



# RECOMMENDATIONS FOR THE EFFECTIVE AND PROPORTIONATE DMA IMPLEMENTATION

RECOMMENDATIONS PAPER

*December 2022*

Co-ordinated by Alexandre de  
Stree



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.

This paper is part of a larger CERRE project entitled ‘Effective and Proportionate Implementation of the DMA’ which is a collection of nine papers focusing on the trade-offs around the different possible interpretations of the regulation. The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Apple, Arcep, Booking.com, ComReg, DuckDuckGo, Google, Mediaset, Meta, Microsoft, Qualcomm, Spotify, TikTok, Vodafone, Ofcom, and ARCOM. 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.

© Copyright 2022, Centre on Regulation in Europe (CERRE)

[info@cerre.eu](mailto:info@cerre.eu) – [www.cerre.eu](http://www.cerre.eu)



## TABLE OF CONTENTS

ABOUT CERRE.....	3
ABOUT THE AUTHORS.....	4
INTRODUCTION.....	5
1. RECOMMENDATIONS ON GATEKEEPER DESIGNATION .....	5
2. RECOMMENDATIONS TO INTERPRET AND IMPLEMENT THE DMA OBLIGATIONS .....	6
2.1. General recommendations .....	6
2.2. Increasing online advertising transparency: DMA Article 5(9) and (10) and 6(8) .....	9
2.3. Switching Tools and Choice Screens: DMA Article 6(3) and 6(4) .....	11
2.4. Prohibition of self-preferencing: DMA Article 6(5).....	14
2.5. Vertical and horizontal interoperability: DMA Articles 6(4), 6(7) and 7 .....	15
2.6. Data portability for end users and business users: DMA Articles 6(9) and 6(10).....	16
2.7. Data access for search engines: DMA Article 6(11) .....	17
3. RECOMMENDATIONS FOR EFFECTIVE PROCESS AND INSTITUTIONAL DESIGN.....	18



## ABOUT CERRE

Providing top-quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards, and policy recommendations related to the regulation of service providers, the specification of market rules, and improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments, and regulatory authorities, as well as at strengthening the expertise of the latter, since, in many Member States, regulators are part of a relatively recent profession.



## ABOUT THE AUTHOR



**Alexandre de Streele** is a CERRE Academic Director and a Professor of European Law at the University of Namur and the President of the Namur Digital Institute (NADI). Since April 2021, he is also the Chair of the EU Observatory on Online Platform Economy.

He is visiting professor at the College of Europe and SciencesPo Paris, and an assessor at the Belgian Competition Authority.

His main areas of research are regulation and competition policy in the digital economy as well as the legal issues raised by the developments of artificial intelligence. Recently, he advised the European Commission and the European Parliament on the regulation of online platforms.

Previously, Alexandre worked for the Belgian Deputy Prime Minister, the Belgian Permanent Representation to the European Union, and the European Commission



## INTRODUCTION

The Digital Markets Act (DMA)<sup>1</sup> entered into force on 1 November 2022 and its rules will apply from 2 May 2023. The Commission should designate, for the first time, the gatekeepers subjected to the rules by September 2023 at the latest, and those platforms should comply with prohibitions and obligations in March 2024.

Building on a series of eight issue papers as well as previous work done by CERRE on the DMA,<sup>2</sup> this paper provides points of attention and recommendations to implement the DMA. Section 1 focuses on gatekeeper designation, section 2 focuses on the obligations, and section 3 deals with the process and the institutional design.

## 1. RECOMMENDATIONS ON GATEKEEPER DESIGNATION

The Commission should designate a gatekeeper on the basis of a three-criteria test: (i) significant impact on the EU internal market; (ii) the control of an important gateway for business users to reach end-users; and (iii) an entrenched and durable position.<sup>3</sup> To facilitate such designation, there is a rebuttable presumption that the three criteria are fulfilled when some quantitative thresholds (in terms of financial and user size) are met. However, on the one hand, a firm above the thresholds may try to rebut the presumption and show it is not a gatekeeper, and, on the other, the Commission may designate a firm below the thresholds when it meets the three-criteria test. As the issue paper on gatekeeper designation explains, three legal issues would benefit from being clarified.

First, we recommend that **every decision to regulate a Core Platform Service (CPS) will require a designation that the undertaking in question is a gatekeeper in relation to the provision of that specific service** and that, accordingly, references to ‘active users’ for the purposes of gatekeeper designations are referenced only to users of this CPS in question.

Second, we recommend that the **evidential standards used** in market investigations considering whether **to exclude a firm that otherwise meets the quantitative thresholds for gatekeeper designation should be the same as those used** in market investigations considering whether **to include a firm that otherwise does not meet the same quantitative thresholds**,<sup>4</sup> subject to the practical constraints that arise from differences in the timescales available to the Commission to complete its investigations.

Third, the **application of Annex A of the DMA**, with the possibility that services provided by the same firm within the same CPS category may be assessed separately for gatekeeper designation if they are used for ‘different purposes’, **will need to be clarified through specific cases** and firms should not be able to abuse this provision in order to evade designation. Conversely, the Commission should ensure

---

<sup>1</sup> Regulation 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 2019/1937 and 2020/1828 (Digital Markets Act), OJ [2022] L 265/1.

<sup>2</sup> <https://cerre.eu/publications/european-parliament-digital-markets-act-dma-resilient-effective/>  
<https://cerre.eu/publications/digital-markets-act-economic-regulation-platforms-digital-age/>

<sup>3</sup> DMA, Art.3.

<sup>4</sup> Resp. DMA, Art.3(5) and 3(8).



that services are not unnecessarily included in the list of designated CPSs where firms are not gatekeepers in relation to the provision of those services.

## 2. RECOMMENDATIONS TO INTERPRET AND IMPLEMENT THE DMA OBLIGATIONS

The EU lawmaker decided to base the DMA on detailed rules instead of broad standards to facilitate its implementation and increase legal certainty.<sup>5</sup> However, **several obligations and prohibitions are not self-executing** because, on the one hand, they apply to technologies and business models which are diverse, fast-evolving, complex, and not always fully understood and, on the other hand, several trade-offs between conflicting values and interests, such as between openness and privacy or service integrity, have been left open by the lawmaker. This section raises some points of attention and provides recommendations in order to make the implementation of those obligations effective and proportionate.

### 2.1. General recommendations

#### (a) Clarify the interpretation of the obligations

The legal interpretation of several obligations, in Articles 5, 6, and 7, would need to be clarified by the Commission and the Courts. Given the importance of legal certainty for gatekeepers and their business users alike, those clarifications will be crucial, especially for the obligations that need product re-design, which may take time. Those clarifications are of three types.

The first type relates to the **material and geographical scope of application of some obligations**. Regarding the material scope, as indicated below, clarifications may be needed on the definition of publisher that benefits from the online ad transparency regime (art.5.9, 5.10, and 6.8), on multiple issues regarding the switching and default obligations (art.6.3) and 6.4), on the applicability of self-preferencing prohibition (art.6.5), on the intended scope and depth of access of the vertical interoperability obligation (art.6.7), on which data and context that need to be ported (art.6.9 and 6.10) or on the beneficiaries of search data access (art.6.11). Regarding the geographical scope, as indicated below, clarifications may be needed on search data sharing or horizontal interoperability (art.7). Those clarifications should build – and be consistent with – the EU digital acquis such as the GDPR,<sup>6</sup> cybersecurity legislation<sup>7</sup>, IP, and trade secret laws.<sup>8</sup>

The second type of legal clarifications relate to the **precise meaning of some obligations**. As indicated below, clarifications may be needed on the online ad metrics that need to be made more transparent

---

<sup>5</sup> Impact Assessment Report of the Commission Services on the DMA, SWD(2020) 363, para.153.

<sup>6</sup> Regulation 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 (General Data Protection Regulation), OJ [2016] L 119/1.

<sup>7</sup> Such as Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ [2016] L 194/1

<sup>8</sup> Such as Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9 and 2001/29, OJ [2019] L 130/92 or Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ [2016] L 157/1



(art.5.9, 5.10, and 6.8), on how many alternatives need to be included in the default setting or how many access points to switch a default should be offered by the gatekeeper (art.6.3 and 6.4), on which self-preferencing practice is prohibited given its context (art.6.5) or which consent should be required when data are ported (art.6.9 and 6.10).

The third type of clarification, which may be the most fundamental, relates to **how compliance with the obligation is to be assessed and demonstrated**. As explained in the issue paper on the DMA compass, this may include the agreement between the Commission, the gatekeepers, and the main other stakeholders on a **set of quantitative measurements** on the impact of each obligation on relations between the gatekeeper and other relevant parties. Those indicators should be designed with transparent, fair, and open industry-wide discussions. They would introduce a degree of objectivity and shared factual understanding even if the interpretation of the measurements and the conclusions to be drawn from them will remain a matter of contention and be under the control of the Commission. However, those quantitative measures would be one signal among others that need to be considered alongside qualitative representations from the gatekeepers and their business users.

**To provide those legal clarifications ‘to the market’, the Commission has several means with different timings.** Before March 2024, the Commission may discuss them informally and on a case-by-case basis with the gatekeepers and their business users. After 2024, the Commission may give those clarifications more formally and individually to each gatekeeper when it reacts to their compliance reports, when it engages in formal regulatory dialogue, and/or when it opens non-compliance proceedings.<sup>9</sup> Ultimately, of course, the final clarification and legal interpretation will be given by the Court of Justice of the EU. As soon as there is a relevant body of experience, the Commission could then ‘codify’ those legal clarifications and interpretations in general guidelines.<sup>10</sup>

#### **(b) Establish robust mechanisms for implementation**

To comply with the DMA, **gatekeepers will have to adapt their products and services**. Those adaptations should ensure that the goal of each obligation and the DMA as a whole are met, while respecting the principle of proportionality.

In many cases, it is optimal that **those mechanisms are process-based and will be determined by the regulated gatekeepers** who know their products the best. However, to alleviate the risk that the gatekeepers undermine the effectiveness of the DMA, the establishment of those mechanisms should be done **in partnership with the business users who may want to rely on the mechanisms to offer their services, and under the supervision of the Commission**. In reviewing gatekeeper submissions, the Commission could seek input from third parties (including those representing consumers), draw on the extensive evidence collected by gatekeepers through A/B testing, and potentially require its own testing. The Commission could usefully also set out how it expects gatekeepers to engage with third parties too.

---

<sup>9</sup> Resp. art.11, 8 and 29 DMA.

<sup>10</sup> DMA, Art.47.



In some cases, the redesign of the product and/or the establishment of new mechanisms will entail significant engineering changes which can take time. This is why the **Commission should be able to ‘stop the clock’** of the very tight deadlines of the DMA when an obligation needs to be clarified to be implemented and when the gatekeeper cooperates in good faith with the Commission and their business users.

### (c) Effectiveness and proportionality

Those interpretation and implementation questions should be solved by applying the two main overarching regulatory principles of the DMA, effectiveness and proportionality.

First, the measures taken by the gatekeepers should be **effective** in two ways:<sup>11</sup> achieving the overall objectives of the DMA as a whole (general effectiveness) and achieving the objectives of each obligation (specific effectiveness).

- **General effectiveness** refers to the two DMA overarching objectives of “contestability” and “fairness”. Contestability mostly relates to reducing strategic and some structural entry barriers while fairness is an issue where the imbalance between gatekeeper and business user deprives the latter of adequate reward for its efforts. In the end, both objectives may be understood with reference to **(long-term) competition in digital markets** among the gatekeepers and between the gatekeepers and entrants. Thus, competition plays a central role at all times, but in a way that the DMA helps to channel or structure it or, in other words, that regulation aims to support and complement market forces to maximise end-user welfare instead of substituting them. Moreover, both objectives are linked and ultimately aim to promote business and end-user choice as well as the degree and the diversity of innovation in the digital economy.
- **Specific effectiveness** relates to the objectives of each obligation which can be measured, as suggested above, with quantitative metrics on the impact of obligations on relations between the gatekeeper and other relevant parties.

Second, the measures taken by the gatekeepers should also be **proportionate**.<sup>12</sup> The application of this principle has several consequences:

- It determines **whether a DMA measure is necessary**, in the sense that the same result might not be possible to achieve through a less intrusive measure. Thus, proportionality limits what the Commission may impose on the gatekeepers to comply with the DMA and how far the gatekeepers should adapt their products and services. Also, the proportionality principle channels the economic analysis that normally underpins an efficiency defence in antitrust (but

---

<sup>11</sup> DMA, Art.8(1).

<sup>12</sup> DMA, Art.8(7).



is not present in the DMA) into a narrower framework and it compels the defendant firm to work within the specific set of core goals of the DMA.

- It also helps the Commission and the Courts to find the right **balance between the different trade-offs** left open within the DMA between conflicting values and interests, such as between openness on the one hand, and privacy, service integrity, IP or user safety, on the other.
- In the same vein, it contributes to **avoiding or mitigating the risks of unintended consequences** of the DMA implementation, in particular, the reduction of innovation and consumer choice which are the ultimate objectives of the DMA. More specific examples mentioned below relate to the risk of collusion by increased transparency in online ads, the risk of unclear and misleading third-party prompts and ‘slamming’ when app stores become more open, or the risk of strengthening the position of the gatekeepers to the detriment of smaller players.
- It also contributes to ensuring **consistency across the different legislations composing the quickly expanding EU digital platforms acquis** and to solving the tension between different laws having different objectives, such as the DMA and the GDPR or the cyber security legislations.

The principle of proportionality will also determine how far **objective justification based on service integrity, security, or privacy**, as allowed in the DMA, can be relied upon by the gatekeepers.<sup>13</sup>

## 2.2. Increasing online advertising transparency: DMA Article 5(9) and (10) and 6(8)

### (a) Legal clarifications needed

The implementation of the provisions about advertising transparency will need to establish the **definition of ‘publisher’**, as it is not defined in the DMA. A useful approach would be to draw on the understanding of ‘publisher’ elaborated in recitals 54-60 in the **Copyright in Digital Single Market Directive**.<sup>14</sup> The term publisher would then refer to firms that invest in the production or acquisition of content and associated rights and have editorial responsibility. A wider definition of publisher that includes others that sell advertising inventory, including social media possibly owned by gatekeepers, for example, could significantly complicate the implementation of these provisions.

The **term ‘metric’** is also not defined in the DMA, which is understandable as ‘metric’ may be defined in numerous different ways, and there is potential for innovation in this area. However, it may still be advisable to **set some parameters** to demonstrate what providing “information on a daily basis on (...) the metrics on which each of the prices, fees, and remunerations are calculated”<sup>15</sup> means. The

<sup>13</sup> DMA, Art.6(3), 6(4), 6(7), 7(3) and 7(6).

<sup>14</sup> This Directive also fails to exactly define ‘publisher’ among its definitions; however Recitals 54-60 give an indication of what they are understood to be: Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9 and 2001/29, OJ [2019] L 130/92.

<sup>15</sup> DMA, Art.5(9)



information should be broad enough to allow the receivers to gain a **thorough understanding of how the prices** have been established and be specific to individual ads without the involvement of personal data. These should allow for comparison across advertisers and across CPSs where multiple services are offered by the same gatekeeper.

Through greater transparency, the DMA should facilitate fair and open industry-wide discussions on assessing advertising effectiveness and appropriate performance indicators. Striking the right balance between providing actors in the ecosystem with the information necessary to ensure contestability and fairness, and safeguarding the users of advertisement-supported services will likely **require extensive discussions about what measures of effectiveness are appropriate and what metrics should be used at all.**

#### **(b) Effective mechanisms to implement the obligations**

Daily provision of information in most cases should be done **through an API** for it to be useful. There will likely need to be an **experimental phase** during which gatekeepers, advertisers, and publishers try various solutions. Given the history of tensions and power imbalances among these three groups of stakeholders, the Commission may need to undertake a listening exercise afterwards with the intention of setting parameters or issuing guidance.

Giving access to performance measurement tools rather than data can give equitable access to the insight from personal data, where it is used in performance measurement, without further dissemination of user data. **Tools can be made available in a way that benefits smaller publishers and advertisers in the same way as larger ones.** However, there is also a risk that widespread access to gatekeeper performance measurement tools will further solidify the position of certain definitions of performance and data-intensive practices. There is a need for engagement with these tools by advertisers and publishers to spark an industry-wide discussion about methods and approaches to measure performance, independence, and auditability.

As discussed in the issue paper on online advertising transparency, the incentives to consent to share pricing information are not the same for advertisers and publishers. Third-party agents acting on behalf of advertisers will often have separate interests and incentives quite different from the advertiser that has engaged them. Given the level of concentration on the key function of ad-buying and the role that they play combined with the fact that only a few Member States have laws that ensure transparency between them and advertisers, their position in the consent chain merits close attention. **The implementation of these provisions by gatekeepers should be done in a manner that facilitates or even encourages consent from advertisers, publishers, and their agents.** If this does not happen in the short term once the DMA has gone into effect, the Commission might need to develop guidance on the means of getting consent from these businesses.



### (c) Avoiding unintended consequences

Sharing pricing information can come with a **risk of collusion**. Trade in advertising that goes through digital gatekeepers is often highly automated and automated systems using machine learning may tend towards collusion, even without communication or instruction, both in pricing strategies and in bidding strategies. Such tendencies might not necessarily trigger antitrust responses, but a balance must be made, and **careful monitoring** will likely be necessary to ensure that fairness and contestability are maintained or established across the various functions in the advertising ecosystems where gatekeepers are involved.

Access to information on pricing and data for independent ad verification will be useful to publishers that have the capacity to process the data and adapt strategy based on the insight gained. This may lead to a **widening gap between larger publishers**, such as those with media holdings in multiple Member States or those with strong positions in large national markets, **and smaller publishers**, such as regional or local media. This **could raise competition and media plurality concerns**. Regulators responsible for media plurality in Member States will need to assess the consequences for smaller publishers once the DMA will have been in force for some time.

More fundamentally, the DMA must include **respect for the principles enshrined in the GDPR**, even in the often data-intensive trade in advertising. The provisions in Articles 5(9&10) and 6(8) should **not be implemented in a way to encourage the further spread of highly targeted and personal data-intensive types of advertising**.

## 2.3. Switching Tools and Choice Screens: DMA Article 6(3) and 6(4)

The following recommendations relate to issues of scope and probable effectiveness of the default switching elements of Articles 6(3) and 6(4). As these articles are multi-faceted, the focus is on three key clauses:

- Article 6(3.ii) relates to the second sentence of Article 6(3), which relates to the provision of switching tools to facilitate the ongoing ability of end users to change their default settings;
- Article 6(3.iii) relates to the third sentence of Article 6(3), which relates to the requirement of an upfront choice screen for end users to select their default settings;

Article 6(4.ii) relates to the second and third sentences of Article 6(4), which relates to the ability of third-party apps and app stores to prompt end users to switch default, and the ensuing ability of end users to do so.



## (a) Legal clarifications of the scope of application

### *Application of Article 6(3) to non-standard browsers*

It seems likely that **search apps and in-app browsers would be classified as browsers**, therefore Article 6(3) should apply to them on that basis. While this may have some benefits for contestability, it also risks being misleading where such browsers do not offer appropriate functionality to be used as default browsers. It may therefore be appropriate for **gatekeepers to place some minimum requirements on what functionality ‘browsers’ must offer in order to be chosen as a default**, but such requirements should be transparent and proportionate.

### *Application of Article 6(3.ii) to services other than browsers, virtual assistants, and search engines*

In our view, Article 6(3.ii) should be interpreted as covering all products or services for which there is a default setting on its operating system, virtual assistant, or web browser, and not just browsers, virtual assistants, and search engines. Mail, Calendar, Maps, and audio player services seem obvious examples.

At the same time, **‘within browser’ defaults should arguably be out of scope**. However, the line between what is effectively part of the browser and what is distinct may well be subject to debate. It would be useful to have clarification on these issues.

### *Application of Article 6(3.ii) to non-proprietary defaults*

While the wording within Article 6(3.ii) is not totally clear, Recital 49 suggests that Article 6(3.ii) is most likely to apply only to those default settings which relate to a gatekeeper’s own proprietary services and **not to defaults where services are provided under contract by a third party**. However, the legal position on this important issue is complex and requires clarification.

In addition, in the specific case of default settings for apps on operating systems, we note that there is also a potential link here with Article 6(4)(i). This requires that gatekeepers enable the ‘effective use’ of third-party apps and app stores with their operating system. One possible interpretation is requiring the easy switching of any relevant default settings within a designated Operating System (albeit this does not apply to default settings within browsers or voice assistants). This requirement is not limited to situations where the gatekeeper has its own rival services. Again, it would be helpful to have more clarity on how Article 6(3)(ii) relates to Article 6(4)(i).

### *Application of Article 6(4.ii) to pre-installed apps/app stores*

Article 6(4.ii) formally applies only to downloaded third-party apps and app stores. As such, it seems to **exclude any apps and app stores that have been pre-installed**, meaning that they would not have the right to prompt end users to switch their default setting to them. However, this seems somewhat at odds with Recital 50. It would be useful to have clarification on this issue.

### *The issue of multiple ‘access points’*

We consider that Articles 6(3) and 6(4) could reasonably be interpreted as requiring gatekeepers to enable end users to choose to **switch a default across all access points at once**, but also – for those



who are keen or for those search engines with more limited interoperability – to enable choices **also to be made separately** for each individual access point.

We consider that this conclusion is relevant to both the ongoing switching tools required in Article 6(3.ii), the initial choice screens for browsers, virtual assistants, and search engines required under Article 6(3.iii), and the ability to switch following a prompt under Article 6(4.ii). It would be useful to have clarification on this issue.

## **(b) Effective mechanisms to implement the obligations**

### *Design of the Article 6(3.ii) switching tools*

It seems reasonable to conclude that, in enabling end users to change their default settings under Article 6(3.ii):

(1) end users should be able easily to **switch to (at least) any alternative option that is currently installed on the user’s device;**

(2) the switching tools should **provide a full list** of the relevant currently installed options;

(3) the gatekeeper should **not be allowed to charge** providers a fee to be ranked higher on this list,

and (4) access to the switching tools should be easy. It would be useful for Commission to confirm whether it supports these conclusions.

### *The need to be able to reverse decisions*

The Commission could consider further the importance of enabling **default switching decisions also to be easily reversed.**

### *The use of behavioural techniques to inhibit switching or induce switching back*

It is likely that the **disproportionate or discriminatory use by gatekeepers of behavioural techniques** – such as prompts and warnings – to inhibit switching, or induce switching back, would be **non-compliant** with the DMA. It would be useful to clarify this.

### *Timing of initial choice screens*

The Article 6(3.iii) wording “end user’s first use” seems most likely to mean that **defaults must be chosen anew with every first use (or installation) on a new device.** However, it would be useful to have clarification on this point.

### *Payment for access to initial choice screens*

It may be reasonable to conclude that gatekeepers should **not charge for access or prominence** on the Article 6(3.iii) choice screens, but it would be useful to have clarification on this point. We note that the DMA is silent on the question of whether the gatekeeper can charge an ongoing fee, or revenue share, to providers who are successful in being chosen.



### *Choice architecture of the initial choice screen*

The Commission should set out its high-level expectations around the **choice architecture of the initial choice screens, and hold the gatekeepers to account in showing how they are meeting these expectations**. In reviewing their submissions, it should seek the input of third parties, draw on the extensive evidence collected by gatekeepers through A/B testing, and potentially require its own testing.

### **(c) Avoiding and mitigating unintended consequences**

#### *The risk of unclear and misleading third-party prompts and ‘slamming’*

In designing its user interface to address the risk of end-user harm arising from **misleading third-party prompts and ‘slamming’**, the gatekeepers face a delicate balance. The Commission should meet with gatekeepers and third parties to consider **solutions**. More generally, this is an area that should be kept under review.

#### *The risk of excessive prompts and choice fatigue*

Given the clear risk of **‘choice fatigue’** arising from excessive switching prompts by third parties, based on their rights under Article 6(4.ii), it would be useful for the Commission to meet with gatekeepers and third parties to seek **solutions**. More generally, this is an area that should be kept under review.

#### *The risk of harming services with limited market power*

Article 6(3.iii) could have the **unintended consequence of requiring the opening up of some default settings to competition where the current service provider is relatively small**, to the potential benefit of their larger rivals. It is not entirely clear how it can be avoided under the existing DMA framework, but the Commission should be alert to this possible outcome and keep the issue under review.

## **2.4. Prohibition of self-preferencing: DMA Article 6(5)**

### **(a) Legal clarifications needed**

It could be clarified whether Article 6(5) is widely applicable, in the sense that the prohibition of a more favourable treatment of a gatekeeper’s products or services compared to third-party offers **applies both on the end user and the business user side**. We recommend following such a broad interpretation for reasons of effectiveness. A narrow focus on end users would allow a platform as the first-party provider of complementary services sold to sellers to escape the self-preferencing prohibition.

It is unclear to what extent fees associated with rankings are subject to Article 6(5), and if so, whether charging high symmetric fees could be a violation of Article 6(5). It could be clarified whether and to what extent a gatekeeper’s pricing of ranked items falls within the meaning of Article 6(5). While high or differential fees may fall under different provisions of the DMA, **Article 6(5) could be restricted to the design of rankings as a non-price strategy** (which does not preclude the possibility that a third party has to make a payment to be ranked).



### (b) Implementation issues

The prohibition on self-preferencing of the DMA requires context. Therefore, the Commission and the Courts should **not apply this prohibition in a mechanistic manner**. Instead, they should identify self-preferencing conducts that are likely to be against the long-term interest of consumers and use guidance from economics to specify adequately the self-preferencing prohibition. That requires understanding when consumers consider a first-party offer superior to similar third-party offers. Giving prominence to a superior first-party offer should not be seen in conflict with Art 6(5), as such behaviour coincides with the one of a gatekeeper who acts in the best interest of consumers.

Platforms can make life difficult for third-party sellers by using price and non-price instruments. Thus, in the context of self-preferencing, an effective policy against foreclosure and refusal to deal may require **a combination of Articles 6(5) and 6(12)**. Specific commitments must be seen in a broader context to avoid circumvention through other means.

## 2.5. Vertical and horizontal interoperability: DMA Articles 6(4), 6(7) and 7

### (a) Legal clarifications needed

The **vertical interoperability provision in Article 6(7) is broad**. Therefore, the gatekeeper may receive several access requests for different essential functionalities. To make the provision effective, there should be a process for handling access requests efficiently. One possible approach would be to allow the **gatekeeper to define this process under regulatory oversight**.

The **geographical scope** of the horizontal interoperability obligation should also be clarified, in particular, whether the scope is European (i.e., the obligation only requires that a user in the EU should be able to communicate with any other user also based in the EU) or global (i.e. it requires every user to connect to every other user, including outside of the EU).

### (b) Effective mechanisms to implement the obligations

Gatekeepers should be able to define the technical terms of access but follow the **'equivalence of input' when this respects the principle of proportionality**; that is, the entrant should have access to the same functionalities, and on the same terms, as the vertically integrated gatekeeper for its own complementary products and services relying on the essential features. When it is not proportionate, an equivalence of output may alternatively be imposed.

To ensure compliance with those principles, one possibility would be to have a first level of monitoring, where access providers would submit compliance reports, certifying that they satisfy with the principle. In the case of business user complaints, more stringent forms of monitoring (e.g., via audits) could be introduced.

The most appropriate approach for defining access interfaces for interoperability would be to **let the gatekeeper manage access and interfaces** because it has the best knowledge of its services and user interface design, potential risks to integrity, and user security and safety and how those risks evolve over time. In case of complaints and concerns about possible non-compliance, the regulator would investigate the technical specifications of the access interface.



To protect the integrity and security of hardware and software systems, it would make sense to offer access only to players that comply with certain security or privacy standards. **To screen access seekers, access licenses** could be granted based on objective criteria and revoked in case of misconduct. One possible approach would be to allow the gatekeeper to grant access licenses based on public and objective criteria. Another possible approach would be to confer this role to the regulator or an independent third party. Finally, there could be a middle ground where the gatekeeper grants access, but if the access seeker is denied access, it can appeal to the regulator.

### (c) Avoiding and mitigating unintended consequences

The DMA provides that interoperability must be provided “free of charge.”, but the precise scope of this principle is not totally clear. To ensure that the implementation of the interoperability sends the right incentives to all parties, we would recommend that, provided that the principle of non-discrimination is respected, the **costs of providing access for the gatekeepers be covered**, at least partly, **by the access seeker**.

Horizontal interoperability may **reduce multihoming**, which is another important driver of contestability. Therefore, the Commission should monitor the extent of multihoming for messaging services following the implementation of the horizontal interoperability provision.

## 2.6. Data portability for end users and business users: DMA Articles 6(9) and 6(10)

### (a) Legal clarifications needed

The **precise scope of the data** covered by the portability obligations could be clarified, in particular regarding observed data, and whether contextual information in data should also be provided. Specifically, with regard business users’ portability, it could be clarified whether **adversarial portability** is covered.

Several issues related to **user consent for data portability** could also be clarified, especially how granular the consent should be, and whether end-user consent needs to be obtained for each business user or for each core platform service separately. All those clarifications should be consistent with the GDPR rules.

### (b) Effective mechanisms to implement the obligations

The implementation of data portability obligations will require the development of **new tools and mechanisms combining data portability with the protection of privacy, security, and service integrity**. Those tools will support the collection of users’ consent and the transfer of the data. It should be clarified whether end-users should rely on the tools provided by the gatekeepers or may also use tools provided by third parties provided security and service integrity is protected. Any such tools would need to take into account the obligations imposed upon data controllers/gatekeepers by the GDPR to verify the identity of an individual before providing access or portability to personal data relating to them. Those tools could also rely on **open standards** and protocols.

The effectiveness of the portability tools could relate to the **availability and performance of the interface** used for data portability. If the availability and performance of the provided interface is low,



then portability cannot be effective. Performance and availability can be benchmarked against the gatekeeper's other consumer-oriented interfaces

### (c) Avoiding and mitigating unintended consequences

The obligation to offer tools for data portability to consumers may **crowd out independent Personal Information Management Systems (PIMS)** and therefore reduce competition in the market for data intermediation services.

## 2.7. Data access for search engines: DMA Article 6(11)

### (a) Legal clarifications needed

The **precise scope** of data to be shared (with respect to the detail on the query, the search results page, and the user), what is the **scale of data to be shared** (e.g., full or random samples), and what is the appropriate **timeliness of the data** (frequency of updates and recency of the data) could be clarified.

More clarification is also needed on **which platforms could benefit** from the search data access, more specifically, whether the obligation only benefits the general search engines or goes broader as search engine data may be repurposed to innovate and pursue different types of services. In the latter case, search data sharing obligation may provide a stepping stone for entry of new digital firms (not necessarily in the search market) which may ultimately be able to become a sizable competitor and thus increase contestability in digital markets.

The **geographical scope** of the obligation could also be clarified: does it cover only data provided by users in the EU or does it go beyond?

### (b) Effective mechanisms to implement the obligations

The gatekeepers, in agreement with the business users and under the supervision of the Commission, could set up a **combination of technical and institutional mechanisms which achieve more contestability through search data access while respecting privacy and security**. Technical solutions cover K-anonymity, differential privacy, and the recent development towards the creation of 'synthetic search logs'. Institutional solutions involve trusted data intermediaries and data sandboxing (*in-situ* data access).

Regarding the **determination of FRAND price**, a mechanism for negotiation between the gatekeeper and search data access seeker could be established and adapted to the technical and institutional mechanisms set up as well as the arbitration between the key rights and interests at play. In particular, this mechanism could clarify what is the process by which data access options are determined (i.e., who can pick data to be provided and how many different access options must be made available) and whether a price of zero could ever be 'fair and reasonable'.



### 3. RECOMMENDATIONS FOR EFFECTIVE PROCESS AND INSTITUTIONAL DESIGN

#### (a) Oversight and compliance tools

The **compliance report** is a central feature of the DMA: it is the basis upon which the Commission and third parties can monitor the degree to which gatekeepers comply with their obligations.<sup>16</sup> We recommend that these reports should set out both **how the gatekeeper proposes to modify its conduct so as to comply as well as a demonstration that these measures are likely to prove effective**. In the first instance, this may be achieved by the following means: (i) demonstrating that various options were considered and the one most likely to fulfil the aims of the DMA chosen; (ii) showing that discussions with interested third parties about compliance measures were carried out to test various compliance options; (iii) embedding a regular review of the effectiveness of these measures in the process in collaboration with the compliance officer. The last point suggests that compliance reports should be **living instruments that evolve** as gatekeepers understand how to make compliance more effective and as technology changes. Given the importance of these reports, the **Commission should advise on the form and content** of compliance reports early on to set expectations about their contents in line with the suggestions we have made above.<sup>17</sup>

Two procedures exist when gatekeepers are in doubt about how to comply with Articles 6 and 7 obligations: **specification decisions and regulatory dialogue**.<sup>18</sup> While the former is well governed, more detail should be provided about the role and place of the regulatory dialogue. We recommend that dialogue is a less intrusive form of regulation that should occur before starting proceedings for a specification decision. However, the process for dialogue should be transparent and involve third parties.

As already indicated above, to facilitate compliance assessment, the Commission, the gatekeepers, and all other stakeholders could agree on a set of **quantitative measurements, each relating to a particular obligation or obligations**, on the impact of obligations on relations between the gatekeeper and other relevant parties. Those quantitative measures, combined with more qualitative representations from the gatekeepers and their business users would be useful in assessing the compliance with - and the effectiveness of - the DMA obligations.

Powers to require **enhanced supervision**<sup>19</sup> should only be triggered when other enforcement mechanisms do not function.

#### (b) Responsive enforcement

While the DMA has no hierarchy of enforcement methods, we recommend that an **approach based on responsive regulation should be deployed**. This system relies on assuming that gatekeepers wish to comply and that third parties have a voice in shaping that compliance effort. It follows that the first

---

<sup>16</sup> DMA, Art.11.

<sup>17</sup> DMA, Art.46(1f).

<sup>18</sup> DMA, Art.8.

<sup>19</sup> DMA, Art.26.



stage is to persuade gatekeepers to comply via regulatory dialogue informed by the views of third parties. If this does not secure compliance, then enforcement can become progressively harsher until the gatekeeper responds to these signals and complies. This means that greater recourse is made to the supervisory measures in the DMA than to the punitive measures.

In the aftermath of a non-compliance decision, the gatekeeper is expected to explain how it proposes to comply. We recommend two things: (i) that these proposals are **market-tested** as a matter of routine; (ii) that the **Commission gives a clear signal** whether the proposal complies with the DMA.

Fining policy<sup>20</sup> is likely to emerge incrementally but we **do not recommend issuing fining guidelines in the short term**. It is prudent to facilitate cooperative compliance in the first instance.

Gatekeepers enjoy a series of fundamental rights and are entitled to a good administrative process.<sup>21</sup> **Secondary legislation to codify procedures is required to ensure fundamental rights protection** and respect for the principles of good administration. Best practices documents can emerge like in antitrust that can accompany procedural rules.

### (c) Participatory enforcement and private enforcement

Third-party involvement<sup>22</sup> can be enhanced by affording participation at every stage when the gatekeeper is required to design or redesign its compliance efforts – e.g. during the initial phase of writing the compliance report, during regulatory dialogues and procedures leading to a specification decision as well as in the aftermath of a non-compliance decision. At each stage and while protecting confidentiality and business secrets, **the third party should be able to comment on a gatekeeper’s proposal based on clear information**.

Private enforcement is available as the DMA is a Regulation that has direct effect;<sup>23</sup> however, we recommend that **gatekeepers facilitate alternative dispute resolution** with business users for those obligations that deal with the relationship between business users and gatekeepers. The coordination mechanisms set out in the DMA<sup>24</sup> to prevent national courts from rendering decisions that may not be in line with the policy of the DMA are the same as in antitrust law and no more can be achieved to prevent divergent decisions. **Claimants may be advised to exercise self-restraint and pursue follow-on actions** – i.e. bring damages claims after a formal finding by the Commission. **Assigning DMA cases to a court specialised** in similar topics in the Member State may be helpful.

### (d) Adaptative enforcement

The Commission should **monitor the evolution of the market conditions**, particularly the quantitative measurements on the impact of obligations on relations between the gatekeeper and other relevant parties (as suggested above). This will allow the Commission to determine whether the DMA obligations and the measures taken by the gatekeeper to comply with them achieve their intended

---

<sup>20</sup> DMA, Art.30.

<sup>21</sup> DMA, Arts. 21, 22, 23, 34, 36.

<sup>22</sup> DMA, Art.27.

<sup>23</sup> TFEU, Art.288.

<sup>24</sup> DMA, Art.39.



effects. If it is not the case, the Commission may engage in a discussion with stakeholders (gatekeepers, business users, end users ...) to understand why so. This information will allow the Commission to decide whether to adopt the specification of the measure to be taken by the gatekeeper or to open a non-compliance proceeding.<sup>25</sup>

#### **(e) Institutional design and support by national authorities**

National Authorities have a potentially important role to play as sources of information about non-compliance or as investigators assisting the Commission.<sup>26</sup> We recommend that **National Authorities make it clear that they are points of contact for complaints** and they could cooperate to agree on how to best facilitate the processing of complaints. Also, as done for banking supervision, the Commission could set up a **joint investigation team** with a staff of the national authorities.

The **DMA high-level group**<sup>27</sup> which is the hub between the Commission and several networks of national authorities coming from different legal fields (competition law, consumer protection, data protection, electronic communications, and media) could have the following important tasks: (i) ensuring **consistency in the application of the EU digital acquis**, hence consulted on the interpretation of DMA obligation or assessment of tools for which there is a potential tension between the DMA objectives and rules with other EU rules and objectives (such as privacy, competition, security ...), and (ii) **coordinating the EU and national cases against the gatekeepers**.

---

<sup>25</sup> Resp. DMA, Art.8(9) and Art.29.

<sup>26</sup> DMA, Art.37.

<sup>27</sup> DMA, Art.40.



Avenue Louise 475 (box 10)  
1050 Brussels, Belgium  
+32 2 230 83 60  
info@cerre.eu  
www.cerre.eu  
📧 @CERRE\_ThinkTank  
🌐 Centre on Regulation in Europe (CERRE)  
📺 CERRE Think Tank