DIGITALEUROPE

27 May 2021

Digital Markets Act position paper

Executive summary

DIGITALEUROPE fully supports free and fair competition and the EU's ambition to ensure that European consumers and businesses can reap the benefits of the Single Market. DIGITALEUROPE represents the entire digital ecosystem, from start-ups to some of the largest players. Thus we welcome the important discussion about improving contestability and fairness and hope that the Digital Markets Act can provide workable solutions for real challenges.

Digital platforms have driven significant innovation in Europe and enabled jobs and growth by providing services to hundreds of thousands of businesses and millions of consumers. At the same time, new and fast-moving markets can give rise to challenges, some of which will require intervention. For example, prohibiting business users from bringing complaints or unjustified forms of self-preferencing.

DIGITALEUROPE acknowledges the concerns raised about the European digital economy and wishes to contribute to the debate on how to address them. In this paper, we propose constructive suggestions to help improve the proposed DMA.

- DIGITALEUROPE believes that the proposed approach of pre-defined obligations and prohibitions of business conduct are too broadly formulated and will have unintended consequences for the companies in scope and their users. We recommend a **more tailored approach based on regulatory dialogue** between platforms, enforcers and users, which ensures that the DMA provisions are as targeted as possible.
- Improved regulatory dialogue would create a better understanding of market dynamics, the interests of platforms and users, and the technical considerations, resulting in more proportionate and effective outcomes. This will ensure that the DMA does not undermine other EU digital policy objectives such as user safety, protection against illegal content, cybersecurity and privacy. Any concerns regarding the speed of enforcement could be allayed through the use of strict deadlines.
- To improve legal certainty, some of the definitions need to be further refined or aligned with other EU laws. In addition, DIGITALEUROPE

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

strongly believes that **key definitions should not be left to delegated acts**. All relevant stakeholders should be given the opportunity to contribute to developing definitions and methodologies which can significantly impact the implementation of the law.

- To ensure balanced regulatory outcomes, DIGITALEUROPE believes that the principles of accountability, politically independence and judicial review should be better enshrined in the DMA, and procedural safeguards should be reinforced. In its current form, the proposal will lead to a high concentration of power in the regulator's hands.
- DIGITALEUROPE has concerns about the feasibility of the implementation timeline. We **recommend a 24-month implementation period** to leave sufficient time to build and implement new processes.

Table of Contents

Introduction

Digital platforms have driven significant innovation in Europe and enabled jobs and growth by providing services to hundreds of thousands of businesses and millions of consumers. For the smallest players, online platforms have created unprecedented global expansion opportunities, lowering entry barriers and allowing them to scale and compete beyond their home markets. European citizens can share and consume information and conveniently shop across borders in predictable environments. Online platforms have also played, and continue to play, a key role in achieving a truly Digital Single Market.

At the same time, new **and fast-moving markets can give rise to challenges, some of which will require intervention**. Numerous expert reports have tried to shed light on some of the potential shortcomings of the current regulatory environment and its enforcement.

The DMA is an ambitious legislative project. It seeks to regulate many different business models that each pose very specific challenges and that do not easily lend themselves to horizontal rules. The approach of pre-defined obligations and prohibitions of business conduct, seemingly inspired by individual competition cases (several still ongoing), will inevitably have unintended consequences for the companies in scope, European businesses and consumers. In its current form, it could unduly impact the benefits of online platforms for SMEs, undermine consumer choice and user protections (including security and privacy), and reduce incentives to innovate. **A more tailored approach based on regulatory dialogue between large platforms, enforcers and users**, which ensures that the provisions of the DMA are as targeted and limited as possible, appears more appropriate and would lead to more effective outcomes.

DIGITALEUROPE acknowledges the concerns around the contestability and fairness of the European digital economy and wishes to contribute to the debate on how to address them best. The European institutions should aim for a workable DMA that targets specific concerns and limits intervention to what is appropriate. Any new rules should be proportionate and evidence-based, legally certain, as well as in line with existing EU laws and other digital policy objectives.

The case for a more balanced & legally certain framework

The DMA aims to regulate highly complex and dynamic markets made up of a broad set of very different services and business models. Its approach fails to fully reflect this complexity and lacks the flexibility needed to address changing market conditions, customer habits, and technological progress. Both the businesses covered and the individual core platform services themselves pose unique questions that require a tailored approach that allows accounting for inter alia the competitive context, technical limitations and customer preferences. As proposed, the DMA fails to provide a balanced and future-proof solution. DIGITALEUROPE urges the co-legislators to consider the following improvements:

Due to their multi-sided nature, platforms need to balance the interests of all of their users (end-users and business users) and the viability of the service as a whole. At times, these interests will conflict, which requires difficult balancing decisions that the European policymakers should reflect in the DMA. As outlined in Article 1.1, the DMA focuses exclusively on contestability and fairness and ignores the impact for consumers, such as on safety, privacy, and security and for the growth and innovation potential of SMEs. For example, obligations in Art. 5(c) & Art. 6(1)(c), increase the risk of consumers downloading insecure apps from non-verified sources and will increase the fraud exposure for shoppers that get lured away from safe online marketplaces.

A more complete and clearer set of regulatory objectives

Any regulatory intervention in the DMA should not only be measured against fulfilling the objectives of platform fairness and contestability but needs to balance these against secondary objectives: user preferences, security and privacy, as well as protection against illegal/harmful content and fraudulent practices – and broader innovation by business users and the gatekeepers themselves. These goals should be explicitly recognised, as is the case in the objectives article of the European Electronic Communications Code. Additionally, the DMA fails in sufficiently assessing the impact of its provision on European consumer welfare. The DMA consists of a number of provisions that – if adopted in their current shape and form – will profoundly change the way online platforms are delivered to both European businesses and consumers in the future. A more considered process is needed for deep cutting measures that are susceptible to impact the value and experience of consumers or the innovative capability of the platform require more reflection.

A clearly defined scope focused on real concerns and legal certainty

European policymakers should consider the criteria for gatekeeper definitions to ensure the companies covered actually pose contestability risks. The current designation setup grants the Commission too large discretion, undermines legal certainty and risks imposing burdens on platforms or services that do not seem to be the target of concerns. Under any circumstances, the provisions of the DMA need to be as targeted and limited as possible and should only apply to companies whose dominance in a specific market has been established. In addition, neither the DMA nor the accompanying impact assessment studies have shown the rationale for the inclusion of certain core platform which do not constitute multi-sided markets and are characterised by significant competition.

Tailored approach to obligations and prohibitions

The diversity of services, business models and interest in the platform economy makes a one-size-fits-all approach unworkable in practice and too reductive to ensure proportionality and beneficial outcomes. Beyond very clearly defined unfair commercial practices, all other obligations should be tailored to each online service. Therefore, a proper regulatory dialogue should be introduced as precondition for clarifying the scope and application of obligations (Art. 5&6) to increase legal certainty for both gatekeepers and their business users andavoid an overly broad application of the regulation.

Accountable and transparent regulator

The DMA will lead to a high concentration of power in the regulator's hands, with powers to investigate and re-design core services and business models and access gatekeeper algorithms and databases. The European Commission will also be able to specify the designation process and review the list of obligations via delegated acts. In order to ensure that the regulator has the correct incentives, it should be politically independent, transparent and accountable about its decision-making process, and procedural safeguards should be reinforced.

Legal basis

We still believe that the existing instruments already available to the EC, if applied smartly and efficiently – are sufficient to tackle competition issues created by so-called "gatekeepers". The DMA is an additional very far-reaching instrument that intends to implement a quasi-regulatory supervision over certain market participants and bears the risk of creating legal uncertainty and causing unwanted side and spill-over effects which could have a chilling effect on the digital efforts and competitiveness of European companies. Thus, a very cautious approach is key when considering the content of the DMA, and in any case, the provisions of the DMA need to be as targeted and limited as possible.

The Commission proposed the DMA based on Article 114 of the Treaty on the Functioning of the European Union (TFEU), which governs internal market provisions, instead of Article 352 TFEU, which gives the EU the necessary powers to protect competition in the internal market. This means that the DMA needs to address the risk of fragmentation of rules applicable to gatekeeper companies in Europe. However, as the German competition law reform has shown, Member States continue to legislate in this area, covering largely the same issues and the same set of companies. From a legal perspective, it is unclear how two sets of rules could apply in a complementary way as the Commission has suggested, given that conducts covered can heavily overlap with national rules. Taking a practical perspective, the question arises of how companies that are active across the whole EU Single Market, would comply with deviating legal requirements or orders from different national authorities.

The relationship between the DMA under Article 114 TFEU and competition law enforcement under Article 101 and 102 TFEU should also be clarified. Given the possibility of overlap between the two, it should be clearer how the regulator will choose which tool to use to ensure enforcement in the future, and how data is shared between DG COMP and the DMA regulator. Under any circumstances, contradictions between the DMA and EU competition law must be avoided. This also concerns the DMA's Article 12 on notifications of mergers and acquisitions, which would now exist in parallel to existing competition law provisions and in particular the EU Mergers Regulation (139/2004). This could lead to legal uncertainty and potentially higher costs in time-critical transactions. It also remains unclear whether the information provided under the DMA would be made available to competition authorities or the EC's DG COMP and subsequently for which purposes it could be used.

Regardless of the question of whether Article 352 TFEU would be the appropriate legal basis, by relying on Article 114 TFEU, any legislative measure has to comply with the principle of proportionality, i.e. the measure must be appropriate for attaining the objective pursued and not go beyond what is necessary to achieve it. Imposing broad obligations and prohibitions on a diverse group of platforms and services or on the gatekeepers' corporate group, however, might go beyond what is required to address the issues targeted by the DMA. In fact, obligations should be targeted to the concerns that the Commission seeks to address, and only be imposed on the specific line of business, which raises concerns according to the EC. Furthermore, a blacklist of practices, i.e. practices prohibited for any company designated as a gatekeeper, is very likely to go beyond what is proportionate to address market contestability concerns. The DMA should tailor obligations to specific business models and apply a test of pro and anti-competitive effects of gatekeepers' practices.

Scope, definitions and designation of gatekeepers

Core platform services

The set of core platform services targeted in the draft proposal (intermediaries, search engines, social networking, video-sharing, communication services, OS and cloud services) are extremely different in nature. Some are interactional platforms or transactional platforms, while others are technical. The diversity of these services and underlying business models and market conditions makes the scope of the DMA complex, particularly when all targeted companies will then be subject to the same obligations. As underlined by the Regulatory Scrutiny Board, the European Commission did not provide sufficient evidence to demonstrate why all these services raise concerns, and why others – like streaming platforms – have not been included in the scope. Neither is it clear why, and more importantly, how the same obligations would apply to each of the core platform services.

For several services, it is unclear whether there are any market contestability issues. Some, in fact, exhibit very low entry barriers or significant multi-homing by users and others are characterised by dynamic and fierce competition. The DMA's impact assessment does not explain why these specific services were chosen and whether there are sufficient common concerns to justify being subject to the same horizontal rules. Some of the services outlined are already covered by sector-specific legislation. Furthermore, the Digital Services Act, published alongside the DMA, seeks to promote more responsibility for hosting services providers, reducing the prevalence of illegal and harmful content. Where the DSA obligates platforms to enforce more strictly against business users, the DMA in its attempt to increase competition, will increase illegal conduct outside platforms' control. In particular, Art. 5 (c) will allow business users to lure consumers off platform to conduct business there. This will significantly increase the risk of rogue players providing malware outside of app stores and fraud exposure for shoppers outside marketplaces. Platforms will not be able to protect consumers in these settings or provide recourse in case of problems. The DMA and DSA must be properly aligned, particularly when it comes to protecting users against harm.

In addition, the DMA – in its current shape– does not clarify how the definition of core platform services (CPS) apply when they are strongly interlinked. For example, many of regulated individual CPSs form part of a broader service offering of interconnected features that are part of one app or end-user experience. This is particularly true for online social networking services which are "ex se" defined as CPSs and whose features (e.g., marketplaces, communications services, etc.) might also individually qualify as CPSs. Clarity is needed to ensure that regulatory intervention does not prevent the ability of

gatekeepers to offer interconnected end-user experiences and add value for both businesses and consumers.

Definitions

To ensure legal certainty and proportionality, some of the definitions should be further refined or aligned with other EU laws. The definitions are key to the scope of the DMA and should therefore not be left to delegated acts outside of the control of the EU legislator.

Several definitions refer to other EU legislation, some of which is currently being or may in future be reviewed with potential impacts on the DMA. Moreover, the use of "end users" and "business users" leads to entirely different results depending on the methodology used and the core platform service it is applied to. This leads to significant uncertainty regarding the scope of obligations and prohibitions, and inconsistency between drastically different markets structures.

Monthly active end users

The definition of 'monthly active end users' is unclear. The proposal in Art. 3(2) tries to clarify its meaning as 'the average number of monthly active end-users throughout the largest part of the last financial year'. However, it is not clear whether this should be considered to mean 'unique' end-user or how one should deal, in the communication space, for example, with a single unique end-user participating in multiple sessions over time (especially if it would not be possible to determine exactly how many unique users are using the service). A clarification should also be included in the DMA that the requirement of 45 million monthly active end-users solely relates to direct end-users of the "core platform service" and not to "indirect" end users that are not customers of the "gatekeeper" itself but customers of the "gatekeeper's" business users.

Business users

The term 'business user' is also unclear. According to Art. 2(17), it means any natural or legal person acting in a commercial or professional capacity using core platform services for the purpose of or in the course of providing goods or services to end-users. This definition appears not to require any contractual relationship between the core service provider and the potential business user. This stands to capture an almost unlimited range of potential business users, as virtually any company could claim to be 'using' the platform service.

The Commission has decided to modify the long-established legal definitions of business users and end-users established in the EU recommendation 2003/361. By blurring the distinction between end-users and business users, the proposal creates uncertainty around one of the main criteria to define a gatekeeper. The

wording should clarify that employees should not be counted as business users (as they do not personally subscribe, in a professional capacity, to a core platform service) nor as end-users (as they are merely defined as the opposite of a business user).

Ancillary services

The definition of ancillary services (Art. 2(14)) broadly covers "online advertising services" without any distinction between the different solutions offered. Online advertising services are defined as being both a primary core platform service (Art. 2.2(h)) and an ancillary service, creating legal uncertainty regarding the status and obligations related to these services. In some situations, online ads are the core business of a platform service. For social networks, for example, ads are the product that providers offer to their customers and the medium that enables them to provide their services free of charge to end-users. Moreover, including advertising services in the definition of ancillary services would also not be consistent with the P2B Regulation, which defines 'ancillary services' as services that are the technical support for the provision of a service offered to the consumer by the platform. We believe that the DMA should clarify that online ads constitute a primary service rather than an ancillary service. This would require carving out online ads from the definition of ancillary service.

Designation of gatekeepers

The DMA opts for simplicity of enforcement over precision of scope in its choice of quantitative criteria for legal presumptions in the designation of gatekeepers. If the DMA seeks to address market contestability concerns, these should be addressed with appropriate tools, beginning with assessing the market situation. The turnover or number of users says little about the impact on the EU internal market or the contestability of market positions. Thus, it is an insufficient proxy for the gatekeeper designation. Several of the academic reports and studies featured in the impact assessment accompanying the DMA refer to elements such as market entry barriers, the level of user multi-homing and simply the level of existing competition that would or would not justify intervention.

The designation process for gatekeepers raises important concerns about legal certainty, particularly for companies close to meeting the presumption thresholds. It is problematic that the mechanism used to determine whether a company is listed as a "gatekeeper" reverses the burden of proof once the criteria defined in Art. 3 are met. It requires companies to conduct a self-assessment and to provide the required information to the EC. A company fulfilling these criteria can only rebut the gatekeeper presumption by a substantiated submission of facts.

The DMA provides for stringent obligations and prohibitions that require significant compliance steps by companies covered and that deeply intervene in business models. A looming gatekeeper designation risks undermining the planning certainty businesses need to grow in the single market.

For this reason, rather than immediately applying the full set of obligations and prohibitions, the DMA should introduce a two-step approach: a first step where gatekeepers' designation leads to further regulatory scrutiny, and a second where the obligations are imposed and further defined on a case-by-case analysis. This process would be more flexible. Such an approach may potentially take more time than imposing blanket obligations on a broad set of players, but it would at the same time also ensure that only real issues are addressed and avoid the detrimental effects that an overly broad application of the regulation would have. Furthermore, strict deadlines for these procedures could ensure faster application.

Designation criteria

The set of criteria used to designate a gatekeeper raises questions in terms of legal certainty and accountability and whether it ensures proportionate and beneficial regulatory outcomes. The three main criteria outlined in Art. 3.1 are vague, despite being the ultimate tests for intervention by the regulator, which, will make it difficult for a targeted undertaking to rebut the designation process, let alone assess whether they fall within the scope of the Regulation.

Size does not necessarily demonstrate a lack of contestability in the market. It is therefore crucial that the designation process takes into account the characteristics of the platform as well as the existing competitive pressures such as the degree of multi-homing among users and/or business users. In this light, DIGITALEUROPE welcomes the opportunity provided to rebut the designation based on quantifiable criteria in order to look at qualitative criteria as well, in case of such rebuttal.

It is also worth noting that the specific threshold chosen by the European Commission are not always clear or able to demonstrate market power:

- It is unclear how turnover and market capitalisation may be an indicator of significant impact, while relevant criteria like market share are not taken into account.
- A requirement of providing a core platform service in at least 3 EU member states raises the question of whether companies that otherwise fulfil all criteria do not pose the same concerns. The number of users does not reflect users' ability to multi-home or access content and services in other ways or the level of individual usage. Furthermore, a

strict 10% of the EU population requirement does not reflect the huge differences in the reach of various services.

Since the quantitative thresholds in the DMA are weak proxies for market power and it is fundamentally unclear how the criteria in Art.3.6 will be interpreted, a '**safe harbour**' should be incorporated within Art.3. This would expressly exclude core platform services that are clearly not positioned to act as a gatekeeper from the scope of the regulation. Such a safe harbour may be appropriate where, for instance, a core platform service meets the quantitative thresholds but, due to the presence of a clear market leader, holds less than 10% of the relevant market. This would provide greater legal certainty and ensure that the resources allocated by the Commission are not wasted dealing with unproblematic cases. The absence of a safe harbour may invertedly stifle contestability, subjecting incumbents' challengers to obligations which are not commensurate with their importance on the market.

Furthermore, the **turnover threshold** should solely apply for turnover linked to "gatekeeper" (digital) activities since otherwise companies could be captured which achieve only a very limited turnover with digital activities however – due to their core activities – still have revenues exceeding EUR 6.5 billion per year.

The fact that the Commission can use delegated acts to develop and review the underlying methodology is particularly worrying from a legal certainty perspective. The decision-making process will not be subject to the legislator's scrutiny and may indirectly impact the scope of the DMA, e.g., the definition of "active user" may differ significantly, especially between the different core platform services.

Finally, Art. 3(6) qualitative criteria should be further clarified to improve legal certainty and ensure the regulator takes into consideration market realities:

- The reference to "other structure market characteristics" for example, is not defined and overly broad.
- The regulator should also consider the existence of multi-homing on at least one side of the market and the existence of alternative opportunities to reach consumers and business users both out and on the targeted core service.
- The ability of the regulator to target foreseeable gatekeepers it very problematic from a legal certainty and innovation perspective.

Obligations

The DMA appears to be based largely on past and ongoing competition investigations in the digital economy. The approach of turning remedies applied

to specific companies and business models under certain market conditions into generally applicable rules is problematic. It risks regulating practices that are not generally concerning and creating unwanted side effects for business models, for which they were not originally designed. There is no evidence stemming from these cases nor general economic research that would conclude that these practices have a detrimental effect across all business models and markets. The fact that a company is designated as "gatekeeper" should not automatically trigger the application of Articles 5 and 6 to all its core platform services that meet the requirements of "important gateway for business users to reach end-users", which in itself remains unclear. Instead, the Commission should, in a second step, designate those services that do pose a risk to market contestability and exhibits unfair practices.

Ahead of the DMA publication, discussion centred around "grey-listing" certain obligations, allowing for their application on a case-by-case basis taking context into account. However, the published proposal does not do this and only states that the Commission will discuss how to comply with the Article 6 measure. This is neither a true grey list, nor is it a balanced case-by-case approach. It currently means that all Article 6 obligations apply to all gatekeepers, resulting in overregulation and imposition of obligations that will mean a high burden without changing the contestability of certain markets.

The DMA should allow gatekeepers to bring forward arguments to rebut the applicability of an Article 5 or 6 measure to their business model where the practice has pro-competitive effects or consumer benefits. Under this defence, a gatekeeper could argue that in its particular circumstances, a specific prohibition or obligation would create an efficiency loss that would outweigh any potential gains to the contestability of digital markets. Similarly, it should be possible for a gatekeeper to bring forward evidence that a specific Article 5 or 6 measure is not relevant to its business model or would represent a disproportionate compliance effort compared to the increase in market contestability. Any concerns regarding enforcement speed could be addressed with strict deadlines for the procedure. This would also ensure that companies do not lose fundamental due process rights, which they would have had in a competition investigation of the same practice.

Necessity of a tailored approach

The proposal is framed to avoid a case-by-case assessment based on market-related factors such as market power, capacity to exclude, foreclosure effects and consumer harm. It thus prioritises speed above all other considerations.

However, **the prohibitions mentioned in the DMA are so broadly formulated that they risk capturing many pro-competitive practices, or impact pro-consumer company policies linked to user safety, privacy and security**. Many of the prohibitions would discourage investment, pose data security issues, create disincentives to opening up a service to third parties and deprive consumers of valuable services or expose them to higher fraud risk.

The fact that all obligations will apply automatically and to their full extent once a company is defined as a gatekeeper, independent of its market position, size and business model is not proportionate given potentially significant differences between companies that might fall under the definition. Since Art. 5 & 6 are a significant intervention for any affected company, there should be tailoring of which provisions are applicable to the specific gatekeeper.

Tailoring the obligations is the only workable option because it recognises that there is **no one-size-fits-all solution**. Each online service is different and must be assessed on its own merits. Given the DMA address often the same questions as would have been addressed under competition law, a comparatively thorough assessment should take place. There is a risk that a blacklist of blanket prohibitions could be used to ban conducts, which are not anti-competitive. The application of the ex-ante framework should be subject to robust (effects-based) analysis.

Data practices

In relation to data practices, the DMA introduces obligations on (i) real-time data portability, (ii) real-time access to business user and end-user own data and (iii) search engine competitors' access to search data in FRAND terms. The DMA also prohibits (i) the combination of personal data and (ii) the use of business user data for competing services.

The provisions on data practices are overly broad and imprecise in scope and will result in some cases in less competition to the detriment of consumers where gatekeepers no longer provide or introduce a service that competes with an existing market leader. Such broad provisions could also reduce present and future incentives to build platform services for business users in the first place or limit the activities to which they have access.

Data portability

The proposal creates an asymmetry between those companies that are considered to be gatekeepers and their competitors. In relation to their platforms, the gatekeepers would be required to facilitate business users moving their data to a competitor through data portability tools (Art. 6(1)(h)). In contrast, the competitor would not be required to do the same. This would distort competition.

In addition, the DMA fails to recognise that enabling portability would also require technical implementation on the side of data recipients, i.e. competing platform services. It is unclear whether these services even have any interests in such transfers given they have no control over the data transferred and cannot verify data either.

Combining personal data

Furthermore, the use of personal data is already subject to GDPR rules that set the requirements for lawful processing of personal data, including when combining data from different services. Any new regulation on sharing and processing personal data must take into account existing rules protecting privacy and security of users, particularly under the GDPR. For example, Art. 5(a) would force gatekeepers to require consent for combining data, when GDPR offers over legal basis for processing. There should still be legitimate reasons for combining data, for example for customer support, where the legitimate interest, contract fulfilment, and other legal bases offered in the GDPR should remain available. Finally, the DMA should not prevent gatekeepers from encouraging good privacy practices more broadly. From a customer perspective, it is questionable whether each and every purchase on an Appstore, every consumption of a third party video or the purchase of a product in a marketplace should trigger a user prompt for "consent for data access for the business user". Not only would this create a sheer endless number of user prompts but also it overlooks the issue that many business users are located outside the EU and it remains unclear whether personal data access, even customer consent should be given.

The prohibition on the use of data from different services would severely impact customer experience as data is an important input for improving and innovating the user experience on services. For instance, if companies cannot combine two complementary services, they will not be able to make the most relevant recommendations for their users. Furthermore, the combination of data from different services is allowed under the GDPR. It will therefore confuse consumers in terms of their privacy rights, when the DMA proposal has a privacy right that contradicts the GDPR rules on the combination of data. As a result, a case-by-case assessment of the prohibition's scope is required to identify the few instances where consumers and contestability are harmed. For several of the core-platform services in scope, it is questionable whether new entrants have difficulty competing because of a lack of data and whether data use restrictions would facilitate new entrants at all.

Furthermore, some data is used exclusively to maintain security, prevent fraud, fix bugs etc., across services, and its use should never be limited. Online services are targets of cyber-attacks and fraud and exposed to technological vulnerabilities. Gatekeepers' services generate data that is used to maintain the

security and integrity of the services. An obligation not to use data (i.e. also to combine) would adversely affect the ability to detect fraud.

Data access

The reference to giving access to non-aggregated data raises important privacy challenges. Some services strive to gather non-personally identifiable data and providing them to business users in aggregate format increases anonymity. The DMA should be careful to avoid mandating the collection of data where data is not collected in the first place or forcing service providers to render non-personally identifiable data identifiable – as it stands, Art. 6 (1)(i) could force service providers that only gather customer data on an anonymised basis to re-identify the user in order to comply with business user non-aggregated data access requirements.

Data sharing would also lead to cybersecurity concerns. Consumers expect that their information is processed according to high standards. Once the data is shared outside of the original service provider's platform, the provider can no longer ensure data protection and it is unlikely that all business users will have the same level of security in place to protect the data. In addition, real-time and continuous data access also raises potential conflict with the GDPR, which requires verification of the data subjects' identity before processing data access requests.

As it stands, the DMA proposal appears to overlook that data can be used to promote competition and also that platform service providers already have incentives to provide strong data analytics to their business users, as long as it fits consumer expectations of user safety, privacy and security. This principle should be taken into consideration.

Data is not technically easy to transfer, particularly continuously and in real-time – as mandated by obligation Art. 6(1)(h) and 6(1)(i). There is no commonly agreed standard or infrastructure for exporting data. These are being reviewed by the IoT sector inquiry and need to be developed. As a result, the provision should not enter into force until the appropriate international and European standardisation bodies have developed or identified suitable standards and technical specifications for the transfer of data. Without such standards, the provisions would not have the desired result.

The proposal should introduce a safe harbour for gatekeepers. Where customer data is shared with a business user, the business user becomes a data controller in its own right and has to comply with the obligations under the GDPR when processing the customer data. However, according to Article 26 of the GDPR, "joint controllers" are liable for the entire damage caused by the processing. To

avoid any legal uncertainty, the proposal should provide that the gatekeeper cannot be held liable for any third party's misuse of the data.

Self-preferencing

In relation to the self-preferencing provisions, the DMA introduces obligations on (i) wide Most Favoured Nations (MFNs)/parity clauses, (ii) free choice of distribution channel for business users, (iii) the end-user right to un-install apps, (iv) equal access and interoperability and (v) app store access on fair terms. The DMA also prohibits (i) the self-favouring ranking.

Use of parity/MFN clauses

There is no basis for a blanket ban on wide MFNs (Art. 5(b)). MFNs should be subject to case-by-case assessment based on the specific context in which MFNs apply. The 2019 expert report on EC-commissioned Competition policy for the digital era argues that "[MFN] or best price clauses may have both pro-and anti-competitive consequences and their effects depend on the particular characteristics of the markets. A case-by-case analysis is therefore necessary". It must be recognised that service providers have a legitimate interest in taking reasonable measures to maintain the service's competitiveness. As a result, the proposal should be narrowly defined to include only contractual obligations that prevent business users from offering more favourable pricing terms on competing third-party services. Other forms of MFNs should be subject to competition law only. There is no basis for prohibiting such MFNs without a case-by-case assessment of their effects.

Promoting offers outside of the platform

With Art. 5(c), the DMA proposal as it stands also poses a risk of free-riding and makes the enforceability of commission-based business models impossible at scale. This would undermine investment incentives and interests of platform users if the prohibition includes restrictions on steering on the service itself (e.g. links in offers to complete the transaction off-platform). For instance, it would turn marketplaces or app stores into unpaid advertising platforms allowing sellers to capture users and direct them to fulfil the purchase on their own sites. This obligation, which would be unacceptable offline, would also send a signal to growth-oriented platform service providers that commission-based business models is not a legitimate business strategy.

Pre-installed apps

When it comes to the uninstallation of pre-installed apps Art. 6 (1)(b), this practice is already embraced by many service providers. Consumers expect an

adequate out-of-the-box experience when purchasing a device. Whilst the requirements outlined in the obligation is already in line with current business practices, some pre-installed apps are essential to the functioning of a device, across the life-cycle, including in controlling specific interfaces and hardware tools, and well to access other services and content (like app stores and browsers). The article's reference to services that cannot be technically offered on a standalone basis may be too narrow to ensure adequate user experience across the life-cycle of the device

Fair and non-discriminatory ranking

. DIGITALEUROPE also believes that any prohibition of discrimination in favour of own gatekeepers services should be confined to measures regarding display and ranking that deliberately demotes business users' offers or boost the prominence of gatekeeper's own offering. It should not apply when the attributes and weighting are applied equivalently to a business user and own offers. Doing so would interfere with the ability of the gatekeeper to display offers that it predicts provides the best overall value for customers. The requirement in Art. 6(1)(d) that the gatekeepers must apply "fair and non-discriminatory" conditions to ranking services means, in practice, that the rule is open to interpretation and will lead to a complaints' wave. The EC would become an appeals board for controlling the business decisions of online intermediation services, interfering with their ability to manage their businesses in the interest of consumers.

Access and interoperability

Operating systems – whether on consumer devices or enterprise server-side platforms - are technical platforms that manage hardware and user interfaces and are core to the functioning of devices. They play a key role in managing device performance, ensure compliance with product safety rules, and frame access from a security and data protection point of view. This is particularly important in a mobile, wearables and IoT context, where the device hosts and generates significant amounts of sensitive personal data (i.e. health/fitness related sensors, location data, etc.)

Developer functionality

The effect of obligation Art. 6(1)(c) and 6(1)(f) should be carefully considered against the ability of an operating system provider to manage, at scale, third party access to device functionalities. The side-loading of software straight from the open internet has been a long-standing challenge from a cybersecurity point of view, in order to effectively manage protection against malware and other cyber-security threats, making it harder for operating-system providers to assess

and manage threats overall. Allowing side loading will have an important impact on security and privacy.

Providing third party access to a specific technical functionality has important user implications. From a consumer perspective, access can impact user experience and security, thereby affecting user trust/interest in the underlying technology or service. Business users can only rely on access to stable, mature functionalities as a platform to innovate and, in some cases, build a business and livelihood.

In this light, Article 6(1)(f) is not sufficiently defined to be immediately applicable and should only be imposed on a case-by-case basis. A caveat around operating system integrity should also be introduced, so that access is encouraged, but not at the expense of security, privacy and technical performance.

Fair and non-discriminatory application store access

The obligation to apply "fair" access conditions in Art. 6 (1)(k) presents a challenge since what is fair for one set of users may be seen as unfair for others. The lack of legal certainty here is likely to lead to the contestation of both gatekeeper compliance and related Commission decisions. To ensure a fair business environment, the DMA should rather seek to address and define what is unfair and prohibited. This is the approach taken by the Unfair Commercial Practices Directive or the Unfair Trading Practices Directive in the agri-food sector.

Tying-Bundling

In relation to the tying and bundling provisions, the DMA introduces an obligation on (i) integration and effective use of third party apps and it prohibits (i) the restriction on business users' use of competing identification services, (ii) the restriction on free choice of services and (iii) the restriction on the ability to switch apps and services

If the tying and bundling provisions also cover a gatekeeper's own services, in contrast to providing log-in services for third parties, it would create an unlevel playing field and give rise to serious security risks. Any company offering services to users must be free to design and provide the identification service used to authenticate consumers accessing their services. The gatekeepers are responsible for preventing security breaches. They cannot be forced to permit the use of third-party identification services even if they are claimed to be or even demonstrated to provide the same security level.

We suggest limiting the scope of prohibitions to technical actions that serve only to prevent switching and seek to deliberately break interoperability.

Audit & compliance of advertising services

In relation to the audit and compliance provisions, the DMA introduces the obligations on (i) advertising pricing and remuneration and (ii) advertising performance transparency. The DMA also prohibits (i) the restriction on complaints.

However, some of the issues covered by the proposal are already adequately covered by the P2B Regulation. In keeping with principles of "better regulation" and proportionality, the DMA should cover only instances where there is a clear need for new rules to protect competition and users of a gatekeeper service.

The Commission should also consider the relationship with national laws that already require disclosure of rates and transparency with online advertising. For instance, the French Loi Sapin, which requires media-buying agencies (and digital advertising services) to report directly to the advertiser a month after their advertisements appear, with a rate card and details about the services that were performed. Both Loi Sapin and Art. 5(g) are intended to ensure transparency in the online advertising market.

Another issue is that a broad category of auditing/verification of advertising systems by non-vetted third parties raises several concerns. In practice, this will likely require access to some personally identifiable data of end-users and to business-sensitive company data, which should only be granted to vetted third parties.

Suspension & exemption of obligations and prohibitions

As it stands, the DMA's conditions for a suspension and exemption are extremely restrictive. We suggest a more flexible approach, especially given that the change in technologies is rapid. For example, Art. 8 only allows for exemptions where the undertaking as a whole is no longer economically viable. This appears overly restrictive as even a completely unviable core platform service would not be sufficient for an exemption.

As under the current EU competition law framework, an efficiency/pro-competitive suspension/exemption should be provided in the DMA. The prohibitions mentioned in the DMA are so broadly formulated that they risk capturing many pro-competitive practices. Thus, there is a risk that a blacklist of blanket prohibitions could ban conducts that are not anti-competitive, and in turn, be detrimental for consumers. Many of the prohibitions would discourage investment, pose data security issues, create disincentives to opening up a service to third-parties and deprive consumers of valuable services.

Accordingly, the EC should introduce explicitly the possibility for the gatekeeper to bring a defence in order to escape the application of some obligations by demonstrating, for instance, that its practices do not harm market contestability and B2B unfairness.

In addition, DIGITALEUROPE calls for clarity to the concepts of 'public morality' and 'public security'. Such concepts are vague and create legal uncertainty.

Market investigation, enforcement and sanctions

In the framework of legal due-process, the remedies, sanctions and market investigations should be proportionate and well-defined. They should be imposed in the most effective manner to address the consumer harm, and they need to be tailored to the variety of business models in digital markets. There is no one-size-fits-all solution since digital companies have different business models.

Requests for information

According to Art. 19, the Commission may request information from undertakings and associations of undertakings to provide all necessary information. The Commission may also request access to databases and algorithms of undertakings. Such request for information is not limited to gatekeepers, but can also affect third parties. In our experience, such requests for information are cumbersome, time-consuming and subject to very short deadlines. The Commission should use such requests for information to non-gatekeepers with utmost caution in order not to lose acceptance for the DMA and acknowledge the limited resources of companies. The request for access to databases and algorithms should be restricted to gatekeepers themselves and not extend to any third party.

Remedies

Given how intrusive structural remedies are to companies' business model, they should be a measure of last resort. The current "three strikes" approach, i.e. basing structural remedies on three infringements in a given time, raises serious questions such as how the Commission's enforcement priorities may impact the number of infringements, whether investigations can be split into several infringements and whether infringements need to happen on the same core platform services or across all services. In the latter case, it is unclear which structural measure would be applied.

Furthermore, the regulator should regularly review the remedies to assess whether the obligations/prohibitions imposed on a company are still required. Due to the fast-moving nature of the digital markets, a company could lose its

gatekeeper status. The remedies and sanctions imposed following the regulator's assessment should be imposed on the corporate group's specific division, which has a gatekeeper status and not on unrelated activities.

Market investigation tool

DIGITALEUROPE is concerned that the market investigation tool in the DMA grants the EC far-reaching and very invasive competencies. The EC can use the tool to designate platform providers as "gatekeepers" even if they do not fulfil the thresholds in Article 3. In addition, the EC can define new "core platform services" beyond the ones included in the definition in Article 2 and also expand the list of obligations applicable to "gatekeepers". This enables the EC to extend the scope of the DMA significantly at its own discretion. This uncertainty created for companies in the digital field by the DMA contradicts its actual intention to promote innovation, growth and competitiveness in the digital economy.

Regulatory dialogue

Regulatory dialogue is described as an important tool to further define the obligations in Article 6 (Recital 33 ,58 & 60) however, the mechanism for such a dialogue is limited and exposes the gatekeeper to the risk of sanctions. The Commission should be obliged to provide an answer to the gatekeeper and refrain from opening any enforcement proceedings for non-compliance while the dialogue is ongoing.

This dialogue should create a more detailed comprehension of market dynamics, the interests of the platform and platform users, and technical and engineering considerations. It should allow the obligations to be tailored to the core platform service. Regulatory dialogue should also apply to the gatekeeper designation process, particularly when considering qualitative criteria. The obligations in Article 5 should also be open to regulatory dialogue.

In the context of this dialogue, a gatekeeper could argue that in its particular circumstances, a specific prohibition or obligation would create an efficiency loss that would outweigh any potential gains to the contestability of digital markets. Similarly, it should be possible for a gatekeeper to bring forward evidence that a specific Article 5 or 6 measure is not relevant to its business model or would represent a disproportionate compliance effort compared to the increase in market contestability. It will also diminish the prospect of appeals in courts, which would further delay positive impact of the DMA on the market. This dialogue should be led by the regulator, and it should not impact the regulator's ability to launch formal investigations

Any concerns regarding the enforcement speed of such an expanded regulatory dialogue are unfounded. In contrast to competition law enforcement, the

Commission in the framework of a dialogue will not have to establish the relevant market nor the conduct's harm. It can thus jump straight to the remedy step. In addition, strict deadlines could be applied the regulatory dialogue procedure. This would also ensure that companies do not lose fundamental due process rights.

Procedural safeguards

The proposal offers the European Commission very important powers, not only in ensuring compliance but also in specifying how that compliance should look, and adapting the DMA's scope and obligations over time. To ensure balanced regulatory outcomes, the principles of accountability, politically independence and judicial review should be better enshrined in the DMA.

Given the complexity of some of the obligations, the deadline of 14 days linked to the right to be heard in Article 30 should be extendable in specific situations to ensure proportionality.

Finally, the proportionality principle, currently only referred to in the recitals, should also be reinforced, and linked to a broader set of articles, including information requests.

Implementation timeline

The transition and implementation periods throughout the DMA raise major concerns given they appear too short for the steps expected. Several obligations require significant changes to business models, in-depth legal assessment and even technical implementation work. For example, introducing any data sharing or data usage restrictions will mean changes to existing databases; introducing interoperability of systems may require a complete rebuild of key functions. The DMA should foresee a minimum of two years transition period and an option for companies – in dialogue with the Commission – to present implementation plans that go significantly beyond two years.

FOR MORE INFORMATION, PLEASE CONTACT:

Hugh Kirk

Policy Manager

hugh.kirk@digitaleurope.org / +32 490 11 69 46

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, Tech in France
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK