] The CJEU reinforced this interpretation in its *Planet49* ruling (C-673/17), stating unequivocally that consent must involve active behaviour and cannot be presumed.[7] The Court further held that storing or accessing information on a user's device necessitates informed consent, thereby rejecting opt-out models. Importantly, consent must be granular—separately obtained for each distinct processing operation—and capable of being withdrawn without detriment. Controllers are bound by the accountability principle to demonstrate the validity of the consent they collect.[8]

---

[6] European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679*, Version 1.1 (4 May 2020).

[7] Judgment of the Court of Justice of the European Union of 1 October 2019, *Planet49* (C673/17), ECLI:EU:C:2019:801.

[8] Paweł Barta et al., "Commentary on Article 6," in *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem*

These stringent requirements establish a high threshold for valid consent, particularly when sought by actors with significant market dominance, such as the digital platforms designated as gatekeepers under the Digital Markets Act. The asymmetry in bargaining power between individuals and dominant platforms heightens the risk that consent will not be freely given, informed, or genuinely revocable. In such contexts, the formal appearance of consent may mask de facto coercion or user habituation to unavoidable data practices—issues that traditional data protection mechanisms have struggled to resolve effectively.

Despite ongoing enforcement efforts by national data protection authorities (DPAs) and the European Data Protection Board, the GDPR's architecture has revealed its limitations in confronting systemic abuses at scale. Similarly, classical EU competition law, rooted in ex post enforcement under Articles 101 and 102 TFEU, has proven slow and ill-suited to address the anticipatory and structural dimensions of digital market power. Although notable efforts such as *Bundeskartellamt v. Meta* have introduced privacy into the antitrust discourse, these developments remain fragmented and jurisdictionally constrained.[9]

In response, the European Union introduced the DMA as an *ex ante* regulatory regime tailored to the systemic risks posed by gatekeepers. This instrument seeks to prevent, rather than merely remedy, exploitative or exclusionary conduct. Crucially, the DMA addresses certain shortcomings of the GDPR by explicitly prohibiting the combination of personal data across services without valid user consent and mandating interoperability, data access, and platform neutrality. These obligations function independently of the GDPR, but they also reinforce its goals by embedding structural guarantees that pre-empt coercive data practices.

2. Consent under the DMA and Its Impact on the GDPR Legal Framework

The Digital Markets Act introduces a paradigm shift in regulating dominant digital platforms by imposing *ex ante* obligations on so-called *gatekeepers*. According to Article 3(1) DMA, a gatekeeper is an undertaking that provides a core platform service and (a) has a significant impact on the internal market, (b) operates a core platform service which serves as an important gateway for business users to reach end users, and (c) enjoys an entrenched and durable position in its operations—or is

danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Komentarz in *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, ed. Paweł Litwiński, 1st ed. (Wydawnictwo C.H. Beck, 2021).

[9] Judgment of the Court of Justice of the European Union of 4 July 2023, *Bundeskartellamt v. Meta* (C-252/21), ECLI:EU:C:2023:537.

foreseeably acquiring such a position. The designation procedure under Article 3(4) further empowers the European Commission to formally list undertakings as gatekeepers, based on qualitative and quantitative criteria, creating a clearly defined regulatory perimeter.

Once designated, gatekeepers are subject to a set of obligations outlined in Articles 5, 6, and 7 DMA. Among these, Article 5(2) plays a critical role in the data governance framework, as it introduces a substantive limitation on how gatekeepers may process personal data. It provides that a gatekeeper shall not: "without complying with the relevant provisions of Regulation (EU) 2016/679: (a) process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper; (b) combine personal data from the relevant core platform service with personal data from any other core platform services or from any other services provided by the gatekeeper or with personal data from third-party services; (c) cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services; and (d) sign in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and has given consent in the sense of Article 4(11) and of Article 7 of Regulation (EU) 2016/679."

This cross-reference to the GDPR has a profound legal effect. It imports into the DMA context the high threshold for valid consent developed under Articles 4(11), 6(1)(a), and 7 GDPR, but operationalises it in a structurally different regime. Unlike the GDPR, where consent is merely one of six equally valid legal bases for processing under Article 6(1), the DMA effectively eliminates alternative grounds, such as contract performance or legitimate interest, in the specific scenario of combining personal data across services.

In the case of contractual necessity (Art. 6(1)(b) GDPR), processing must be genuinely necessary to fulfil the contract's core service. Common breaches are related to asserting that extensive profiling or targeted ads are "essential" for a platform's primary service (despite EDPB guidance that truly "necessary" means it cannot function without such processing) or combining user data from multiple services. In *Bundeskartellamt v. Meta*, the court emphasized that "needing" data for customized features does not automatically make it "necessary" for basic service functionality.[10] EDPB repeatedly underscores a narrow interpretation of "necessary." Customization or targeted advertising is typically not deemed inherently necessary for providing the core functionality of a service.

Moreover, when it comes to legitimate interest (Art. 6(1)(f) GDPR), the controller's interest must be balanced against the data subject's rights and freedoms. Common breaches include treating revenue-driven advertising interests as auto-

[10] Judgment of the Court of Justice of the European Union of 4 July 2023, *Bundeskartellamt v. Meta*.

matically "legitimate" or failing to offer meaningful opt-outs that would allow users to avoid invasive tracking or profiling. EDPB guidelines and CJEU rulings highlight that balancing must account for the platform's market power and user vulnerability; a gatekeeper's interest in personalized ads does not necessarily override user privacy rights.

Consequently, DMA effectively narrows the scope of legal grounds for data processing by introducing stricter conditions. The EDPB has highlighted this limitation in its Opinion 08/2024, emphasizing that gatekeepers must not use their dominant position to nudge users into providing consent under pressure or as a precondition for accessing the service.[11]

In other words, gatekeepers cannot rely on other legal bases from Article 6 GDPR to justify cross-service data processing—even where such justifications might otherwise be permissible under the GDPR. This approach constitutes a deliberate legislative recalibration. By embedding a strict consent requirement directly into competition regulation, the DMA aims to prevent gatekeepers from leveraging their ecosystem power to circumvent user autonomy through contract or default design choices. It explicitly precludes common strategies such as bundling consent with terms of service or invoking legitimate interest for behavioural profiling—tactics frequently employed to sidestep the high bar for GDPR-compliant consent.

Moreover, the DMA requires that such consent be "freely given, specific, informed and unambiguous," echoing the language and interpretative standards from the GDPR, including those elaborated in the *Planet49* ruling and EDPB Guidelines. Furthermore, gatekeepers are prohibited from using so-called "consent or pay" models without offering a genuinely equivalent no-cost alternative, particularly where the service is otherwise offered free of charge.[12] This interpretation, though not explicitly found in the text of the DMA, stems from recent enforcement actions, including the European Commission's April 2025 decision addressing Meta's use of such models.[13] In that decision, the Commission found that users were not given a real choice and that consent was not freely given, thereby breaching both GDPR standards and DMA obligations.

The two regimes operate in a complementary but asymmetric manner. While the GDPR governs the processing of personal data generally, the DMA constrains the structural preconditions under which certain processing is allowed, targeting systemic behaviours rather than isolated infractions. This differentiation responds to

[11] European Data Protection Board, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, adopted on 17 April 2024, available at: https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf , accessed 5 July 2025.

[12] Klaudia Majcher, "Freedom, Power, and Contestability: Interactions between Article 5(2) DMA and the GDPR," Kluwer Competition Law Blog, published 22 October 2024, https://legalblogs.wolterskluwer.com/competition-blog/freedom-power-and-contestability-interactions-between-article-52-dma-and-the-gdpr/.

[13] European Commission, *Decision on Meta's Consent Model*, published 23 April 2025, https://digital-markets-act.ec.europa.eu/commission-finds-apple-and-meta-breach-digital-markets-act-2025-04-23_en.

the specific challenges posed by digital conglomerates, whose ability to accumulate and repurpose user data at scale cannot be adequately addressed by the reactive enforcement model of the GDPR alone.

3. Enforcement Challenges and Institutional Division of Competences

While the elevation of consent as a cornerstone of lawful data processing under both the GDPR and the DMA appears, in principle, to empower data subjects, the increasing reliance on consent also presents significant challenges. Scholars have argued that an overemphasis on consent risks creating a compliance burden that paradoxically undermines user autonomy. As Ella Corren points out, the proliferation of consent requests may lead to "consent fatigue," rendering individuals less capable of making meaningful choices and more likely to accept intrusive processing by default.[14] This critique suggests that the strengthening of consent mechanisms does not automatically translate into stronger data protection, especially when power asymmetries between users and gatekeepers persist.

These difficulties are further compounded by the structural divergence in enforcement mechanisms under the GDPR and the DMA. The GDPR is enforced primarily by national data protection authorities (DPAs), coordinated through the European Data Protection Board (EDPB), with a significant role played by lead supervisory authorities under the so-called one-stop-shop mechanism. By contrast, enforcement of the DMA is centralized in the hands of the European Commission, which acts as the sole enforcer. This institutional asymmetry creates potential tensions: while the GDPR leaves room for diverse national interpretations and enforcement approaches, the DMA pursues uniform application by design.[15]

Moreover, the enforcement competences of the Commission under the DMA extend to practices that also fall within the remit of data protection law. Article 5(2) DMA, as previously discussed, prohibits certain types of personal data processing unless based on GDPR-standard consent. However, it is the Commission—not the DPAs—that enforces this prohibition. This dual structure raises open questions about fragmentation, duplication of proceedings, and the risk of conflicting interpretations regarding what constitutes valid consent. While coordination

[14] Ella Corren, "The Consent Burden in Consumer and Digital Markets," *Harvard Journal of Law & Technology* 36, no. 2 (2023): 551.

[15] Iga Małobęcka-Szwast, "Commentary on Article 5," in *Akt o rynkach cyfrowych—Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828. Komentarz* in *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, ed. Mateusz Grochowski, 1st ed. (Wydawnictwo C.H. Beck, 2024).

mechanisms may be developed in the future, the current regulatory framework lacks a formalized process for resolving such overlaps between the data protection and competition regimes.

In response to the DMA's constraints, some gatekeepers may restructure their offerings to separate essential from non-essential processing activities, thereby reducing reliance on personal data for ad-targeting or cross-service analytics. The GDPR principle of data minimization resonates with the DMA's insistence on functional user alternatives that do not rely on exhaustive data collection.[16] Platforms might, for instance, develop "light" service versions with minimal data usage to enable a genuine choice for users who opt out of more invasive practices.

Debates persist regarding whether gatekeepers can lawfully require payment from users who decline data-intensive processing. The DMA suggests that simply imposing a fee on non-consenting users may be impermissible if it effectively nullifies the freedom to say no. Any such model would be subject to scrutiny under Article 5 of the DMA, particularly if a free version of the service exists or if the pay-only alternative appears punitive. As enforcement agencies clarify the regulatory landscape, it remains to be seen whether certain "consent or pay" options will survive under the dual GDPR–DMA regime.

In essence, the DMA amplifies the GDPR principle of free and informed user decision-making by prohibiting gatekeepers from relying on weaker or overbroad legal bases for data processing, such as legitimate interest or contractual necessity, when delivering key platform services. This dual framework fosters greater user autonomy and curtails exploitative data practices. Gatekeepers can no longer simply rely on fallback justifications; they need valid, uncoerced consent.

Although the GDPR and the DMA are grounded in different legal spheres, they converge on a shared objective of ensuring genuine user autonomy. The GDPR seeks to protect fundamental rights by demanding a robust legal basis for data processing, while the DMA aims to preserve market contestability by preventing gatekeepers from leveraging their dominance to coerce consent. This synergy is reflected in the stringent conditions the DMA imposes on gatekeepers, effectively reinforcing the GDPR's emphasis on freely given, informed, and specific user consent.

The European Data Protection Board and the European Commission have announced plans to coordinate on issues at the intersection of the GDPR and DMA, an initiative likely to yield more detailed guidance on how gatekeepers should reconcile data protection obligations with competition-based restrictions.[17] Future case law, enforcement decisions, and interpretive documents will further clarify how these

[16] Hatim Rahman et al., "Taming Platform Power: Taking Accountability into Account in the Management of Platforms," *Academy of Management Annals* 18, 1 (2025): 251–94, https://doi.org/10.5465/annals.2022.0090.

[17] European Data Protection Board, *EDPB to Work Together with the European Commission to Develop Guidance on the Interplay of the GDPR and the DMA*, 2024.

two regulatory frameworks should be applied, particularly in complex scenarios involving multi-service integration and targeted advertising at scale.

Through Article 5 of the DMA, EU law now exerts a direct influence over which GDPR legal grounds can be legitimately cited by gatekeepers. The result is a narrower scope for contractual necessity and legitimate interest, with corresponding emphasis on uncoerced user consent. In this manner, the DMA both reinforces and extends GDPR principles by insisting on robust user autonomy, enhanced accountability for dominant platforms, and the prohibition of exploitative data practices. The evolution of EU law thus illustrates how data protection and the DMA's *ex ante* rules increasingly function as complementary tools to address the challenges of pervasive data-driven business models. Dominant platforms must recognise that genuine user freedom is not merely an aspiration within the GDPR; under the DMA, it has become a firm legal requirement with tangible market and enforcement implications.

Summary

The European Union's regulatory response to the rapidly evolving digital ecosystem reflects both the ambition and the difficulty of legislating in a space where technological innovation consistently outpaces legal adaptation. While the General Data Protection Regulation laid the foundation for a fundamental rights-based approach to personal data processing, the Digital Markets Act introduces a complementary *ex ante* instrument that directly targets the structural imbalances in platform-dominated markets. The effectiveness of this dual framework now hinges on the European Commission's enforcement strategy.

This article has demonstrated that although the DMA is formally distinct from the GDPR, it places substantial constraints on the data processing practices of gatekeepers by limiting their reliance on weaker legal bases such as legitimate interest or contractual necessity. By mandating real, unbundled user choice, the DMA effectively elevates the standard for valid consent in contexts where market dominance might otherwise undermine voluntariness.

Recent developments confirm this regulatory trajectory. The EDPB's Opinion 08/2024 and the European Commission's decision concerning Meta's "consent or pay" model exemplify a growing synergy between data protection and digital market regulation. These developments suggest a strategic shift from purely parallel enforcement to a more integrated regulatory philosophy—one that embeds data protection concerns directly into competition-driven obligations.

Notably, the DMA departs from the GDPR's decentralised enforcement model by granting the European Commission exclusive competence to monitor and sanction gatekeeper conduct. This centralisation aims to ensure coherence and efficiency in

enforcement, yet it also introduces challenges related to institutional coordination and potential regulatory fragmentation. The interplay between the GDPR, national DPAs, and the Commission under the DMA thus raises important normative and practical questions, particularly concerning the consistency of standards, the risk of overlapping obligations, and the allocation of investigative authority. As enforcement practice evolves, the Union's capacity to reconcile its dual commitment to fundamental rights and fair markets will be increasingly tested.

In this sense, the GDPR provides the normative grammar for lawful data processing, whereas the DMA imposes a structural syntax that reshapes how gatekeepers must operationalize consent, transparency, and accountability. Together, these regimes not only reinforce one another but also articulate a broader vision of user empowerment in the digital age. By aligning fundamental rights protection with market fairness, the EU aspires to re-balance the asymmetrical power relationship between dominant platforms and individual users—an endeavour whose success will ultimately depend on coherent, robust, and forward-looking enforcement.

BIBLIOGRAPHY

Barta, Paweł, Maciej Kawecki, and Paweł Litwiński. "Commentary on Article 6." In *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Komentarz* in *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, edited by Paweł Litwiński, 1st ed. Wydawnictwo C.H. Beck, 2021.

Corren, Ella. "The Consent Burden in Consumer and Digital Markets." *Harvard Journal of Law & Technology* 36, no. 2 (2023): 551–613.

Majcher, Klaudia. "Freedom, Power, and Contestability: Interactions between Article 5(2) DMA and the GDPR." Kluwer Competition Law Blog, published 22 October 2024. https://legalblogs.wolterskluwer.com/competition-blog/freedom-power-and-contestability-interactions-between-article-52-dma-and-the-gdpr/.

Małobęcka-Szwast, Iga. "Commentary on Article 5." In *Akt o rynkach cyfrowych—Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828. Komentarz* in *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, edited by Mateusz Grochowski, 1st ed. Wydawnictwo C.H. Beck, 2024.

Rahman, Hatim A., Arvind Karunakaran, and Lindsey D. Cameron. "Taming Platform Power: Taking Accountability into Account in the Management of Platforms." *Academy of Management Annals* 18, 1 (2025): 251–94. https://doi.org/10.5465/annals.2022.0090.

Wójtowicz, Aleksandra. "U.S. and EU Clash over Regulation of Digital Content Moderation." Polski Instytut Spraw Międzynarodowych, published 21 March 2025. https://pism.pl/publications/us-and-eu-clash-over-regulation-of-digital-content-moderation.