cerre

# DMA REGULATORY INTERPLAYS

ISSUE PAPER

*February 2026*

Alexandre de Streel
Giorgio Monti

As provided for in CERRE's bylaws and procedural rules from its “Transparency & Independence Policy”, all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: ACM, Amazon, Apple, Arcep, DuckDuckGo, EETT, Google, Mozilla, Qualcomm. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.



info@cerre.eu – www.cerre.eu

# Executive Summary

This issue paper calls for a structured strategy to ensure coherence across the EU digital rulebook, with particular attention to the implementation of the Digital Markets Act (DMA). **As overlaps between the DMA and instruments such as the Digital Services Act (DSA), IP laws or the General Data Protection Regulation (GDPR) become more operationally significant, policymakers should adopt clear interpretative guidance that identifies synergies, mitigates tensions, and transparently manages unavoidable trade-offs**. Joint guidelines—developed through open and participatory processes—should go beyond aggregating institutional positions and instead provide practical compliance pathways, clarify proportionality standards, and specify where safe harbours may apply. In particular, structured frameworks are needed to reconcile DMA interoperability and data-access obligations with intellectual property rights and data protection requirements, ensuring that enforcement remains both effective and innovation-friendly.

To reduce regulatory fragmentation, the report recommends **strengthening institutional coordination and rationalising overlapping obligations**. Legislative simplification through targeted omnibus reforms should eliminate redundant rules while preserving substantive protections, and future initiatives could consolidate enforcement cooperation across the more than 270 EU and national bodies involved in digital oversight. The Commission's planned "digital fitness check" should be grounded in rigorous, evidence-based evaluation of the DMA's impact, supported by systematic data collection and a dedicated assessment framework. In parallel, enforcement practices should prioritise EU-level solutions where conduct is cross-border in nature, limiting the risk of divergent national remedies and gold-plating that increase compliance costs and weaken the internal market.

With respect to data protection, the paper recommends **operationalising coherent parallel application of the DMA and GDPR**. Clear workflows should be developed to guide cooperation between gatekeepers and business users, for instance in areas such as consent management and data portability. Regulators should promote tested, user-friendly choice architecture and require gatekeepers to substantiate how compliance designs achieve legal objectives. Where guidance suggests specific compliance measures, authorities should clarify whether these create presumptions of compliance and ensure that recommendations are proportionate and grounded in a clear legal basis.

Finally, the issue paper highlights the **need for more governance of enforcement**. Enhanced dialogue among regulators should aim to produce unified compliance solutions rather than duplicative or conflicting remedies. In the medium term, more structured and pragmatic regulatory cooperation with initiatives like the Digital Clearing House 2.0 should be encouraged. In the longer term, policymakers may consider the establishment of an independent EU digital enforcement agency to ensure consistency and effectiveness. In private enforcement, national courts should coordinate closely with the Commission and exercise caution when granting injunctive relief, preserving the DMA's principle that gatekeepers retain discretion in designing compliance unless specific remedies are strictly necessary. Together, these recommendations aim to reduce legal uncertainty, lower compliance burdens, and enhance the effectiveness and legitimacy of the EU's digital regulatory framework.

# Table of Contents

# 1. Coherence of the EU Digital Rulebook

## 1.1. The importance of regulatory consistency

The interplay between the Digital Markets Act (DMA) and the other EU and national legal frameworks applicable to DMA designated gatekeepers and benefiting business users has become an increasingly salient issue as DMA enforcement advances. **As concrete cases emerge, a range of trade-offs between the different rights, objectives, and interests protected by distinct legal instruments which were left unresolved by the EU legislator are now becoming more visible.** If left insufficiently addressed, these tensions risk undermining regulatory predictability, legal certainty, and consistency across the EU digital rulebook. This challenge is particularly acute in the current policy context, as the EU seeks to boost productivity and regain global competitiveness, with the digital sector widely recognised as a key engine of growth and innovation.[1]

In its recent Report on the interaction between the Digital Services Act (DSA) and 54 other EU legal acts, the European Commission observed that: [2]

> *"The (stakeholders) surveys highlight a broad consensus on the need for clarity, coherence, and coordination within the Union's digital regulatory landscape. (…) To ensure effective enforcement, protection of users, and a level playing field for businesses, stakeholders call for streamlined guidance, better institutional cooperation, and practical tools that make the regulatory framework more accessible and predictable."*

These observations apply with equal force to the interaction between the DMA and other areas of EU law. So far, the most discussed DMA interplays relate to competition law (as the DMA was partly based on antitrust cases), privacy rules (as we explained in section 2) and cybersecurity rules.[3] However, several other regulatory interplays are key for an effective and proportionate implementation of the DMA, in particular with the DSA or the IP rules.

### *The Interplay with Digital Services Act*

The DMA and the DSA form two complementary pillars of the EU digital rulebook. Although the two instruments pursue distinct objectives—contestability and fairness in the case of the DMA, and safety, transparency, and accountability in the case of the DSA—they apply to overlapping categories of large digital service providers. As such, they should be understood not as isolated regimes, but as interlocking components of a broader regulatory framework. The DMA seeks to prevent entrenched gatekeepers from leveraging their intermediation power to distort competition and stifle innovation. The DSA, by contrast, aims to mitigate systemic risks related to illegal content, disinformation, fundamental rights violations, and societal harms arising from the functioning of online platforms. Despite these different focal points, **both regulations share several underlying principles**, such as

[1] Draghi M. (2024), The future of European competitiveness; Part B: In-depth analysis and recommendations, Report to the Commission.

[2] Report from the Commission of 17 November 2025 on the application of Article 33 of Regulation 2022/2065 and the interaction of that Regulation with other legal acts, COM(2025) 708, p.10.

[3] Those interplays were already discussed in last year CERRE DMA Report: https://cerre.eu/publications/dma-implementation-forum/

increasing transparency of platform practices, reducing information asymmetries, enhancing accountability of large digital intermediaries, and protecting users (both business users and end users) from unfair or harmful practices. In this sense, the DMA and DSA can be seen as two sides of the same coin: one addressing market structure and economic power, the other addressing systemic risks and societal impact.

Several areas offer clear opportunities for coherent and mutually reinforcing implementation.

- **Transparency of rankings and recommender systems:** the DMA requires gatekeepers to ensure transparency in ranking practices, particularly where self-preferencing or discriminatory treatment may distort competition. The DSA, in turn, imposes transparency obligations concerning recommender systems, including the main parameters used and the options available to users to modify or influence those systems. A coordinated interpretation of these provisions can enhance both economic fairness and user autonomy. Greater transparency in ranking and recommender systems can enable business users to compete on more equal terms (DMA objective), empower users to understand and control how content is curated and prioritised (DSA objective), and facilitate regulatory oversight by reducing informational asymmetries. Ensuring consistency in technical and disclosure standards across both instruments would reduce compliance complexity while strengthening regulatory effectiveness.
- **Harmful online choice architecture (dark patterns):** the DSA contains explicit provisions addressing manipulative or deceptive interface designs that distort user decision-making. The DMA addresses unfair practices imposed by gatekeepers on business users and end users, including restrictions on switching, steering, or interoperability. There is clear potential for synergy: manipulative interface design can both harm users (a DSA concern) and entrench gatekeeper power by increasing switching costs or limiting effective multi-homing (a DMA concern). Coordinated enforcement could ensure that interventions targeting dark patterns also support broader contestability goals.
- **Online advertising:** the DMA includes obligations on online ad transparency and concerning data combination and restrictions on leveraging user data across services without consent, thereby targeting competitive advantages derived from data accumulation. The DSA establishes transparency obligations for online advertising, including disclosures about targeting criteria and advertiser identity. Together, these measures can increase transparency in digital advertising markets, reduce exploitative or opaque targeting practices, limit the entrenchment of data-driven market power, and strengthen user trust and accountability.

To avoid fragmentation or inconsistent interpretations, **enforcement actions should consider the cumulative impact of obligations under both regimes**. Moreover, evidence gathered in DSA systemic risk assessments could inform DMA investigations into market practices and remedies under one framework should not undermine objectives pursued under the other.

**Moreover, while synergies are significant, care must also be taken to avoid duplicative or conflicting obligations.** Clear guidance should delineate where obligations pursue distinct objectives and where they overlap substantively. Legal certainty is particularly important for platforms subject to extensive reporting, auditing, and transparency requirements under both regimes. A coherent interpretative framework should aim to align definitions and technical standards where feasible, clarify the

interaction between transparency obligations and ensure proportionality in cumulative compliance burdens.

## *The Interplay with IP rights*

IP protection constitutes a fundamental component of the European Union's legal order. The right to intellectual property is explicitly protected under Article 17(2) of the EU Charter of Fundamental Rights and is further embedded in international agreements such as the TRIPS Agreement. The rationale underpinning IP protection is well established: by granting exclusive rights to inventors and creators—including those responsible for the diffusion and commercialisation of innovations—IP law seeks to incentivise investment in research, development, and creative production. Therefore, **there is no inherent conflict between the objectives of IP law and the DMA as both regulatory frameworks ultimately pursue innovation**. IP law does so by rewarding and protecting inventive and creative efforts, while the DMA seeks to preserve contestability and fairness in digital markets, thereby ensuring that innovation is not stifled by entrenched gatekeeper power. In principle, competitive digital markets and robust IP protection are mutually reinforcing.

However, **tensions may arise in practice**. Certain DMA obligations—such as interoperability requirements or data access mandates —may intersect with protected IP rights, including patents, copyright in software or database rights.[4] In such situations, two analytical steps are crucial.

First, it is essential to clearly **identify the policy choice made by the EU legislator** when adopting the DMA. Where the DMA imposes specific obligations that potentially intersect with IP rights, this reflects a conscious legislative balancing between market contestability and exclusivity-based incentives. Importantly, the recognition of IP as a fundamental right does not render it absolute. Under EU law, fundamental rights—including property rights—may be subject to limitations, provided that such limitations are provided for by law, respect the essence of the right, pursue objectives of general interest recognised by the EU, and comply with the principle of proportionality. The DMA itself embodies a legislative determination that ensuring fair and contestable digital markets constitutes an objective of general interest of high importance within the internal market.

Second, in **implementing and enforcing the DMA, authorities—primarily the European Commission—must apply its provisions in an effective and proportionate manner**, in line with the general principles of EU law and the Charter. This entails a necessity assessment as the DMA obligations that intersect with IP should be effective enough and go no further than necessary to achieve contestability and fairness; this implementation is context-sensitive as enforcement decisions should carefully distinguish between legitimate exercises of IP rights and strategic uses of IP to entrench gatekeeper power. A rigid or overly expansive interpretation of DMA obligations could risk undermining the incentive structures that IP law seeks to preserve. Conversely, an overly deferential approach toward IP claims could frustrate the DMA's core objective of reducing structural barriers to entry and expansion in digital markets.

To ensure legal certainty and coherence, policymakers and enforcement authorities should articulate a **structured framework** clarifying how possible specific and substantiated IP claims could be assessed

[4] For example, interoperability mandates could require gatekeepers to provide access to interfaces or technical information that is otherwise protected under IP regimes. Similarly, data portability and access provisions may raise concerns where datasets are subject to copyright or database protection.

in DMA proceedings. Such a framework could require gatekeepers invoking IP protection to substantiate the scope and necessity of the claimed exclusivity, and for the Commission to assess whether the IP right is being exercised in a manner consistent with its essential function, evaluate whether equally effective and less restrictive alternatives are available and consider the long-term dynamic effects on innovation, both at the level of the gatekeeper and for third-party market participants. By making the balancing exercise transparent and predictable, the EU can reduce legal uncertainty and mitigate litigation risks while preserving both innovation incentives and competitive market structures.

## 1.2. How to achieve regulatory consistency

**To manage and rationalise regulatory interdependencies within the EU digital acquis**, there are several legal and institutional mechanisms.

First, the **Commission could adopt interpretative guidelines—potentially developed jointly with other EU institutions and bodies—to clarify the interaction between different legislative instruments**. The joint Commission–European Data Protection Board (EDPB) Guidelines on the interplay between the DMA and the GDPR is the first example of this approach;[5]

This first strategy, which remains at an early stage, is particularly valuable insofar as it has the potential to enhance regulatory predictability and consistency in a flexible manner and without reopening long and complex legislative negotiations. But because soft law does not change hard law, it is always without prejudice of the interpretation of the legal text by the Courts. We discuss in more detail the draft Joint Guidelines on DMA-GDPR in the next section. At this stage, suffice it to say that the process for adopting those joint guidelines should be transparent and participatory involving all the stakeholders. Equally important, the outcome should not amount to a mere aggregation of institutional, legal or policy positions. Rather, it should constitute a coherent piece of soft law that clearly identifies how synergies between the respective legal frameworks can be maximised, how tensions can be mitigated, and how unavoidable trade-offs can be resolved in practice.

Second, the **Commission has initiated a process of legislative simplification through so-called omnibus proposals**. To date, three such proposals have been tabled with a view to simplifying the EU digital acquis: two primarily addressing data-related legislation, and a one focused on artificial intelligence.[6]

This second strategy seeks to rationalise the EU digital rulebook by removing or consolidating overlapping regulatory obligations. A prominent example is the Digital Omnibus proposal of November 2025, which includes a proposal to repeal the Platform-to-Business (P2B) Fairness Regulation.[7] To the extent that the DMA already contains a range of obligations designed to ensure fairness in platform-to-business relations for gatekeepers, this repeal may be justified. Moreover, while the DMA and the DSA introduce asymmetrical regulation targeted at platforms with significant market power, the P2B Fairness Regulation applied horizontally to all platforms, regardless of their

[5] EC-EDPB Joint draft Guidelines of October 2025 on the interplay between the DMA and the GDPR.
[6] COM (2025)501 and COM(2025) 837 for data; COM(2025) 836 for AI.
[7] Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ [2019] L 186/55.

economic position. From this perspective, its repeal can be seen as a correction of regulatory overreach, with the potential benefit of alleviating compliance burdens for smaller platforms.

At the same time, several substantive elements of the P2B Fairness Regulation could usefully inform DMA implementation through guidance. For example, Article 5 of the P2B Regulation and the associated guidelines,[8] which establishes transparency requirements regarding the ranking of search results vis-à-vis business users, could provide a helpful interpretative framework for compliance with Article 6(5) DMA. Similarly, Articles 11 to 13 on internal complaint-handling systems and alternative dispute resolution mechanisms could serve as reference points for designing effective and proportionate dispute resolution frameworks for gatekeepers under the DMA.

In addition, a future omnibus proposal could be tabled to strengthen both the legal capacity and the incentives for cooperation among the EU and national regulators responsible for enforcing the digital acquis—numbering more than 270,[9] according to the Draghi Report. As discussed in Section 3, this would entail the establishment of a dedicated secretariat to support such cooperation, as well as the introduction of mechanisms allowing for the exchange of confidential information.

Third, the **Commission has announced a "digital fitness check" intended to assess how different elements of the EU digital rulebook operate in combination**. This exercise aims to identify synergies and good practices, as well as remaining gaps, overlaps, and inconsistencies—both at the substantive and institutional levels.[10]

This third strategy has the potential to support the most ambitious reforms, as it could enable a more systematic streamlining of the EU digital rulebook at both the substantive and institutional levels. For this exercise to be effective, however, the Commission will need to engage in a more explicit and rigorous analysis of the trade-offs between overlapping legal regimes and the interests they protect.[11] This, in turn, requires a robust, evidence-based evaluation of the core instruments of the digital rulebook, including the DMA. In a companion issue paper on the impact of the DMA, we therefore call for the development of a dedicated evaluation framework tailored to the DMA's objectives and enforcement mechanisms, as well as for the systematic collection of relevant empirical data.

[8] Commission Guidelines of 7 December 2020 on ranking transparency pursuant to Regulation 2019/1150 of the European Parliament and of the Council, OJ [2020] C 424/1.

[9] Draghi Report, Part A, p.26.

[10] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/15554-Digital-fitness-check-testing-the-cumulative-impact-of-the-EUs-digital-rules_en.

[11] M. Bassini, M. Maggiolino and A de Streel, Better Regulation and Evaluation for the EU Digital Rulebook, CERRE Report, 2025: https://cerre.eu/publications/better-law-making-and-evaluation-for-the-eu-digital-rulebook/

# 2. Interplay with Data Protection Law

While we have commented on the relationship between the GDPR and the DMA in earlier reports,[12] this issue remains controversial and unresolved and there has been more activity in this policy space that affects how the DMA and the GDPR interact. Below, we discuss three developments. As with previous reports, **we do not discuss whether gatekeepers comply with EU Law. We identify legal and policy issues that affect the interpretation of the rules and the expected impact of the DMA** and make policy recommendations.

The documents discussed below rightly underscore the point that the **relationship between DMA and GDPR is not one whereby the former is a *lex specialis* to the latter.[13] Rather, the two Regulations must be read in a manner that enables the party subject to both obligations to comply with these in a coherent manner**. This is an important observation which should be set out regularly as many still argue that the lex specialis argument has a role to play. This is not the case here for two reasons. First, because the DMA explicitly limits the gatekeeper's entitlement to rely on certain legal bases of the GDPR to process data. Thus, there is no need to invoke a legal doctrine of lex specialis because the DMA provides for an explicit qualification of the GDPR when gatekeepers comply with Article 5(2) DMA. For all other provisions of the DMA, the GDPR applies in parallel and without modification. Second, because when consent is used as a legal basis in the DMA, then the gatekeeper must comply with both DMA and GDPR. That the DMA adds certain requirements in a specific instance does not turn it into a lex specialis.

## 2.1 Pay or consent models

On 17 April 2024 the European Data Protection Board issued an Opinion on consent or pay models.[14] This Opinion is limited to interpreting the GDPR considering recent case-law, notably the *Meta* judgment.[15] However, the EDPB has interpreted it in a way that in its view aligns with the DMA to ensure a coherent application.

The EDPB takes a restrictive reading of the ability of a large online platform to rely on a consent or pay model where the end user is presented only with an option to consent to personal data collection or to pay for the service and have no data collected.[16] It reiterates the view that 'personal data cannot be considered a tradeable commodity.'[17] However, this position is weakened by the advice it sets out, which is that the platform has to provide the end user with a third option which is free of charge, without behavioural advertising but with a form of advertising which involves the processing of less personal data. In other words, the **EDPB foresees a three-tiered choice architecture**: (i) pay to have a service where no personal data is collected save what is strictly needed to run the service; (ii) a free

[12] A. de Streel, R. Feasey and G. Monti, *DMA@1: Looking Back and Ahead*, CERRE report, 2025: https://cerre.eu/publications/dma-implementation-forum/.
[13] The doctrine of *lex specialis derogat legi generali* stands for the proposition that that a more specific legal provision should take precedence over a more general one when the two laws are in conflict.
[14] EDPB Opinion 08/2024 of 17 April 2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms.
[15] Case C-252/21 *Meta Platforms v Bundeskartellamt* EU:C:2023:537.
[16] In contrast the ICO in the UK takes a more permissive stance. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/online-tracking/consent-or-pay/about-this-guidance/.
[17] EDPB Opinion 08/2024, para 180.

version with less personal data collection which provides equivalent services to the end user if they share more data, where consent is needed; (iii) a free version with more personal data collection. The three-tiered option is one that appears to align with DMA recitals suggesting that end-users should be offered with a 'less-personalised but equivalent alternative.'[18] Irrespective of the merits of this approach to DMA compliance, it is hard to see how one can insist that personal data is not traded when end users are making a choice about how much data to reveal (and thus to trade) in exchange for the service.

What the EDPB Opinion is also weak on is the **design of choice architecture**, an issue which instead has been dealt with in part by the Italian competition authority (Autoritá Garante della Concorrenza e del Mercato, AGCM) in a commitment decision relating to Google using its consumer law powers, where the concern was that end-users were nudged to agree to more data collection and processing rather than to make choices to limit this.[19] We will discuss this case further later regarding its significance for inter-agency cooperation (see section 3). For now, it offers a useful case study on the importance of regulatory involvement in choice architecture.[20]

On substance, the AGCM's commitment decision means that Google will change its consent requests allowing users to understand more fully the implications of consenting to the use of personal data. It also provides that the user can limit consent only for certain services and does not expect a degradation of service if this choice is made. The commitment decision contains infographics to illustrate the choice screens and how Google plans to amend them. While a market test was carried out, it remains puzzling to us why the firm is not required to provide any evidence of having tested these choice screens and explaining why it considers these changes are effective. The screens are **tested by the AGCM for legal compliance,[21] but they are not tested for their effectiveness** in achieving the goal of the law, in this case consumer protection.[22] For example, it is assumed that sending an email to users about their choices and their impacts is suitable to repair any harm caused by previous choice options.[23] No evidence is used to determine if this is likely to be the effect of this measure. The design of choice screens is key for many obligations in the DMA and further efforts are needed to identify best practices.[24]

## 2.2 Joint Guidelines DMA/GDPR

The draft Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation were issued by the Commission and the EDPB on 9 October 2025 and were

[18] DMA, Recital 36. Meta's alignment with this is presently under review: Commission finds Apple and Meta in breach of the Digital Markets Act Press Release IP/25/1085 (23 April 2025).
[19] Case PS12714 (4 November 2025).
[20] A. Fletcher, 'Choice Architecture for End Users in the DMA' (CERRE, 2023), A. Fletcher and Z. Vasas, 'Implications of Behavioural Economics for the Pro-competitive Regulation of Digital Platforms (2025) 40 Oxford Review of Economic Policy 808.
[21] Case PS12714, section VII.
[22] On choice archicture and consumer protection, see C. Busch, A. Fletcher and M. Ledger, Towards an EU Consumer Law Fit for the Digital Age, CERRE Report, February 2026.
[23] Case PS12714 para 39.
[24] See for instance, https://research.mozilla.org/browser-competition/choicescreen/.

opened for comment until 4 December 2025.[25] At the time of writing responses are unavailable; below we provide our assessment.

### *2.2.1 Trade-offs and cooperation between gatekeepers and business users*

The draft, as the Opinion discussed above, explains that the **DMA and the GDPR should be interpreted in a comparable manner so that the objectives of both can be met**. However, we see that this is frequently challenging because the business models of some gatekeepers are based on extensive collection and processing of personal data. On the one hand, we agree that excessive collection and processing of personal data with weak or non-existent consent functionalities is harmful for end users. On the other hand, advertising-based business models provide end users with many valuable services and benefit small traders who can advertise effectively.[26] The DMA and competition law seek to make markets where this business model is prominent, as well as related ad tech markets, more contestable.[27] Similarly, while respect for personal data protection is vital, access to data is essential to stimulate competition in search markets and it has been argued that restrictive interpretation of anonymisation can create entry barriers that undermine the market opening effects of Article 6(11) of the DMA.[28] There are thus a number of **trade-offs to be addressed** by the regulators.

**Moreover, examples would be particularly helpful in situations where gatekeepers' compliance requires that they cooperate with business users**. Guidelines should help gatekeepers and business users understand their obligations and their rights under the DMA and under the GDPR. As long as they comply with both laws, gatekeepers remain free to differentiate their business models according to the level of privacy protection they offer. Some examples from the draft are selected below to illustrate the need for gatekeeper-business user cooperation in ensuring compliance with the DMA and therefore the **need of robust governance mechanisms** as explained in the companion paper on governance as a personal data breach caused by a business user can be a reputational risk for the gatekeepers.

- When it comes to Article 6(4) DMA, both gatekeepers and app developers are separate controllers, so both must comply with GDPR. The draft guidelines recognise that some coordination is needed, for example gatekeepers should avoid designing technical measures or entering into agreements that prescribe the way the app developer chooses to comply with the GDPR.[29]
- Under Article 6(4) DMA, in cases where there is a data breach, appropriate means for handling this jointly or alone are needed so that both parties comply with Articles 33 and 34 GDPR.[30]
- When the app store or app provider must seek consent to process personal data, the

[25] Draft available at: https://www.edpb.europa.eu/news/news/2025/dma-and-gdpr-edpb-and-european-commission-endorse-joint-guidelines-clarify-common_en.
[26] https://www.tse-fr.eu/sites/default/files/TSE/documents/sem2024/eco_platforms/aridor_juin_2024.pdf.
[27] See e.g. AGCM, App Tracking Transparency (16 December 2025). An executive summary is available here: https://en.agcm.it/dotcmsdoc/pressrelease/A561_SUMMARY.pdf. The AGCM does not question the legitimacy of the business model.
[28] See https://prufer.net/wp-content/uploads/2025/12/consultation-response-on-the-ec-edpb-draft-guidelines-jp.pdf.
[29] Para 93.
[30] Para 97.

gatekeeper must enable them to provide interfaces with prompts for consumers. Gatekeepers may offer some services to help developers, but the latter should remain free to select their own approach to GDPR compliance.[31]

- When data portability processes start (Article 6(9) DMA), both gatekeeper and the business that receive the ported data must comply with GDPR and the gatekeeper has to provide appropriate information about the recipients to the data subject. It may also have to provide the data recipient with tools to exclude from the dataset the personal data of individuals other than the end-user seeking portability.[32]
- Article 6(10) DMA compliance requires that gatekeepers allow business users to obtain the consent of end users for access to their personal data. The guidelines recognise that cooperation is needed so that gatekeepers facilitate this while recalling that GDPR compliance obligations vest on the business user as well.[33]

In all these instances, effective workflows are necessary for business users understand what options are available and what they can expect from gatekeepers and what technical options are available to them to both avail themselves of the DMA rights and comply with the GDPR. Any guide that facilitates cooperation will make entry more effective. Some of the workflow could be tested either by the Commission or in a consultation with business users and gatekeepers. Going even further, we can envisage that the workflow following those guidelines would be presumed to comply with the DMA if it is approved; this kind of safe harbour helps with planning and can lead to quicker compliance.

On pay or consent, the draft guidelines are aligned with the earlier EDPB Opinion and focus on the importance of '**user-friendly choices and consent designs**.'[34] However, this is a complex exercise since the guidelines explain that there there should be a separate opt-in for each purpose e.g., personalisation of content, personalisation of advertisements, and service development are three different purposes and a separate consent moment is required for each.[35] As we have explained in earlier reports and above, more efforts should be devoted to **designing choice architecture that allows end-users to understand what they are agreeing to**.[36] The DMA places an obligation on gatekeepers to demonstrate compliance (the same obligation is found in the GDPR[37]) and priority should be placed on requiring gatekeepers to explain why certain choice architecture has been selected, what kind of testing has been carried out.

Here also, a **multi-party regulatory dialogue - supported by robust governance mechanisms - may be of assistance** to develop a common understanding about appropriate choice architecture. In the medium term, arriving at a common understanding can reduce compliance costs and make choice easier for consumers if choice design is similar across all platforms.

[31] Paras 100-101.
[32] Paras 113-114.
[33] Paras 160-164.
[34] Ibid., Para 19 and section 2.3.
[35] Ibid., paras 30 and 31.
[36] https://cerre.eu/publications/dma-implementation-forum/.
[37] GDPR, Article 24, which reads "… the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

### 2.2.2 Nudging compliance design

An interesting feature of the draft guidelines are instances where the document provides indications about **how a gatekeeper demonstrates compliance. These are framed as desirable types of conduct** (what a gatekeeper 'should' do). Here are some examples:

- Art 6(4) DMA allows gatekeepers to take steps to protect the integrity of hardware or operating systems as well as the security of end users. The draft guidelines advise that gatekeepers should keep a list of the measures put in place and for each explain the applicable provisions of EU Law as well as the rationale justifying why there are no other effective means to comply with these legal requirements;[38]
- With data portability under Art 6(9) DMA, the guidelines provide that gatekeepers should keep an internal list of all categories of data that can be ported;[39]
- Similarly, with art 6(10) gatekeepers are encouraged to keep a record of all categories of data that are provided or generated by business users and end users.[40]

However, the draft guidelines may impose **obligations that appear too demanding and without a particularly clear legal basis**.

- The suggestion that gatekeepers implement periodic reminders to end users about their personal data portability choices;[41]
- The suggestion that the gatekeeper make available tools to enable third parties to establish contact with individuals other than the end-user to help the personal data recipient comply with the GDPR;[42]
- The suggestion that gatekeepers should ensure appropriate visibility and accessibility of personal data portability solutions with dedicated interfaces.[43] One can see the rationale for this: presently all gatekeepers provide an option to port personal data, but this is not flagged clearly on the platforms, which may explain the relatively low take-up. On the other hand, we consider that other actors may be better positioned to inform users of the value of porting their data and making them aware of how they can do so or even providing services by which data can be ported easily.

These recommendations are significant contributions to the more general requirements of compliance in the DMA. They are based on Article 8 DMA which requires that gatekeepers demonstrate compliance and provide suggestions about how this may be achieved. It is worth recalling that Article 24 GDPR also requires that the controller 'shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.' In other words, **both Regulations require the design of compliant systems, with the DMA uniquely affording the opportunity for the Commission to receive reports**

[38] Para 90.
[39] Para 111.
[40] Para 154.
[41] Para 123 and likewise for art 6(10) see para 164.
[42] Paras 114 and 116.
[43] Para 124.

**on compliance**. These measures in the guidelines help regulated parties understand the expectations of the Commission and EDPB.

On the other hand, these are framed as suggestions (what a gatekeeper should do, not what it shall do) and it is not clear if they provide a safe harbour (i.e. if the gatekeeper follows, then there is a presumption of compliance, and if these measures are about securing compliance with the GDPR, the DMA, or both) nor if the refusal to follow these suggestions creates a risk of non-compliance. **The advantage of a more prescriptive approach, which should not go further than the obligations foreseen in the DMA and the GDPR, is that it provides greater certainty**, for example by suggesting that taking certain measures creates a safe harbour for compliance. It is also important that these recommendations have a **clear legal basis and that they are tested for proportionality**. There is nothing to stop the Commission from indicating measures that would be desirable, but if these are likely to be disproportionate then they can be flagged as optional steps without an obligation to apply them. Gatekeepers may have incentives to deploy these measures anyway if this can generate consumer demand.

## 2.3 The Digital Omnibus Package and the GDPR

As already indicated, in November 2025 the Commission presented a series of measures to amend some of the EU's digital laws to simplify the framework and improve competitiveness.[44] The proposals do not suggest amendments to the DMA, but some of the proposals to revise the GDPR have follow-on effects on the DMA, and we focus on this point here.

First, the **definition of personal data** is amended so that data is personal only if the controller can identify the individual "taking into account the means reasonably likely to be used by that entity."[45] This might facilitate the application of Article 6(11) DMA because it rests on a subjective interpretation of whether data is personal for the data controller.

Second, Article 9, which relates to **sensitive data** is amended so that an additional legal basis for processing this data is added: 'processing in the context of the development and operation of an AI system … or an AI model.' This may become relevant as the DMA might extend to regulate services that use AI technology.

[44] SWD(2025) 836 final. Article 3, amending Article 4 of the GDPR

[45] See here the Court's approach in Case C-413/23 P, EDPS v SRB, EU:C:2025:645, paras 68-89. Cf. EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) (10 February 2026), paras 16 and 17. Their criticism that the amendment goes beyond the judgment is unfair since the EU legislative body is entitled to modify secondary law. Moreover, it is arguable that the Commission proposal is in fact aligned with the judgment and merely clarifies a complex judgment, see especially the Courts insistence on limits to the notion of personal data at para 88.

# 3. Enforcement challenges

## 3.1. Public enforcement

### *3.1.1 Dialogue between regulators*

The risk of multiple investigations into similar facts by different regulators has been discussed extensively. As we had suggested earlier, the ECJ case law has created a clear pathway to avoid the risk of decisions being quashed for failing to comply with the principle of ne bis in idem. A crucial component of this is **dialogue between all the national and the EU regulators (in charge of the protection of competition, the consumers, the privacy or the cybersecurity) involved in supervising the gatekeepers**, which is essential to avoid a finding that the rights of the gatekeeper have not been infringed.[46] Such dialogue seems to occur and the Commission is satisfied by the processes that are emerging, in particular with the competition authorities.[47]

Indeed, dialogue is particularly prominent with the Bundeskartellamt (BKA), given its **special competition powers** found in Section 19a GWB. The parallel application of such rule is foreseen in the DMA.[48] The German Federal Ministry for Economic Affairs and Energy has issued a report on the application of Section 19a and has noted that there has been close cooperation that in one case allowed the firm in question (Google) to "take a uniform approach to implementing the DMA obligations and the commitments made to the BKA."[49] The case in question extended Article 5(2) DMA obligations to other Google services not covered by the DMA.

Insofar as the BKA intervenes in markets not covered by the DMA (e.g., automobile infotainment systems) the law complements the DMA. However, it is possibly more problematic when the intervention addresses conduct by gatekeepers which extends the DMA obligations. For example, when Meta (whose Facebook service is a designated CPS) was forbidden under Section 19a to tie its VR glasses with Facebook, this is not conduct prohibited by Articles 5(7) or 5(8) of the DMA.[50] Indeed, some gatekeepers responses to the Commission DMA consultation point to the risk of fragmentation if NCAs apply their own rules on top of the DMA.[51] Fragmentation causes two kinds of negative effects: first, it makes compliance more costly because services have to be adapted for each Member State, insofar as the gatekeeper opts to only comply in one jurisdiction (e.g., in the VR Glasses case it appears Meta only offers a non-tied VR glass service in Germany).[52] And this has a second cost in that not all

[46] In this respect the joint guidelines para 216 are a bit oddly drafted as they seem to suggest that consultation is optional.
[47] Commission Second Annual DMA Report COM(2025) 166 final, paras 65-67.
[48] DMA, Recital 11 and Article 1(6).
[49] Bundesministerium fur Wirtschaft und Energie, Report pursuant to Section 19a (4) of the Act Against Restraints of Competition, page 6. https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/E/20260107-evaluation-19a-gwb.pdf?__blob=publicationFile&v=6 Machine translation was used to read the text.
[50] J-U Franck, 'Abuse Proceedings Against Digital Gatekeepers under Section 19a of the German Competition Act: Taking Stock of Early Results (May 2024).
[51] European Commission, DMA Review - Summary of the contributions to the targeted consultation, call for evidence and AI consultation (2025), p.6.
[52] BKA, 'Meta (Facebook) responds to concerns of the Federal Cartel Office – VR glasses can also be used without a Facebook account in the future' 22 November 2022.

EU consumers gain from enforcement. On the other hand, when national authorities identify market failures that are not addressed by EU Law, this can stimulate better EU-level regulation.

Here, a **trade-off is made between an administrable legal system (one common set of rules) and a system with the potential to address missing market failures and allows regulatory experimentation (national differentiation)**. It is not clear to us that this trade-off has ever been discussed and it may be suboptimal to afford NCAs the option to always apply stricter measures. In this context, recall the Draghi Report's criticism of the gold-plating practices by Member States as one key factor harming competitiveness.[53] While he refers to the harm this causes to SMEs, there is follow-on harm also when large firms are subjected to different regulations. As the Facebook case shows, for example, an EU-wide remedy untying Facebook and VR equipment would be more likely to attract investment in VR devices that can interoperate with the services offered by tech giants.

Another example of this coordination may be found in the commitment decision issued by the Italian AGCM when applying **consumer law** to Google's consent model for the combined use of data (discussed also in 2.1 above). In this instance, the application of national law appears to overlap with the DMA. The AGCM coordinated enforcement with the Commission officials responsible for enforcing Article 5(2) DMA and also consulted with other national authorities (the regulator for electronic communications (AGCOM) and the data protection authority).[54] It transpires from the documents that are publicly available that the Commission and Google also engaged in bilateral dialogue pertinent to resolving the issue in front of the Italian AGCM.[55] In its commitment decision, Google's actions are designed to comply both with consumer law and with the DMA. In this sense, while the Italian NCA is not directly competent to apply the DMA, it makes sense for the gatekeeper to achieve compliance with the DMA in parallel to avoid further proceedings. Unfortunately, it is not clear from the commitment decision whether the gatekeeper committed to this conduct for the EU as a whole, although it would appear that this is the case because one specific commitment (emailing end-users) was made specifically with respect to consumers based in Italy, suggesting the reminder of the commitments may be EU-wide.

There are two takeaways from these national decisions, which echo recommendations some of us have made already[56]. The best option in these settings **where a gatekeeper does not comply with EU Law (whether the DMA or other EU rules) would be for the Commission to apply the DMA and in the long term to consider the development of well-resourced EU-level digital enforcement agency**. This is particularly key in digital markets when the conduct of the firm is usually the same across jurisdictions. This ensures that a single approach is followed (ensuring legal certainty) and that the concerns are addressed across the whole EU market (ensuring effectiveness).

A good example in this context is the AGCM's investigation in Meta AI, where this conduct is now also considered by the Commission for all EU markets bar Italy.[57] The conduct under consideration is: (1)

[53] The future of European competitiveness, Part A: A competitiveness strategy for Europe (2024) p.30.
[54] Case PS12714, Alphabet Inc and Google Ireland Ltd, Decision of 4 November 2025, Paras 11-13 https://agcm.it/dotcmsdoc/allegati-news/PS12714_acc.%20impegni%20+%20chius..pdf a press release in English is available at: https://en.agcm.it/en/media/press-releases/2025/11/PS12714.
[55] See https://www.agcm.it/dotcmsdoc/allegati-news/PS12714_testo%20impegni.pdf page 3.
[56] See Monti and de Streel, 'Improving EU Institutional Design to Better Supervise Digital Platforms' CERRE 2022.
[57] Commission opens antitrust investigation into Meta's new policy regarding AI providers' access to WhatsApp (4 December 2025).

Meta integrating its Meta AI service with WhatsApp and (2) Meta doing the same in its WhatsApp Business Solutions, which is a service Meta offers to businesses for communicating with their customers. Here too, only Meta AI would be available as a chatbot or AI assistant. Interim measures were adopted by AGCM regarding the second practice because of the risk of lock-in: users will develop familiarity with Meta's chatbot and will be unlikely to switch to alternative services later in time.[58] Moreover, the use of Meta's chatbot will allow Meta to improve its services based on user queries, an option which would be denied to rivals who would then may enter with a less useful product for consumers.[59] These risks make interim measures necessary because, the AGCM reasoned, otherwise the market will no longer be contestable.[60] The Commission is now also considering the imposition of interim measures.[61] Two points are worth noting from these proceedings: first duplication is inefficient, and the Commission could take the initiative when there is a real problem at the EU level. Second, the agencies will necessarily have to coordinate a remedy, imposing added coordination costs that could easily be avoided. A further issue, which is beyond the scope of this paper, is the extent to which the conduct in question is also contrary to the DMA and not only EU competition law.[62]

The second is that even if our first recommendation cannot be implemented in the short term, the **kind of coordination we see in these cases can allow for a reasonably resolution which does not jeopardise legal certainty and allows gatekeepers to comply in a manner consistent with all obligations**. One overarching idea that regulators should have in mind when coordinating enforcement is to ensure that this is as coherent as possible for the regulated firm. For example, if the firm has already complied with a DMA obligation in one manner and the national authority is extending the reach of that obligation to a new service, then the firm could simply extend its DMA compliance rather than being asked to devise another solution. The regulated firm should take an active role in this process of shaping and coordinating compliance. For example, if a data collection protocol that complies with art 5(2) is already in place and a national authority uses competition law or the GDPR to request additional limitations on the use of data in setting outside the DMA, then the firm should be able to replicate the protocols designed under the DMA.

### *3.1.2 Networks*

Related to this, the case-law also requires institutional coordination when considering overlapping rules in order to avoid infringing the ne bis in idem principle. In this context, a proposal for a **Digital Clearing House 2.0** has been made by the European Data Protection Supervisor (EDPS) to enhance regulatory consistency and cooperation and facilitate the exchange of information.[63] On the one hand, this is desirable and there is evidence that cooperation among regulators is perceived to be useful in achieving these two objectives.

However, there may be **a risk of creating too many networks and duplicating resources**. For example, there are networks of national regulators in some Member States already and the DMA has its own High-Level Group which brings together expertise from a range of EU laws. The European Competition

[58] Case A576, Meta AI Chatbot (25 November 2025) Para 8 (https://www.agcm.it/dotcmsdoc/allegati-news/A576_provv.%20ampliam.%20istrutt.%20+%20avvio%20cautelare.pdf).
[59] Meta AI Chatbot, para 9.
[60] Meta AI Chatbot, para 12.
[61] https://ec.europa.eu/commission/presscorner/detail/en/ip_26_310
[62] F. Bostoen and J. Kramer, "Is the DMA Ready for Agentic AI?" (CERRE 2025).
[63] https://www.edps.europa.eu/data-protection/our-work/subjects/digital-clearinghouse-20_en.

Network seems to be used to coordinate DMA related activity as well. Given that regulators are under-resourced, spreading individuals across too many networks may have an adverse effect on enforcement.

Such an initiative also requires a more fundamental reflection about how many EU and national agencies are needed to manage the digital rulebook. Rationalising this by reducing the number of agencies can also foster better internal dialogue about how to apply the rules. As suggested above, **centralised enforcement at EU level** can serve as a more effective way of integrating rules.[64] For example, if a single EU Digital Enforcement agency were in charge of DMA, competition and consumer law, one would have a series of internal processes to manage the links among these various laws.

Finally, it is inevitable that the EDPS would issue a recommendation which sees the GDPR, and the rights protected thereunder as the central point around which all other digital laws orbit. It is not clear that this is the most helpful premise for establishing a network of regulators. Conceptually, it is not clear that privacy and data protection rights should dominate other rights and interests. Rather, this project would be more effective if it were designed around two pillars: **(i) that trade-offs among various desirable policy objectives exist and must be addressed; (ii) that good regulation requires a learning environment by which the effects and side-effects of regulation should be considered**. This means that the network would be well-placed to assess the extent to which regulation works and how to improve it. Such a pragmatic approach is preferable than staking out a principle about the normative superiority of data subject rights only to then undermine these rights given the exigencies of business models and the need to grow EU industry. Ultimately, regulatory consistency across legal instruments and across countries should reduce compliance costs and increase regulatory effectiveness.

## 3.2. Private enforcement

There has not yet been a large volume of private enforcement where the DMA is invoked. **Private enforcement may accelerate DMA enforcement** - especially because the Commission has limited capacity - and legal predictability in the long term as case-law and references to the ECJ can clarify the scope of the DMA.

At this stage we want to flag two issues that may require clarification and discussion. The first issue is how national courts should implement the duty of loyal coordination found in the *Masterfoods* judgment for antitrust cases and found in Article 39(5) of the DMA.[65] The key point is that a **national court should not issue decisions that contravene Commission decisions and stay proceedings pending a Commission decision**. Since a lot of compliance occurs via regulatory dialogue and sometimes solutions may occur even without the opening of proceedings, implementing this obligation can prove tricky. Courts should be able to secure information from the Commission about the state of play of any regulatory dialogue. Gatekeepers have a clear incentive to signal such dialogue to a national court.

[64] G. Monti and A. de Streel, Improving institutional design to better supervise digital platforms, CERRE Report, January 2022: Improving EU Institutional Design to Better Supervise Digital Platforms - CERRE.
[65] The judgment has been codified in Regulation 1/2003, Article 16.

The second issue pertains to injunctive relief. When claimants use the DMA to seek damages for non-compliance, there may be risks of a national court interpreting the DMA in a way that departs from the way the Commission would interpret the DMA. In this context, the usual pathway to clarify the law is using the preliminary ruling procedure. This is built into the way EU Law works and restated in Article 39(5) of the DMA. A slightly different issue may arise when it comes to **requests for injunctive relief, where a national court may be asked to impose a specific remedy on a gatekeeper, which could be compared to a Commission specification decision**.

In a recent judgment under the GDPR, the claimant had asked the national court to request an injunction 'prohibiting the controller from committing a further infringement of those rights.'[66] The ECJ found that there was no such right to an injunction on the basis of the GDPR. The question this gives rise to is whether under the DMA there is an EU-law right to such an injunction. On the one hand, the answer could be in the affirmative because the aim of the DMA is prospective: to open markets and to ensure that P2B relations are fair in the future. On the other hand, this entails two risks. The first is that the injunction imposes conduct which is too far-reaching in light of the DMA, and the second is that the gatekeeper is deprived of the option to decide how it wishes to comply with the DMA. Recall that when the Commission issues a non-compliance decision, it cannot stipulate how the gatekeeper shall comply[67]. Behavioural remedies may only be imposed when there has been systematic non-compliance[68]. Consequently, **given that public enforcement of the DMA sees behavioural remedies as a last resort, there could be no EU law right to a forward-looking injunction on the basis of the DMA and when national courts have such powers, they should be exercised sparingly** given that it is for gatekeepers to design compliance.

Having said that, **there may well be instances where there is only one route to compliance, and an injunction can prove effective**. A recent judgment in Germany for example compelled Google to allow end-users to use any email account they wish to sign up to set up an Android smartphone, basing its decision on Article 5(8) DMA. In this case, the gatekeeper has little option about how to design compliance.[69] An injunction on these facts is a proportionate remedy. However, there may be instances where affording gatekeepers the option to design compliance is preferable and an injunction may be framed in this manner rather than mandating specific conduct.

[66] Case C-655/23, para 42, *IP v Quirin Privatbank AG*, EU:C:2025:655,
[67] Article 29(6) DMA.
[68] Article 18(1) DMA.
[69] https://dejure.org/dienste/vernetzung/rechtsprechung?Text=12%20HK%20O%2032/24 at the time of writing the judgment has not yet been published. A short summary is at: https://lawschoolgermany.de/blogs/zivilrecht/jura-online-nachhilfe.

# About CERRE

Providing high quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) is a not-for-profit think tank. It promotes robust and consistent regulation in Europe's network, digital industry, and service sectors. CERRE's members are regulatory authorities and companies operating in these sectors, as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach covering a variety of markets, e.g.,, energy, mobility, sustainability, tech, media, telecom, etc.;
- the widely acknowledged academic credentials and policy experience of its research team and associated staff members;
- its scientific independence and impartiality; and,
- the direct relevance and timeliness of its contributions to the policy and regulatory development process impacting network industry players and the markets for their goods and services.

CERRE's activities include contributions to the development of norms, standards, and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims to clarify the respective roles of market operators, governments, and regulatory authorities, as well as contribute to the enhancement of those organisations' expertise in addressing regulatory issues of relevance to their activities.

# About the Authors

Alexandre de Streel is the Academic Director of the digital research programme at CERRE, professor of European law at the University of Namur and visiting professor at the College of Europe (Bruges) and SciencesPo Paris. He sits in the scientific committees of the Knight-Georgetown Institute (US), the European University Institute-Centre for a Digital Society (Italy) and Mannheim Centre for Competition and Innovation (Germany). His main research areas are regulation and competition policy in the digital economy (telecommunications, platforms and data) as well as the legal issues raised by the developments of artificial intelligence. He regularly advises the European Union and international organisations on digital regulation.

Giorgio Monti is a CERRE Research Fellow and Professor of Competition Law at Tilburg Law School. He began his career in the UK (Leicester 1993-2001 and London School of Economics (2001-2010) before taking up the Chair in competition law at the European University Institute in Florence, Italy (2010-2019). While at the EUI he helped establish the Florence Competition Program which carries out research and training for judges and executives. He also served as Head of the Law Department at the EUI. His principal field of research is competition law.

cerre

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

Centre on Regulation in Europe (CERRE)
CERRE Think Tank
CERRE Think Tank