10 June 2021
EBF_045188

The European Commission's proposal of a Digital Markets Act – EBF Key messages

The European Banking Federation (EBF) identifies the Digital Markets Act (DMA) as a central legislative initiative to address fair competition in a digitally transformed market. Following the EBF's early key messages in 2020, we would like to share updated thinking on the Commission proposal from 15 December 2020. European banks continue their position building, reflecting the discussions of the DMA within the legislative process.

Contents

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

Executive Summary

Europe needs more competition to unlock all the opportunities that digital markets can bring. Today, these opportunities, and the competition of firms, increasingly depend on **timely access to relevant digital infrastructure, consumer gateways, data, and markets.** The EBF therefore welcomes the **ex-ante regulatory approach and general principles underpinning** the European Commission's (EC) proposal for a Digital Markets Act (DMA) towards large online platforms acting as gatekeepers. In particular:

1. The proposal envisages **a broad scope in terms of the "core platform services" that will be covered under the DMA**, while setting quantitative thresholds that act as a presumption and reduce uncertainty for a relevant number of platform service providers whose size do not put them, in principle, in a position to generate competition issues for digital markets.
2. The proposed obligations for gatekeepers are comprehensive enough to address the **key unfair practices that have been observed in the market and have proven problematic regarding the business models of very large online platforms**. At the same time, flexibility is built in to provide the opportunity to analyse in more detail issues that may not have yet materialized.
3. **Data and digital infrastructures** are treated in the proposal as **key competitive factors** which platforms leverage across markets and obligations are proposed to address existing issues for third parties to access them.
4. The **Commission will retain extensive powers regarding the implementation of the tool**. This is welcomed and necessary to avoid fragmentation in regulatory approaches across the EU and ensure a level playing field in the Digital Single Market.

However, to ensure that current imbalances in relation to gatekeepers are addressed, the EBF recommends several amendments to the text, notably with regard to the:

1. **Clarifying the Scope of the Regulation -** notably by including a definition of "provider of core platform services" in the Regulation which allows parts of the same undertaking to be considered as separate gatekeepers when they provide different category of platform services while taking into account the whole undertaking for the purposes of the significant impact on the internal market. As there is no definition of tat the moment, it could result in the assumption that a provider of core platform services is equal to that of the undertaking, and uncertainty over what entity is subject to the different DMA provisions.
2. **Sharpening the criteria for the Designation of Gatekeepers by** including clear definitions of business users, end users, and active users for each core platform service. These concepts can be interpreted differently depending on the type of service and context and, without clear definitions, the proposal could miss identifying all gatekeepers within an undertaking or risk overinclusion.

3. **Strengthening the obligations under Articles 5 and 6, with a particular focus on obligations regarding access to infrastructure (Art. 6(1)(f)) and Access to data (Arts. 6 (1)(h) and 6(1)(i). –**
    a. **Infrastructure** by clearly stating that **access to operating systems hardware or software features must be under fair and equal conditions**, which refers to conditions of economic technical, or any other nature.
    b. **Data portability** by, among other points, clearly **requiring a standardised transfer mechanism** that would allow for easy, secure, real-time, and recurrent data transfers. Standardisation of the data formats and of the transfer mechanism, including security requirements, should be considered, **and can be developed under the frame of the Commission implementing act, for which Article 36 provides the possibility.**
4. **Reinforcing provisions to bolster gatekeeper compliance with obligations** by enhancing article 7 through measures such as strengthening the regulatory dialogue by requesting gatekeepers to notify the measures it intends to implement to ensure compliance with Art. 6 obligations and through introducing a provision to allow third party feedback in proceeding under chapter 5, thereby also allowing business users channels to communicate gatekeeper's non-compliance beyond existing competition tools.
5. **Clarifying provisions related to Enforcement** including on the coordination between the European Commission and national courts, and the governance framework within the Commission.

A separate EBF document will follow with proposals for amendments that reflect the key messages in the text.

Detailed Key Messages

1. Scope of the Regulation

a) Core platform services & providers of core platform services – resolving uncertainties

We welcome that the EC has envisaged a **broad scope** in terms of the "**core platform services"** that will be covered under the DMA, rightly **going beyond the definition of an online intermediation service in the Platform to Business Regulation**[1] **(P2B)** and capturing **other relevant platforms such as mobile operating systems or social networks.** However, we would recommend to clarify several points in Art. 2(2) when referring to "core platform services".

As there is no definition of "***provider*** of core platform services", there is uncertainty between this concept and the concept of **"undertaking."** Leaving this question unresolved could lead to an assumption that a "provider of core platform services" is equal to that of "the undertaking", meaning that it could be difficult to capture which entity is relevant regarding the different provisions of the DMA – especially considering the often complex group structures of corporations.

If the qualification as gatekeeper were to be attributed to the economic unit or "**undertaking" *as a whole*** within the meaning of competition law, any company above a 65 billion EURO of market capitalisation and 45 million customers that starts providing core platform services in the EU would be caught, thereby contributing to market failure. The fact that the **gatekeeper designation applies to business units instead of whole undertakings seems to be a widely accepted understanding of the Proposal's spirit.**[2]

We therefore recommend **to include a definition of "provider of core platform services" in Art.2** which:

1. Allows **parts of the same undertaking to be considered as separate gatekeepers when they provide a different category of core platform services**
2. Takes into **account the whole undertaking for the purposes of the significant impact on the internal market** and relevant procedural provisions in chapters IV and V of the proposal.

This definition would allow to capture feedback effects among gatekeepers within the same undertaking and maintain the element of intervention in relation to the whole undertaking having a significant impact on the internal market.

[1] Regulation (EU) 2019/ of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (europa.eu)
[2] See A. de Streel, A. Fletcher and B. Liebhaberg (2021), "The European proposal for a Digital Markets Act: A first assessment", Centre on Regulation in Europe, p. 13 (available at https://cerre.eu/publications/the-european-proposal-for-a-digital-markets-act-a-first-assessment/).

b) Definition of 'ancillary services'

The definition of ancillary services under article 2(14) explicitly mentions payments services within the meaning of article 4(3) of PSD2 and technical services within the meaning of article 3(j) of PSD2. However, it is unclear whether the identification of these services as ancillary services excludes the possibility that these services could eventually be identified as core platform services themselves (as is the case with advertising services, which are identified in the Proposal both under the concept of core platform services and the concept of ancillary services). We believe that this possibility should not be excluded as in particular some **technical services that support the provision of payment services exhibit the features identified in Recital 12 of the Proposal as inherent to "core platform services".**

For instance, **aggregators of payment services (e.g. mobile wallets solutions)** allow payment service providers the possibility to integrate their payment solutions on a single interface, so that end users can enrol their digital payment instruments issued by the payment service providers and execute payments from that platform / aggregator. **When provided by an undertaking providing other core platform services, payment aggregation services which connect many business users (e.g. payment service providers) with many end users may show strong network effects, lock-in effects, and a lack of multi-homing or vertical integration. We therefore recommend that payment aggregation services, when provided by a provider of any of the core platform services listed under Art. 2, that are considered as a gatekeeper should be treated as "core platform services" themselves.**

The inclusion of payment aggregation services as core platform services would enable the application of all obligations under Articles 5 and 6 to those payment aggregation services qualifying as gatekeepers, **helping to address the following situations:**

- As providers of payment aggregation services are increasingly becoming providers of payment services themselves, they could treat their own payment services/instruments more favourably in terms of display or usability within the payment aggregation services than those of their users (e.g. PSPs). In combination with other core platform services, this could significantly increase lock-in risks for consumers and hinder competition - similar to effects we see related to authentication methods used in digital ecosystems.
- They could impose the use of their own identification services to business users when interacting with end users, which would harm the development of trusted digital identities in the financial sector.
- They could impose access requirements that restrict the conditions under which the same payment instruments are made available through other channels.

Including these providers in the scope would also mean that they are required to enable the effective sharing of data related to the use of the wallet and transactions.

However, as the definition of online intermediation services does not seem suited to cover payment aggregation services, a new definition should be included under Article 2(2*): 'Payment aggregation services' means technical services within the meaning of article 3(j) of Directive (EU) 2015/2366 of the European Parliament and of the Council allowing end users to enrol and execute payment services within the meaning of article 4(3) of Directive (EU) 2015/2366 of the European Parliament and of the Council, on the basis of a contractual relationship between the payment aggregation service provider and the payment service provider whose payment services are aggregated.*

However, we believe that payment services, as defined under Art. 4(3) of PSD2, **that do not themselves allow business users to offer goods or services to consumers but rather are only *the means* by which payment transactions are conducted are rightly identified as ancillary services and should *not* be considered a "core platform service**". In addition, Art. 1 under the P2B Regulation *explicitly* left online payment services out of the scope, based on the belief that payment services do not themselves meet the applicable requirement inherent to an online intermediation service. In addition, we would like to note that as soon as any platform starts performing payment services it should then be regulated under PSD2.

c) Market investigation to add new services to the list of core platform services

We welcome that the proposal includes the possibility for the European Commission to conduct a market investigation to examine whether more digital services should be added to the list of core platform services, and that this would be done through an amendment of the Regulation. This is very relevant as for certain emerging services it might be difficult to know yet whether the providers could derive a gatekeeper position from the provision of such services (e.g. such as blockchain networks).

2. Designation of gatekeepers

Not all digital platforms necessarily have market power that allows them to distort fair competition. **We therefore support the Commission's targeted regulatory action which limits measures to platforms that have the power to influence the market in a substantial manner.** Making this important distinction between large online platforms and other innovators organized under a platform business model or who provide part of their services under a platform business model **allows for fostering an environment for innovation while protecting fair market operations.**

More specifically, we welcome that, in the designation of gatekeepers, **the proposal uses both qualitative and quantitative criteria.** Applying qualitative criteria under Art. 3(1) cumulatively, concretized by Art. 3(2) in terms of quantitative thresholds allows for an effective way to accurately identify large online platforms' gatekeeper role. However, elements of **Article 3 need clarification in order to avoid that the DMA captures large companies whose presence in digital markets do not raise fairness or contestability issues.**

a. Introducing clear definitions of 'end user', 'business user' and 'active user'

The **criterion** for designating gatekeepers needs to **be based on clear definitions to offer as much legal certainty as possible to firms.** In this regard, the **concepts of "business users" and "end users" can be interpreted differently and be of different relevance depending on the core platform service of reference**. For example:

i. For communication or social networking services it might be challenging to judge whether a user, either a natural or legal person, **is acting in a commercial or professional capacity for the purpose of or in the course of providing goods or services to end users,** for instance if the use of the platform service is only auxiliary to their main service and not per se aimed at providing goods or services.

ii. For cloud computing services, it might be difficult to discriminate whether the **threshold of active end users** is reached by companies that act as gatekeepers **unless a clear definition and criteria is provided on what is an "active end user" in this context**. As Recital 13 notes, in this context businesses that rely on cloud computing services might be considered end users.

The Commission should therefore develop **a clear definition of the concept of business and end users for each core platform service, including a clear definition for "active user"**. This should be developed by the Commission together with the methodology for determining whether the quantitative thresholds laid down in Article (3)(2) are met, as contemplated under Article (3)(5). The Commission could consider issuing a delegated Act to do so, within a swift timeframe after the adoption of the proposal. However, this should not lead to further delays of the implementation of obligations in Art. 5 and 6.

b) Criteria under Article 3(6)

In order to ensure sufficient legal certainty and stability in the application of the rules **as regards identification of gatekeepers on the basis of a qualitative assessment and to prevent regulatory arbitrage**, the Commission should **further develop the qualitative criteria contemplated under Article 3(6)** on the basis of which:

i. Providers of core platform services can demonstrate that they ***do not*** meet the gatekeeper definition (even if the quantitative thresholds are passed)

ii. The Commission can, through a market investigation, designate other gatekeepers providing core platform services that **do not meet all the thresholds**. This should also include as a criterion **the presence of other gatekeepers within the same economic group**. Otherwise, this could allow companies providing core platform services from artificially excluding relevant services from the scope of the DMA. It would also not consider the possibility that the core platform service can leverage the possibility provided by the presence of another gatekeeper within the group to grow exponentially. This would take into account the 'future' element already included in the proposal.

When analysing the relevant market structure, the EC should also consider **multi-homing,** as well as the extent and strength of current and potential connections from the core platform market to other markets (in which the platform firm may or may not be present).

Finally, based on suggestions above and to increase legal certainty for all stakeholders, we would recommend the European Commission to **issue a delegated act (per Article 36) outlining how the Commission will evaluate the qualitative and quantitative criteria for the designation of gatekeepers.**

3. Obligations for Gatekeepers

Clear obligations and prohibited practices for large online platforms with economic power can provide European consumers and business users with more choice and access to innovative solutions. **New rules need to be workable and sufficiently future proof** so as to be able to address effectively issues that are currently present in digital markets

with large online platforms, as well as new issues that **could arise in the future** as digital markets continue to grow and evolve.

In this regard, we welcome the EC's approach to outline obligations for gatekeepers in Article 5. Additionally, Article 6 introduces the concept of obligations "susceptible of being further specified". The relationship between these articles should be clarified, especially regarding the effectiveness of its enforcement, considering possible differences in effective protection of fair competition and markets against gatekeeping effects. **Ensuring that both sets of obligations are effectively implemented by designated gatekeepers, regardless of whether they fall under Article 5 or Article 6 is crucial.**

Key aspects under Article 6 should also be secured with sufficient legal clarity and certainty, particularly on:

a. **Art. 6 (1) (f) interoperability**
b. **Art. 6 (1) (h) data portability**
c. **Art. 6 (1) (i) data access**

We also recommend adjustments on other obligations under Article 5 and 6, **as well as on the measures for gatekeepers' compliance with the obligations.** The **operationalization of these obligations must be considered**. While the option is available under Article 36 for the European Commission to present implementing acts on some of the Art.6 obligations, looking at potential barriers to end users and business users to benefit from the new opportunities – and to have the envisaged effects on competition in digital markets – is crucial.

a) Article 6(1) (f) interoperability / access to infrastructure

We strongly support the inclusion of an obligation on access to infrastructure. **It is of vital importance that market participants get equal access as the gatekeeper's group companies in order to obtain or maintain a level playing field and ensure more competitive digital markets.** However, the **current provisions need to be reinforced.**

Gatekeepers often **provide technical infrastructure that is increasingly relevant for the provision of digital services.** These infrastructures include devices and their associated functionality, such as biometric authentication or communication protocols like Bluetooth and near field communication (NFC) as well as App stores and pre-installed apps on devices. However, this infrastructure is not always available on an equal basis to all market participants, with elements controlled by some market players and/or technical providers.

This may be done **by restricting, or simply denying access** to certain platform hardware or software which is necessary for business users of the ecosystem to effectively provide services in competition with the platform operator, or by **degrading interoperability** between the platform and products or services acquired by end users from business users of the platform so that **the user experience is not the same as if such products or services were acquired from the platform operator**[3].

We would like to highlight three examples:

1. An application in Host Card Emulation that is opened for third parties in Android needs to be opened separately every time to activate the NFC-stack card emulation.

[3] The aforementioned concern underlies, for instance, the European Commission's enquiring into potentially restrictive practices by Apple under Articles 101 and 102 of the Treaty on the Functioning of the European Union consisting, among others, of alleged restrictions on access to the NFC technology embedded on iOS mobile

Native Google Pay and Samsung Pay function directly from the locked screen of the mobile phone with biometric authentication.

2. On IOS, third parties have no access to the NFC-stack card emulation without participating to the Apple Pay scheme. Access under equal conditions is crucial as operating systems are based on "native solutions" and in the experience of members, it often happens that even if systems are opened to other users, this opening is done with a "worse solution" than the native one. The native access to card emulation should not be limited to the gatekeeper's own payment solutions.
3. Should a provider of social networking services or interpersonal communication services decide to offer payment solutions as an ancillary service of the former services, Art. 6(1)(f) should grant third parties that provide competing payment solutions access to the software features that are available or used by the gatekeeper. Otherwise, this would significantly undermine innovation in the provision of payment solutions as well as choice for the end users.

Therefore, given the critical importance of access to, and interoperability with, platform elements which are necessary to create a level playing field in the provision of services by business users and platform operators merits, **we propose the following changes:**

i. **Article 6(1)f should be amended to clearly state that access to operating systems hardware or software features must be under fair and equal conditions,** as it is clearly indicated under Recital 52 of the DMA: "*gatekeepers should therefore be obliged to ensure access under equal conditions to, and interoperability with the same operating system, hardware or software features that are available or used in the provision of any ancillary services by the gatekeeper*".

ii. When referring to **equal conditions, it must be clear <u>that these include conditions of economic technical, or any other nature</u>** (e.g. requests for access should not be made illusory by way of prolonged approval procedures, etc.). This is essential to guarantee that third parties can **make direct and stand-alone use of the relevant functionalities for the provision of ancillary services**, e.g. preventing the gatekeeper from imposing access through intermediate services that might imply costs or other frictions to the business user.

   Equal access also applies to remuneration which would be requested by the gatekeeper and is an essential element to ensure the effectiveness of the obligation under Art. 6(1)(f). It should therefore be specified that:

   a. Any remuneration paid to the gatekeeper relating to such access and interoperability shall be fair, reasonable, and non-discriminatory relative to the services of the gatekeeper;
   b. The remuneration is strictly cost based; and
   c. The costs are precisely determined.

iii. Access to the operating systems of the gatekeeper for other service providers should not be restricted to the ancillary services that the gatekeeper provides, but allow also other innovative ancillary services, e.g. e-receipt of the purchase or receipt of a product guarantee and should also cover those cases in which the

devices for contactless payments in stores, as it would appear that Apple Pay is the only mobile payment solution that may use such technology. This has been expressly echoed in Recital 52 of the Proposal.

gatekeeper does not provide the ancillary service directly but through a partnership agreement.

iv. We would suggest including a provision for **independent dispute resolving mechanism** when it comes to any issues that could arise with regards to equal access to infrastructure.

v. In Recital 52, we would recommend to include a reference to **biometric identity readers, including fingerprint or face recognition scanners,** to stress that access to these solutions and services must also occur under Art. 6(1)(f).

b) Article 6 (1) (h) – data portability

The risk in digital incumbents leveraging user data is particularly high in financial services, where the emergence of "data-opolies" may be incentivised by large potential for price discrimination and bundling or cross-subsidising with non-financial activities. The inclusion of an obligation to strengthen data portability from gatekeepers is therefore very welcome. Beyond facilitating switching, the new obligation can contribute "to the development of additional value-added services by third parties" who can access customers' data at their request, and with their consent[4] - something which, as the portability right currently standards under the GDPR, falls short of. Therefore, for personal data, the obligation under Article 6(h) would in effect **be an improved way for individuals to exercise their right to portability under Article 20 of the GDPR**. The proposal also rightly points out the need for gatekeepers to provide tools to users to help exercise these obligations, such as APIs. Currently, data controllers can "prevent a full exercise of users right to data portability if they prove that in a given situation the level of technological development of their organisation makes technical unfeasible[5]."

The EBF also welcomes that the obligation includes portability for business data. The proposal recognizes that an increasing number of firms depend on and transact through digital platforms, making the data stored in these platforms critical to business users. Enabling users to transfer their data from the original service provider to another firm would increase competition in and allow data to be reused across other sectors.

However, we **would suggest the following amendments to Article 6 (1) (h) to help realize opportunities for both end users and business users:**

i. To **state more clearly that both business users and end users can port their data, personal and non-personal, in real-time effectively, as is stated under Recital 54.** With the current wording, some misinterpretations could arise since the current text under Art. 6 (1) (h) only states that the gatekeepers shall "*provide tools for end users to facilitate the exercise of data portability, in line with Regulation EU 2016/679*". In this regard, it must be noted that business users and end-users that are legal persons are not granted any data portability right under GDPR, **so the current wording is insufficient to achieve the aim of Art.6 (1) (h).**

ii. To indicate that for personal data, the obligation under Art. 6(1)h would be an improved way to exercise the portability right afforded to them under the GDPR. Therefore, the aim of article 6 (1)(h) would be better achieved by indicating that

[4] Beslay, L, De Hert, Malgieri, G. P, Papakonstantinous, V & Sanchez, I (2018), "The Right to data portability in the GDPR: Towards user-centric interoperability of digital services", Computer Law and Security Review, p.195
[5] Ibid. p.201. This refers to portability for individuals, as per the GDPR.

the exercise of **data portability should be done in line with *and* building on Regulation EU 2016/679.**

iii. To clearly **require a standardised transfer mechanism** that would allow for easy, secure, real-time, and recurrent data transfers. **Application programming interfaces (APIs) would be an effective way to implement this, as noted under Recital 54.** Standardisation of the data formats and of the transfer mechanism, including security requirements, should be considered, **and can be developed under the frame of the Commission implementing act, for which Article 36 provides the possibility.** Other elements which the Commission could consider including in Level 2 rules include specifying the minimum set of data that each type of core platform service under Art 2 would need to ensure that effective portability is provided for.

iv. Interoperability is crucial, and the Commission should consider the investments and work already undertaken in different sectors with regards to data sharing, such as in the financial sector when developing Level 2 regulation.

v. Regarding security requirements, it should be possible for users to initiate the data transfer through the third party that will receive the data, while the liability for the authentication of users should rest with the gatekeeper holding the data (for this, users would be redirected to the gatekeeper's system).

vi. **The data in scope should be limited to the data provided and generated by users and not inferred data, elaborated by gatekeepers.** It is particularly important to clarify the concepts of **data "provided for", "generated in the context of", "generated through", "collected through", and "inferred from" and ensure their consistency throughout the proposal**.

We understand that the Proposal's spirit is to distinguish between, on the one hand, data "provided by" or "observed from" users and, on the other hand, data "inferred from" or "derived from" the data provided by or observed from users, along the lines of the guidelines of the European Data Protection Board (EDPB).[6] Inferred or derived data are distinguished by the fact that they are newly created by the processor of original data by inputting additional data, know how, intelligence or methods of analysis, which allow to extract new information that is not inherent in the original data, while provided or observed data are the raw ones or those subject to certain types of processing not involving prediction or inference (i.e. for verification or organisational purposes).

An obligation to share inferred data, if included in the proposal, could **entail a number of potential unintended consequences** such as the reduction of digital incumbents' incentives to innovate in methods of analysing data and moral hazard in the form of free riding by new entrants, which may also have less incentives to develop their own methods of analysis.

We therefore propose that the concept of inferred data is clearly delineated from any other types of data so that only the latter are subject to data access and portability obligations, while the former remains relevant only for the prohibition of unfair combination in Article 5(a) of the Proposal.

vii. Recital 54 notes that end users should be granted effective and immediate access to the data they provided or generated in their use of the service of the gatekeeper, and that this should apply **also to "*any other data at different levels of aggregation* *that may be necessary to effectively enable such portability*"**. We

[6] See Article 29 Data Protection Working Party, Guidelines on the right to data portability (wp242rev.01) of 27 October 2017, pp. 9-11 (available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233).

would recommend **clarifying what "any other data" means,** also taking into account the recommendation included above.

c) Article 6 (1) (i) – data access

Art. 6 (1) (i) obliges gatekeepers to provide business users, or third parties authorised by a business user, free of charge, with effective, high-quality, continuous, and real-time access and use of aggregated or non-aggregated data, that is provided for or generated in the context of the use of the relevant core platform services. The same obligation should apply with regards to data related to end users, or third parties authorised by end users, as in many cases end users have a direct contractual relationship with gatekeepers and not only via business users. This way the accumulated data held by gatekeeper platforms could also be made accessible to and transferable by end users not only for porting i.e. switching reasons, but also for granting access to third parties that can offer value added services on that basis to their customer and end user of the gatekeeper platform.

Article 6 (1) (i) should also clarify that gatekeepers shall put in place **appropriate technical measures to facilitate real time access to data**, in particular by putting in place high quality application programming interfaces, **as noted under Recital 55.** Like for Art. 6(1)(h), technical measures are key to make data access solutions effective to enable the proposal to achieve the desired effects of enabling competition and innovation[7].

d) Comments on other Article 5 and 6 obligations

i. **Article 5(a)** aims to ensure that gatekeepers do not combine personal data among their different services in cases where customers have not consented to such treatment. **It should be clarified that the provision is not to be understood as suggesting that platforms that are not designated as gatekeepers may freely combine personal data across services without the individual's consent**, as this obligation is already set in GDPR. This could be made clear by adding wording in recital 36. The DMA aims to ensure that consumers freely choose to opt-in by mandating gatekeepers to make available a "less personalized alternative", (as explained in Recital 36). In our view, this obligation is the only way to ensure that users genuinely consent the use of their data, without being forced to consent to a non-fair use of their data that they would not otherwise accept if they were not dependent on the gatekeeper's platform service. We would therefore recommend making explicit **in Art. 5(a) that gatekeepers shall offer this "less personalized alternative"**.

   Overall, it is important to unequivocally state that **consent must be provided in accordance with GDPR**, which requires that consent be explicit, free, specific informed and unambiguous. Referring only to some of these conditions in **different provisions of the DMA may create uncertainty regarding whether they are applicable only to such cases**. This may entail other adjustments across the Proposal such as the reference to the inherent condition of specificity in Article 5(a), which is superfluous and potentially misleading. The explicit and specific character of consent is already explained in Recital 36.

ii. Where **Article 5(d)** mandates gatekeepers to refrain from preventing or restricting business users from raising issues with any relevant public authority relating to any practice of gatekeepers, it should be made clear that the latter **shall neither be discouraged by means of contractual provisions.** It would also be helpful if

[7] Kerber, W. (2020), *From (Horizontal and Sectoral) Data Access Solutions towards Data Governance Systems,* Joint Discussion Paper Series in Economics, p.19

this Article provided that gatekeepers cannot enforce the terms and conditions for using their platforms in a way that forces business users to breach any legal obligations which may apply to them.

iii. We understand that **Article 5(f)** aims to prevent enveloping practices known as platform enveloping strategies, whereby the gatekeeper may force counterparts (business or end users) to make conditional the use of one of its core platform services upon the use of another of its core platform services. We think that DMA's goals related to fairness and market contestability will only be **served if the DMA clearly prohibits situations where the gatekeeper makes conditional the use of their core platform services upon the use of other of its non-core platform services**.

iv. **Article 6 (1) (a)** prevents gatekeepers from using data generated by business users and/or by the end users of the business users which are not publicly available. This article should also **provide that gatekeepers must not prevent (directly or indirectly) business users from collecting data from their end users use the gatekeeper's platform (provided that the business user has obtained users' consent according to privacy rules where relevant).**

In addition, the data that the gatekeeper should be prevented from availing of in its dual role under Article 6(1)(a) of the Proposal **should include data collected through ancillary services, which may also contribute to its ecosystem advantage.**

v. **Article 6 (1) (d)** prevents gatekeepers from treating more favourably their product/service offering in ranking services and forces them to apply FRAND conditions to such ranking. The wording of the Article should specify **that FRAND conditions applied to ranking shall include "display" as well.**

e) Mechanism for updating obligations

We welcome the possibility included in the Regulation for **the EC to adopt delegated acts to update the obligations under Articles 5 and 6.** This flexibility allows for addressing practices that are unfair and makes the framework stronger in order to ensure competitiveness in digital markets. **Provisions under Article 17** provide for the opportunity to **include future practices that** may limit the contestability of core platform services or may be unfair and which are not effectively addressed by the Regulation and to subsequently adopt a delegated act to amend Articles 5 and 6.

f) Compliance with obligations for gatekeepers

While the proposal is well targeted there is a risk that there is an emphasis on Art. 25 (non-compliance), leading to a situation where issues with the implementation are only flagged and reviewed as part of formal and potentially time-consuming processes i.e., when business or end-users encounter challenges to exercising, for example, effective data portability. This is particularly the case for **compliance with Article 6 and could lead to a de-facto delayed implementation of obligations by gatekeepers.**

Therefore, we do see merit in the possibility of further specification by the Commission as part of an ongoing supervisory dialogue, similar to the one known from the financial services sector. To reduce uncertainty for platforms, business users and end-users, help ensure that obligations are effectively implemented and ease the Commission's work in detailing compliance measures, **we recommend the Commission strengthens the instruments at its disposal.**

i. Enhancing Article 7

Article 7(7) indicates that a gatekeeper may request the opening of proceedings for the Commission to determine whether the measures that the gatekeeper intends to implement or has implemented under Article 6 are effective in achieving the objective of the relevant obligation in the specific circumstances. This paragraph should be amended to state that gatekeepers **would still need to comply with all relevant obligations under Art. 6, even while awaiting the Commission decision. This is to prevent an unintended misuse of this provision to delay the effective implementation of the DMA.**

Additionally, the procedure for specification under Art. 7 of the obligations under Art. 6 **may create uncertainty**. We would therefore recommend **several amendments to ensure that the regulatory dialogue** contemplated under Recital 33 **can be effective for the purposes of Article 7** of the Proposal. This could be achieved **by requesting gatekeepers to notify the Commission of the measures that it intends to implement to ensure compliance with the obligations laid down under Art. 6 at the moment, or within a short time frame, of its designation as a gatekeeper** (e.g. presentation of a compliance plan that indicates points such as a description of the technological means to meet data portability and data access obligations (e.g. description of the APIs, particularly until any Level 2 rules are adopted). This could then also constitute **the starting point for dialogue, while also serving as a tool for monitoring compliance with the rules.**

This practice, which is common in financial supervision, will inevitably lead to a regulatory dialogue which will facilitate compliance with the rule and supervisory tasks.

Where the possibility to proposed level 2 rules exists, these should take a core platform service approach, meaning that measures should be specified for each type of core platform service under Art. 2 whether social media platforms or operating systems. Implementing Act's should also be presented 6 months after the entry into force of the Regulation.

Once any Level 2 rules adopted, it is also important to apply lessons learned and make any improvements. For example, if the authorities see more categories of data that should be made available in a certain category of core platform services, also based on feedback from third parties (see below), additional guidance could be issued to the market. As time goes by and experience increases, Level 2 regulation can reduce the need for regulatory dialogue and increase certainty for all stakeholders, while still leaving the possibility for enhanced supervision and provide room for specificities if a gatekeeper needs it.

ii. Feedback from third parties

Third-party stakeholders may provide valuable insight and warn against potential risks in the measures proposed or implemented by gatekeepers or the remedies to be imposed by the Commission. We would therefore recommend to include a provision in the proposal to allow for this third-party feedback in proceedings under Chapter V, which should also provide **business users with the necessary means or channels to communicate the gatekeeper's non-compliance with these obligations to the EC** (beyond the typical competition tools). New provisions should be included to enable business users to communicate non-compliance, also to help ensure the Regulation's effectiveness. The possibility of requesting third-party feedback should not lead to an extension in the envisaged timeframes.

iii. Suspension and exemptions from obligations

On the one hand, we understand that the provisions under articles 8 and 9 of the proposal are aimed at ensuring proportionality. On the other hand, **we believe that more clarity**

is needed to ensure that the application of these provisions is exceptional and fully justified, and do not undermine the objectives of market contestability and fairness under the DMA.

In this regard, we would like to ask for clarification of the wording "the economic viability of the operation of the gatekeeper in the Union" under article 8.1, as this concept **can be interpreted in many different ways** (e.g. as a financial loss or as a mere reduction of profit) and be assessed on the basis of different legal entities (the core platform service provider or the undertaking). Moreover, when the Commission assesses the suspension request from a gatekeeper, it should consider not only the economic viability of the gatekeeper, but more prominently **the interests of business and end users, and whether the suspension might undermine the objectives of market contestability and fairness.** The same should apply when considering the application to the concept of overriding reasons of public interest' as contemplated under Art.9.

Finally, we also recommend to **include a specific provision to ensure that gatekeepers will not use the customer experience** to bias their choices to provide access to the data mentioned in Articles 6 (1) (h) and (i). **Article 11 (3) is currently not sufficient.**

4. Enforcement

Overall, **the framework of remedies applicable in a case-by-case basis in case of non-compliance, which can be behavioural or structural, is effective and sufficiently broad.** It allows the EC to intervene before competition problems arise due to repeated strategies by gatekeepers and will contribute to voiding fragmentation in regulatory approaches across the EU.

Moreover, remedies imposed ex-ante should minimize the harmful structural effects of unfair practices, without limiting the EU's ability to intervene ex-post via the enforcement of existing EU competition rules.

The Regulation however does not make reference to the involvement of different European Commission Directorate Generals (e.g. DG Competition, DG CONNECT) in the enforcement of the rules. **More clarity is needed as regards the governance framework within the Commission itself when it comes to the DMA.**

We also welcome **the creation of a Digital Markets Advisory Committee,** to be formed by representatives and experts from member states. Considering that many of the obligations imposed on gatekeepers are related to the access, use and sharing of data, including personal data, **appropriate coordination with national data protection authorities must be warranted.**

Finally, a clarification on **whether the obligations under Article 6 could be enforced by national courts** regardless of the prior decision of the Commission or if this provision is not self-executing would be helpful.

We would recommend to introduce in the text a clarification regarding the **coordination between the Commission and national courts** that will be called upon to apply the DMA, in **order to make more explicit what the Proposal already states in Art. 1 (7) paragraph 7.** This clarification should be based on the detailed provisions of Articles 15 and 16 of the Regulation 1/2003 on the implementation of the rules on competition laid down in Article 81 and 82 of the Treaty[8].

[8] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (Text with EEA relevance)

ENDS

For more information:
Liga Semane
Policy Adviser – Data & Innovation
l.semane@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu