ASSOCIATION OF COMMERCIAL TELEVISION IN EUROPE

POSITION PAPER ON THE DIGITAL MARKETS ACT

EC PROPOSAL FOR A REGULATION ON A SINGLE MARKET FOR DIGITAL SERVICES

MEMBERS & PURPOSE - ASSOCIATION OF COMMERCIAL TELEVISION IN EUROPE (ACT)

ACT member companies finance, produce, promote and distribute content and services benefiting millions of Europeans across all platforms. At ACT we believe that the healthy and sustainable commercial broadcasting sector has an important role to play in Europe's economy, society and cultures. Commercial broadcasters are at the heart of Europe's media landscape as producers and distributors of European original content and news. We embrace the digital environment providing new services, formats and content to meet the growing European demand for quality content on various distribution models.

FACTS & FIGURES – TV IN EUROPE (ACT)

INITIAL REMARKS

GROWING DEPENDENCY ON DIGITAL GATEKEEPERS

As producers and distributors of original European content and news, commercial broadcasters form a central pillar of Europe's diverse media landscape. From the very beginning, ACT's members have embraced the increasing use of digital platforms to access content and supported such increasing demand with new services, formats and content tailored to the needs of a growing European online audience. In this process, it has become increasingly clear that some online markets suffer from fundamental structural imbalances, primarily created by a small number of digital platforms that are determining how most Europeans obtain and consume news, information and audio-visual content online.

We share the concerns identified in the Commission's Impact Assessment and outlined in the Explanatory Memorandum of the DMA regarding the unfair trading practices of digital gatekeepers. In particular, we agree that, due to structural problems, competition law is not sufficient in addressing the challenges posed by the largest online platforms acting as Gatekeepers, and that therefore additional obligations are required. Considering the entrenched market positions of such Gatekeepers, the DMA is a long overdue, and possibly the last opportunity to gain back some control over the digital infrastructure and to ensure fair and contestable markets.

By controlling walled-off ecosystems, Gatekeeper services have become largely incontestable while controlling access to large user groups. Such control provides a strong commercial incentive and ability to unfairly extract rents from content providers and other business users that have become dependent on gatekeepers in their effort to reach online audiences. This is particularly striking for Gatekeepers that, like content providers, are funded by advertising and therefore have a strong conflict of interest when intermediating competitors in this area. As a result, today even the largest European broadcasters are faced with a situation where digital gatekeepers with conflicting business interests in effect unilaterally determine the commercial conditions for user access to audio-visual content, and thereby both hinder and exploit broadcasters in their endeavours to fund and provide innovative high-quality services.

WELCOMING THE DMA & CENTRAL RECOMMENDATIONS

ACT welcomes the proposal for a Digital Markets Act (DMA), as it addresses some of the most fundamental shortcomings in the current regulatory framework. For innovation to thrive in the digital economy, including in the media sector, there must be open and fair access to online audiences and corresponding revenue streams. Combined with the equally relevant liability regime for very large platforms proposed under the Digital Services Act (DSA), the DMA envisages practical solutions for genuine and urgent business restraints faced by various industries and companies in the digital sphere.

In order to further enhance the effectiveness of the DMA, ACT's recommendations focus on three key points: (i) a narrow set of designated Gatekeepers, (ii) more extensive obligations, and; (iii) less time-consuming and more effective enforcement mechanisms. The basic requirement for an effective asymmetric regulation is a targeted but all the more effective and speedy prohibition of the harmful practices of incontestable gatekeepers, while simultaneously preventing negative spill-over effects for contestable competitors and intermediaries that do not threaten the competitive process.

In summary, we would suggest focusing the application of the DMA to a very narrow set of Gatekeepers along with tightening the requirements for such players by introducing more effective obligations and enforcement tools.

EXECUTIVE OUTLINE OF KEY AREAS COVERED

CHAPTER I: Subject matter, scope, definitions

CHAPTER I – Subject matter, scope, definitions

- ACT members are concerned that, in the medium-term to long-term, the effectiveness of the DMA will significantly suffer, its purpose will be diluted and its merits will be reduced if the group of addressed "Gatekeepers" is defined too broadly.
- Providers of broadcasting services are not in the position of constituting gatekeepers ; however we see the risk, , that digital gatekeepers would seek to expand their dominance into broadcasting markets. We have already witnessed digital gatekeepers moving into linear broadcasting as well as first attempts to use their platforms to unfairly 'squeeze' themselves in between main-TV audiences and broadcasters with a view to becoming new intermediaries for broadcast channels, Voice-on-Demand services or other TV content. To ensure that such practices are covered, the DMA should not address any of the broadcasting services, unless they are provided by a Gatekeeper identified pursuant to Article 3(7). This would be comparable to the approach taken to advertising services, which, according to Article 2(2)(g), constitute a core platform service only if they are "provided by a provider of any of the core platform services listed in points (a) to (g)".
- Web browsers should be included in the list of core platforms services and the concept of "search results" should be further defined to ensure it covers operating systems for any "smart:": (i.e. internet connected) TVs.
- ACT would suggest increasing legal certainty by clarifying that the term "operating system" as defined in Article 2(10), applies to the extent that operators are designated as Gatekeepers (e.g. in Search, marketplaces…), so that rules of Articles 5 & 6 cover all activities where they control access to online audiences – including in content intermediation.

CHAPTER II- Designation of gatekeepers

Chapter II – designation of gatekeepers

- ACT believes that if the DMA targets a group of platform services that is too broad - or that could be quickly broadened over time - the material obligations may be diluted and the enforcement may be slowed down, without additional benefits.

Material criteria

- The central qualitative criteria in Article 3(1) would benefit from clarification, especially given the that the additional criteria in Article 3(6) do not provide sufficient guidance on material thresholds;
- The central quantitative criteria such as market capitalisation and number of monthly active users are sufficiently precise to provide for a speedier designation process rather than taking the much lengthier route of conducting a complex analysis of multi-sided markets.

Delegated acts to specify criteria

- Given the potential implication of the designation process, the criteria used should be clearer and more transparent.
- Instead of a delegated act that directly broadens the scope of gatekeepers, the Commission should limit itself to a legislative proposal to amend the Regulation in order to include the identified additional criteria in the list of Article 2(6) DMA-A, only after the need for review is signalled by EU jurisprudence.

Procedure for designating Gatekeepers

- Keeping the scope of the Gatekeepers narrow, instead of relying on delegated acts, will speed the designation process.
- It is essential that the obligations laid down in Articles 5 and 6 are implemented as soon as possible, therefore the obligations need to be applicable immediately after the designation.
- If a designated gatekeeper believes that it does not fulfil the thresholds, it should be entitled to request a market investigation in accordance with the relevant provisions of the Regulation. Such request and any following market investigation shall not affect the obligation pursuant to Article 3(8) for a gatekeeper to comply with the obligations laid down in Articles 5 and 6 within a certain number (currently six, more appropriately three) months after its core platform service has been included in the list pursuant to Article 3(7). The Gatekeeper may, however, turn to the General Court to apply for a suspension of the Commission's designation decision. In such summary proceeding, the Gatekeeper shall bear the burden of proof and, if unsuccessful, all costs caused. This would reflect the statutory presumption in Article 3(2) and reduce the risk that companies only challenge designation decisions with a view to delaying the due process.
- While due process remains essential, co-legislators need to ensure that the process does not lead to significant delays, similar to the classic competition cases.

CHAPTER III- PROHIBITTED PRACTICES

2. 1. ARTICLE 5 - OBLIGATIONS FOR GATEKEEPERS INSUSCEPTIBLE OF BEING FURTHER SPECIFIED

2.1.1. Article 5 (a) – opt-in for personal data combination

- Article 5 (a) prohibits the bundling of data from various sources only if the user does not consent to such combination in the sense of an opt-in. When dealing with Gatekeepers, a solution which relies on consent would empty the obligation of substance.
- Combining personal data should be based upon an end user's explicit request to combine data in order to obtain a significantly improved service.
- However there must be a high hurdle for combining such data. This could be based upon an end user's explicit request to combine data in order to obtain a significantly improved service. In such a case, the provider should bear the burden of proof that the combination of data indeed (i) improves the service; (ii) allows the end user a fair share of the resulting benefits; (iii) is indispensable for such improvement, and; (iv) does not eliminate competition[1]. Moreover, in order to ensure that the Gatekeeper remains contestable, the end user's consent should only justify the Gatekeeper's combination of data if the consent is equally given to the business users involved in the intermediation pursuant to Article 6 (1) (i).

2.1.2. Article 5 (b) prohibition of parity clauses

- Article 5 (b) contains an important prohibition for broadcasters, for instance where a Gatekeeper does not allow a broadcaster to offer end users better conditions on different content platforms. The current version is limited to the offering of better conditions on other intermediation services (a broad most-favoured nation clause).
- The prohibition should be expanded to disallowing better conditions through the business users directly (a narrow most-favoured nation clause).

2.1.3. Article 5(d) prohibition of contact with enforcement institutions

- Article 5 (d) should be expanded to also cover conduct that would serve to penalise business users for enforcing the DMA before national courts. This is necessary because the DMA and the DSA distinguish between "authorities" and "courts".

2.1.4. Article 5 (e) – requiring business users to use ID service (and other ancillary services)

- Economists have recommended that tying and bunding practices be presumed anti-competitive and that a general ban be included in the list of Article 6 DMA-A[2]. ACT would support such an approach.
- There is no apparent reason as to why a Gatekeeper should be prohibited from bundling its core platform service with an identification service but allowed to bundle it with another ancillary services. In line with the uniform treatment elsewhere in the DMA, Article 5 (e) should pursue a uniform approach to all types of ancillary services.

2.1.5. Article 5 (f) – prohibition of making access to CPS conditional on use of other service

- To prevent leveraging, prohibiting the tying of one Gatekeeper service with another Gatekeeper service is insufficient, especially while permitting the making of the use of a Gatekeeper service dependent on the use of another service for which the undertaking does not yet enjoy a Gatekeeper position.

---

1 This method of justification is based upon the well-established principles and case law developed under Article 101 para. 3 TFEU, which ensures legal certainty.

2 *Cabral/Haucap/Parker/Petropoulus/Valletti,Van Alstyne*, The EU Digital Markets Act: A Report from a Panel of Economic Experts, 2021, p. 13.

- Should the tying prohibition be limited to bundling two Gatekeeper services together, the prohibition would come too late, because the markets would have already likely tipped and the users would have become dependent on both services in any event.
- The prohibition foreseen should also cover cases of a mixed bundling, often referred to as multi-product rebates. While in the case of a 'pure' bundling the products are only sold jointly in fixed proportions, in the case of mixed bundling, the products are also made available separately, but the sum of the prices when sold separately is higher than the bundled price.
- The Commission's "Guidance on the [..] enforcement priorities in applying Article [102] TFEU to abusive exclusionary conduct" treats pure and mixed bundling equally. Accordingly, a multi-product rebate is seen as abuse of dominance, "if it is so large that equally efficient competitors offering only some of the components cannot compete against the discounted bundled". The DMA should follow the same holistic approach.

2.1.6 Article 5 (g) – price transparency in advertising intermediation

- ACT members are frequently faced with restraints caused by the highly concentrated online advertising markets. Even for the largest media companies, the advertising environment is highly opaque, given the discretionary activities/opaqueness of Gatekeepers. The latter can use their entrenched position to impose their Terms & Conditions to limit the disclosure of information on costs, effectiveness and profits of ad placements.
- Regulation must neutralise the competitive advantages resulting from the unhindered vertical integration and bundling of relevant bidding data.
- One way to achieve this objective is to prohibit a Gatekeeper from using data that is relevant for advertising purposes and that was collected via one advertising service (e.g., an SSP) in another advertising service, with the objective of gaining a competitive advantage vis-à-vis competing bidders. Such use of data that the intermediary could only obtain from another intermediation service of the same undertaking should be considered to be unlawful "insider bidding" and prohibited - akin to insider trading in the financial sector.
- To be able to assess whether a Gatekeeper with an entrenched position has calculated a price fairly and reasonably, a business user needs to know which criteria and which calculation methodology the Gatekeeper used, in particular as regards any biddings in algorithmic auction processes.

2.2. OBLIGATIONS FOR GATEKEEPERS SUSCEPTIBLE OF BEING FURTHER SPECIFIED

2.2.1. Article 6 (1) (a) – prohibition of using non-public data generated by competing business users

- To enhance the effectiveness of the prohibition, the wording in Article 6.1.a. should be aligned with that of Article 6 (1) (i) as regards the type of data that may not be used. It is also to be read in connection with Article 6 (1) (e) which refers to the provision of broadcasters' data by Gatekeepers.
- It should also be clarified that the prohibition also applies where the Gatekeeper uses the data of one business user ("A") to compete not against such particular user, but with another business user ("B") as in both cases competition is unfairly distorted.

2.2.2. Article 6 (1) (b) – app un-installing

- Article 6 (1) (b) amounts to legalising one of the most extreme forms of self-preferencing.
- Currently, Article 6 (1) (b) only obliges Gatekeepers to allow end users to un-install any pre-installed apps. It does not prohibit such pre-installations in the first place. Gatekeepers are not obliged to actively provide a choice to end users. Due to the strong "status quo bias", it is very unlikely that end

users will switch and make well-informed choices if such choices are not presented and explained to them in the first place. This was a key learning from the Commission's Android case.
- The unjustified pre-installation of other core platform services such as a video-sharing platforms, social networks or web browsers by the provider of an operating system can have equivalent effects and should be addressed in the DMA proposal.
- End users should be able to un-install any functionality on a device, irrespective of its technical labelling, as long as this does not jeopardise the security or other functionalities. The Gatekeeper should bear the burden of proof that such risks exist.

2.2.3. Article 6 (1) (c) – enabling of side-loading

- In order to align the obligation with Article 6 (1) (d), this Article should also be expanded to the installation of any competing service, such as video-streaming services and not only with app stores and apps.

2.2.4. Article 6 (1) (d) - prohibition of self-favouring in ranking

- The intermediation power of Gatekeepers could allow them to determine the "winners and losers" on any interface they control and in any market that they intermediate. Accordingly, a strict ban on the unjustified preferencing of own services or those of partners is an indispensable precondition for a well-functioning internal market.
- Self-preferencing by any other core platform service such as operating systems, cloud computing services, advertising systems or ancillary services should be equally addressed.
- In addition, the current wording of the proposal does not address other equally damaging self-preferencing practices such as a preferential crawling, indexing or other "access" of offerings/content to the intermediation service, preferential sharing of data regarding the ranking criteria and how to influence them.
- The complex algorithmic and data-driven ranking of the various types of results in search engines, app stores or marketplaces can only be effectively monitored by a highly specialised and sufficiently equipped enforcement unit, ideally on a day-to-day basis. This is a standard that should be achieved.

2.2.5. Article 6(1)(e) – prohibition of restricting user switching

- To maintain contestability, every provider of a gatekeeper service should be prohibited from technically restricting the ability of end users to switch between services and subscribe to any other service. For example, search engines and social networks should not make it technically more difficult for advertisers to switch to alternative advertising networks in order to serve ads on their platforms or elsewhere.

2.2.6 – Article 6 (1) (f) – access to operating system and other features

- Such leveraging practices should be prohibited, however, not just if any "ancillary service" is favoured, as (narrowly) defined in Article 2(14). The favouring of any of the Gatekeeper's separate services should be equally addressed.

2.2.7. Article 6(1)(g) – transparency in advertising intermediation (performance)

- Article 6 (1) (g) can be seen as a special application of the general obligation under Article 6 (1) (i) (to share data relating to business users) for the advertising industry.

- Access to the relevant ad performance raw data must be provided in an "effective, high-quality, continuous and real-time" manner.
- While it is important that publishers and advertisers may verify the service of the Gatekeeper, it is equally important that they are enabled to measure, on an individual basis, the performance of their own campaigns and to use independent Joint Industry Committees.

2.2.8. Article 6(1)(h) – provision of data portability

- The wording of this obligation should be aligned with that of Article 6 (1) (i), and it should be ensured that the obligation may not be relied upon by one Gatekeeper to gain access to the data of another Gatekeeper.

2.2.9. Article 6 (1) (i) – access to data generated by intermediating between end users and business users

- Data provides broadcasters and other providers of digital services with important insights on how audiences consume and engage with content. Such insights allow to better cater to the interests of all user groups and thereby improve the quality of digital services.
- At present, when distributing content through Gatekeeper platforms, broadcasters often fail to enhance the positive network effects of their services, as Gatekeepers decline to share with them the data allowing them to better fine-tune the offerings to the needs of all users. In particular,Gatekeepers typically refuse to share any data regarding the number of views or any interactions of end users with relevant content.
- In order to use the Gatekeeper services to reach their respective (single-homing) audiences, broadcasters need to make their data available to the Gatekeeper and to accept its conditions as regards the free combination and use of such data.
- To make matters worse, in order to enhance their superior access to data, Gatekeepers increasingly use privacy laws as an excuse to further deprive business users and competing operators of relevant data. While, given end users' dependency on Gatekeeper services, the providers of such service find it easy to collect and bundle data in a GDPR-compliant manner, they reject sharing such data with business users on the basis of alleged GDPR-non-compliance.
- Gatekeepers are in a unique position to facilitate the obtaining of consent. Where a user accesses a third-party service through a Gatekeeper platform, the platform is used to facilitate obtaining consent for both the use of data by itself and the third-party service. The Gatekeeper cannot restrict obtaining consent for its purposes alone.
- The DMA could provide for a balance of interests by adopting a principle based approach - wherever the Gatekeeper fails to obtain consent from end users to share personal data that has been generated in the context of the use of the core platform service with the intermediated business user pursuant to Article 6 (1) (i)), the Gatekeeper should be prohibited from using such data for any purpose other than the original intermediation.
- In particular, a Gatekeeper must not be allowed to combine the data with any data gathered from other sources or use it for the provision of another service. In other words, if the Gatekeeper does not obtain consent from end users to share their data with its business users, the Gatekeeper must also not use this data itself.

2.2.10 – Article 6 (1) (j) – access to search data

- The obligation for Gatekeeper online search engines to grant FRAND-access to relevant search data eliminates the central barrier to entry for online search services and thereby renders the market for general search services contestable.

2.2.11 – Article 6 (1) (k) – prohibition of unfair access conditions

- ACT believes that the most coherent and consistent solution would be to expand the prohibition of unfair (unreasonable) and discriminatory conditions to all designated Gatekeepers.
- There is no justification to allow any Gatekeeper to impose unfair and/or discriminatory T&Cs.

3. Article 7 - compliance with obligations laid down in Article 5 and 6

- ACT would recommend that the co-legislators clarify that all obligations are immediately applicable without any room for delay which may be triggered by the Gatekeeper by means of an *a priori* dialogue between the Commission and the designated Gatekeepers.

CHAPTER IV - MONITORING AND ENFORCEMENT

- Previous competition cases involving digital Gatekeepers demonstrate the high degree of information asymmetry between Gatekeepers and enforcement authorities. To reduce such asymmetry authorities must be equipped with powerful tools to create the transparency and technical know-how necessary to detect and effectively condemn acts of non-compliance.
- The DMA needs to include a clear commitment to the private enforceability of the obligations laid down in Articles 5 and 6 before national courts.
- Currently, the DMA conveys no rights to affected business users, end users or competitors to request any investigation into any observed non-compliance, which is regrettable.
- It should be clarified that business users affected by any conduct of a Gatekeeper have the right to submit formal complaints about Gatekeepers' non-compliance with the obligations laid down in Article 5 and 6 of the DMA proposal. They should also be heard in the decision-making process of the enforcement authorities.
- We also remain cautious with regards to the potential implication of association of undertakings representing Gatekeepers in this process, given the targeted nature of the Regulation.

CHAPTER I: SUBJECT MATTER, SCOPE & DEFINITIONS

Not least due to the broad interpretation of the term "*online intermediation service*", the definition of "*core platform service*" in Article 2 para 2 DMA-P is in some respect extremely broad. According to the Impact Assessment of the Platform-to-Business regulation, amongst the 10,000 online platforms that operate in Europe[3], there are more than 7,000 platforms that would qualify as an "*online intermediation service*"[4]. As such, it is our understanding that, instead of providing the decisive threshold for a "gatekeeper", the definition of a "core platform service" only serves as a rough filter to narrow down the digital services that may potentially be subject to a regulatory obligation pursuant to Article 5 and 6 DMA-P[5].

---

[3] DMA-Proposal, Explanatory Memorandum, p. 1.

[4] Impact Assessment of the Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services.

[5] According to Article 5 and 6, a gatekeeper shall apply the listed obligations "*in respect of each of its core platform services identified pursuant to Article 3(7)*". According to Article 3(7) this list shall include all "*relevant core platform*

We would suggest that this rough filter would benefit from some fine-tuning.

In principle, providers of broadcasting services appear incapable of constituting gatekeepers, we see the risk, however, that digital gatekeepers seek to expand their dominance into broadcasting markets. We have already witnessed digital gatekeepers moving into linear broadcasting as well as first attempts to use their platforms to unfairly 'squeeze' themselves in between main-TV audiences and broadcasters with a view to becoming new intermediaries for broadcast channels, Voice-on-Demand services or other TV content. To ensure that such practices are covered, the DMA should not address any of the broadcasting services, unless they are provided by a Gatekeeper identified pursuant to Article 3(7). This would be comparable to the approach taken to advertising services, which, according to Article 2(2)(g), constitute a core platform service only if they are "*provided by a provider of any of the core platform services listed in points (a) to (g)*".

We would also recommend **adding web browsers to the list of core platform services**. In its *Android* Decision, the Commission distinguished between "web browsers" and "operating systems"[6]. Given the lack of a direct intermediation between consumers and business users, web browsers likewise do not quality as "online intermediation service". However, there is an apparent need to cover web browsers. Google's Chrome web browser has a market share above 60% in Europe. The service forms a central part of Google's ecosystem. By determining the conditions for consumers' access to websites, web browsers fulfil traditional gatekeeper intermediation functionalities. The current investigation of the CMA into Google Chrome's "Privacy Sandbox"[7] illustrates the significance of subjecting web browsers to regulatory oversight. The definition of web browsers can be based upon that used in the EC's *Android* case[8] (see below).

While we read the definition of an "operating system" in Article 2 (10) DMA-E as covering software systems which control the basic functions of *any* hardware, legal certainty could be increased by clarifying in (in a recital) that this also includes **operating systems for any 'smart' (internet-connected) TVs**.

In addition, we also recommend **defining the term "search results"**. For ACT members the obligation under Article 6 (1) (d) DMA-A "*to refrain from treating more favourably in ranking services and products offered by the gatekeeper itself*" is very important. Article 2 (18) DMA-A defines the term "*ranking*" as any "*relevance given to search results by online search engines*". The term "*search results*" is not defined. Considering the creativity of gatekeepers in evading obligations, this gives rise to unnecessary leeway to circumvent the obligation.[9]

Article #	Proposed Regulation, suggested deletion (~~strike through~~) and new insertions
Article 2(2)	For the purpose of this Regulation, the following definitions apply: (1)… (2) 'Core platform service' means any of the following:

services that are provided within that same undertaking and which individually serve as an important gateway for business users to reach end users as referred to in paragraph 1(b)". Hence, once any service of an undertaking fulfils the criteria under Article 3 para. 1 DMA-E, all other core platform services of this undertaking are also subject to the obligations pursuant to Article 5 and 6, provided they themselves are an important gateway.

6 Case AT.4099, 18/7/2018, section 5.2. vs section 5.7 – *Google Android.*

7 See CMA, Press release, 8/01/2021, CMA to investigate Google's 'Privacy Sandbox' browser changes, https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes

8 See definition at section 5.7 Case AT.4099, 18/7/2018 – *Google Android*.

9 For example, in the German competition case of *NetDoktor*, Google argued that placing a separate box with own offerings above all remaining "ranked" search results, i.e. at a fixed "position zero", would not constitute self-preferencing, because such box would not be part of the search results. See LG München I, 10 February 2021, 37 0 15721/20 – *NetDoktor/Google*.

	(a) online intermediation services; (h) web browsers; (10) 'Operating system' means a system software which controls the basic functions of any ~~the~~ hardware that is capable of being connected to the Internet or software that enables software applications to run on it, including for static and mobile devices, televisions or wearables. (18x) 'Search result' means any information presented in any format, including texts, graphics, videos, voice or other output, returned in response and related to any written, oral or equivalent search query, irrespective of whether the information constitutes an organic result, a paid result, a direct answer or any product, service or information offered in connection with, or displayed along with, or partly or entirely embedded in the results interface. (x) 'web browser' means a software used by users of client PCs, smart mobile devices or other devices to access and interact with web content hosted on servers that are connected to networks such as the Internet, including standalone web browsers as well as web browsers integrated or embedded in other services.

CHAPTER II – DESIGNATION OF GATEKEEPERS

We are concerned that, if the DMA targets a group of platform services that is too broad - or that could be quickly broadened over time - the material obligations may be diluted and the enforcement may be slowed down, without additional benefits. There is an important correlation between the threshold for regulating a service and the intensity of such regulation. An effective control of the immense powers of genuine Gatekeepers to structure today's digital economy requires intensive oversight. Instead of considering any expansion of the scope of the DMA, we would therefore recommend clarifying and narrowing down the threshold for a gatekeeper.

Material criteria

As mentioned above, ACT members are very concerned that, in the medium-term to long-term, the effectiveness of the DMA will significantly suffer, its purpose will be diluted and its merits will be reduced if the group of addressed "Gatekeepers" is defined too broadly. The DMA's declared purpose is to address the market power of "*a few large platforms*" that "*represent key structuring elements of today's digital economy*" because they "*act as gateways or gatekeepers between business users and end users and enjoy an entrenched and durable position, often as a result of the creation of conglomerate ecosystems around their core platform services, which reinforces existing entry barriers*"[10]. According to recital (2) such power typically rests upon a combination of "*extreme scale economies*", "*very strong network effects*" and a "*significant degree of dependence of both business users and end users, lock-in effects, a lack of multi-homing [..] vertical integration, and data-driven advantages*". According to recital (3), the DMA therefore focuses on "*a small number of large platforms*" that "*are structurally extremely difficult to challenge or contest by existing or new market operators, irrespective of how innovative and efficient these may be*".

We fully welcome this focus on nearly incontestable, structuring platforms. Considering the significant implications that a gatekeeper status has for a company, the criteria should be as clear and transparent as possible. Legal clarity for the designation will also likely (i) limit the ability of undertakings to misuse the option under Article 3 (4) to present substantiated counterarguments, (ii) reduce the overall number of designation

[10] DMA-Proposal, Explanatory Memorandum, p. 1.

proceedings, (ii) speed up such (remaining) proceedings and limit the administrative discretion in such proceedings. All of this will free capacities for the authority to focus on the crucial enforcement of the DMA, in particular during the decisive first years (where a high number of undertakings needs to be assessed). Against this background, we would recommend to further fine-tune the material criteria for designating a Gatekeeper in Article 3 DMA-P to better reflect the envisaged effective focus on structuring platforms.

In particular, the qualitative criteria in Article 3 (1) DMA-A would benefit from a clarification of the terms "*significant impact*" and "*important gateway*". The additional criteria in Article 3 (6) DMA-A do not appear to provide sufficient guidance as they do not contain material thresholds but list possible aspects that the authority may or may not consider. It should be prevented that the broadly-defined criteria may be used to highlight a particular strength of an overly large number of online platforms to designate them as Gatekeepers.

Ultimately, the only precise thresholds are the quantitative criteria in Article 3 (2) DMA-A. We understand that relying on measurable figures of turnover, market capitalisation and number of monthly users facilitates and speeds up the designation process, as compared to a complex analysis of the multi-sided markets. Therefore, overall we do welcome this approach. To avoid overregulation of competitive markets, a further criterion could be added to reflect the relative size of a provider of a platforms services vis-à-vis other providers of such service. In contrast to the (definition of the) affected markets, the core platform services for which a gatekeeper position may only be designated, are pre-defined in Article 2 (2) DMA. Any company as well as the enforcement authority need to assess whether a given service falls under any such definition. Accordingly, a criterion that refers to the relative size of a provider of such service (in terms of its revenues, capitalisation or number of users) would not necessarily have to add further complexity[11]. This is the case, certainly, for services in Article 2 (2) (b)-(g).

Delegated act to specify criteria

The need to have clear statutory requirements should also be seen against the background of the envisaged power of the Commission "*to adopt delegated acts [..] to specify the methodology for determining whether the quantitative thresholds laid down in paragraph 1 are met, and to regularly adjust it to market and technological developments where necessary*" (Article 2(5)).

Such power may frustrate the DMA's overall approach to address only large platforms that "*have emerged benefitting from characteristics of the sector such as strong network effects, often embedded in their own platform ecosystems*" and that "*represent key structuring elements of today's digital economy*." By definition, even in fast moving markets, such positions cannot be achieved in a short period of time. It takes years to develop any ecosystem. The DMA is to be revised "*every three years*" in any event (Article 38). It is difficult to see how any company could establish a Gatekeeper position in a shorter period of time, which would necessitate the Commission to adjust the Gatekeeper criteria in Article 2.

The objective should be that the final criteria of Article 2 do not necessitate any adjustment, at least not within the first three years of the DMA's existence. Instead of a delegated act that directly broadens the scope of gatekeepers, the Commission should limit itself to a proposal to amend the Regulation in order to include the identified additional criteria in the list of Article 2(6) DMA-A. Such mechanism is already envisaged for any Commission proposals to include new services in the list of core platform services, see Article 17 lit. (a).

[11] The services in Article 2 (2) (b)-(g) would allow a direct comparison. The term "online intermediation service", however, is too broad for a relative comparison. There are too many different types of online intermediation services. To add a relative criterion (relating to the relative size within a category of a core platform service) the types of online intermediation services would need to be further distinguished.

Procedure for designating Gatekeepers

Keeping the scope of Gatekeepers narrow in the DMA (rather than relying on any delegated acts) will also help speed up the designation process, in particular for those services that are genuinely incontestable.

To prevent irreversible harm to competition, ACT members consider it essential that the obligations laid down in Article 5 and 6 are implemented effectively and comprehensively as soon as possible. To be faster than competition law enforcement is one of the DMA's core objectives[12]. It is important that procedural rights are granted and a due legal proceeding pursued. However, this must not be one-sided. Due to the options for a suspension or exemption in Article 8 and 9 DMA, the economic viability of a gatekeeper is not at stake if it has to adhere to any obligation laid down in Articles 5 and 6 a few months earlier. In contrast, (even) such short period of time may suffice to endanger the economic viability of the many dependent business users faced with such practices. Their interests must also be considered when setting timelines. Accordingly, the interest in legal robustness and a due proceeding must be duly balanced with the interest in speed resulting from the detrimental effects of the condemned practices on potentially thousands of affected business users.

A central component of this balancing and a conceptual strength of the DMA is the concept that a Gatekeeper must comply with the obligations laid down in Articles 5 and 6 automatically (within six months) after it has been identified as a Gatekeeper (Article 3(7)-(8)). Such approach appears more effective than a solution where a competition authority first has to "activate" any obligation by issuing a corresponding individual decision[13]. The DMA concept is particular coherent given that the Regulation contains "*a narrow set of very precise unfair practices*"[14] which mostly derive from established competition law cases. This focus increases legal certainty and renders lengthy case-by-case analysis. Accordingly, for the DMA, any need of a regulatory 'activation' of any obligation would be particularly odd.

However, the advantages of the envisaged automatic applicability of the obligations under Article 5 and 6 are at risk. There are several loopholes in the envisaged close timeline for the process of identifying Gatekeepers

[12] DMA-Proposal, Explanatory Memorandum, p. 3-4.

[13] This is a central weakness, for instance, of the German Section 19a for companies with paramount significance for competition across markets, see *Hoppne*r, Plattform-Regulierung light: Zum Konzept der Unternehmen mit überragender marktübergreifender Bedeutung in der 10. GWB-Novelle, WuW 2020, 71-79.

[14] DMA-P, Annex Legislative Financial Statements, p. 61.

and monitoring compliance[15]. In addition, some proposed time periods appear disproportionately long[16], while the limitation periods for imposing fines or periodic penalty payments are surprisingly short[17].

Most significantly, however, the current design of the rebuttal opportunity under Article 3(4) DMA-A risks undermining all of the expected advantages of a quasi-automatic applicability of Article 5 and 6. According to Article 3(4), providers that fulfil the quantitative criteria in Article 3(2) may "*present sufficiently substantiated arguments to demonstrate that they do not satisfy the requirements of Article 3 (1) DMA-A*". For several reasons[18], it is nearly inevitable, that within their three months period to notify the Commission, even the largest global providers of core platform services will make such demonstration. If they do, the obligations laid down in Articles 5 and 6 DMA-A only become binding on such providers after the Commission has carried out a market investigation pursuant to Article 15 (3) and 3(6)) DMA-A. This will take time. The Commission has 60 days to determine whether "*sufficiently substantiated arguments*" have been presented. At that point, there is no time limit for the Commission to decide whether it will initiate a market investigation pursuant to Article 2(6) DMA-A (or if at all)[19]. Even once it has decided to do so, it "*shall endeavour*" only to conclude such investigation within a further five months. The Gatekeeper then has another six months to comply. By then, even the largest Gatekeeper will have gained (at least) *sixteen* months[20] of non-compliance without any

---

15 (i) Where the gatekeeper presents sufficiently substantiated arguments pursuant to Article 2(4), the Commission "*shall apply paragraph 6*". Yet, there is no time limit for the Commission to decide whether or not, based upon paragraph 6, it will launch an investigation in accordance with Article 15. While the Commission "*shall endeavour*" to conclude such investigation within five months (Article 15(3), it could in theory first wait many months before opening such investigation. (ii) Similarly, while Article 15 contains periods for concluding a market investigation, it contains no timeline for the Commission's decision as to whether to open such investigation in the first place. (iii) According to Article 7(2), if the Commission finds that measures of a gatekeeper do not ensure effective compliance with Article 6, the Commission "*may specify the measures that the gatekeeper concerned shall implement*". The Commission "*shall adopt [a] decision within six months from the opening of proceedings pursuant to Article 18*". However, there is no time limit for the Commission's assessment as to whether there is non-compliance and whether to open such proceedings in the first place – this could, in theory, take years. There are likewise no time periods for (iv) the Commission's identification of the relevant undertaking to which a gatekeeper belongs and its listing of core platform services belonging to such undertaking pursuant to Article 3(7); (v) the Commission's decision as to whether to launch a market investigation into systemic non-compliance pursuant Article 16; (vi) the decision to open proceedings pursuant to Article 16 for decisions in accordance with Article 7, 25 or 26; (vii) the decision to assess interim measures and the corresponding proceeding pursuant to Article 22. In competition cases the Commission has often taken more time deciding whether to open an investigation than it took for it to conclude such investigation. In particular the lack of a deadline for a non-compliance finding in Article 25 weighs heavy.

16 In particular: (i) 3 months for gatekeepers to notify the Commission (Article 2(3)); (ii) 6 months for gatekeepers to comply with obligations (Article 3(8)); (iii) 12 months for designating a gatekeeper (Article 15 (1); (iv) 24 months for a market investigation into new services and new practices (Article 17 (1)).

17 Article 28 DMA-E limits the powers of the Commission to impose fines or periodic penalties to a three-year period. In contrast, the stand limitation period under EU competition law is five years, even though there the authorities are typically not faced with the information asymmetries that exist in digital markets.

18 (i) The criteria of Article 3 (1) and (6) are vague – every provider will find arguments as to why they do not apply to it; (ii) the qualitative criteria in Article 3 (2) DMA-A do not imply any problematic gatekeeper status – hence providers have good reasons to bring their case, (iii) the notification process defers the time when the provider needs to comply – creating a strong commercial incentive to use this delaying process; (iv) there is no financial or other risk or disadvantage for the provider to submit such a notification. In other words, a provider may only win but not lose from this process; (v) companies that fulfil the turnover thresholds of Article 2(3) have nearly unlimited resources to compile extensive economic, technical and legal documents to make their case.

19 See footnote 12 above.

20 Notification (Article 3(3): 3 months; Commission's assessment (Article 3(4): 2 months; Market investigation (Article 15(3)): 5 months; Compliance period (Article 3(8): 6 months.

consequences. It will take further months before the Commission can react to any continuing ignorance of the obligations with a corresponding non-compliance proceeding. Moreover, since the obligations only become effective six months after the designation of a Gatekeeper, there is nothing that any affected business users could do about it (even if the obligations were enforceable in civil courts). In the worst case scenario – of the DMA blocking national competition laws[21] – Gatekeepers could use the mechanism to delay the process for up to sixteen months; thereby further entrenching their positions.

SUGGESTED AMENDMENTS

Against this background, we would recommend the following adjustments:

- Contrary to Article 3(4), the Commission should designate any provider of a core platform service that meets all thresholds of paragraph 2 and, based upon the Commission's preliminary assessment, also the thresholds of paragraph 1 that define a gatekeeper. If a designated gatekeeper believes that it does not fulfil the thresholds of paragraph 1, it should be entitled to request a market investigation in accordance with paragraph 6 and Article 15. Such request and any following market investigation shall not affect the obligation pursuant to Article 3(8) for a gatekeeper to comply with the obligations laid down in Articles 5 and 6 within a certain number (currently six, more appropriately three) months after its core platform service has been included in the list pursuant to Article 3(7). The Gatekeeper may, however, turn to the General Court to apply for a suspension of the Commission's designation decision. In such summary proceeding, the Gatekeeper shall bear the burden of proof and, if unsuccessful, all costs caused. This would reflect the statutory presumption in Article 3(2)[22] and reduce the risk that companies only challenge designation decisions with a view to delaying the due process.

[21] See below Chapter IV.

[22] In case of a statutory presumption, the party seeking to rebut this presumption typically bears the burden of proof.

Article #	Proposed Regulation, suggested deletions (~~strike through~~) and new insertions
	2. A provider of core platform services shall be presumed to satisfy: (a) [..] (b) the requirement in paragraph 1 point (b) where it provides a core platform service that has more than 45 million monthly active end users established or located in the Union and more than 10,000 yearly active business users established in the Union in the last financial year; for the purpose of the first subparagraph, monthly active end users shall refer to the average number of monthly active end users throughout at least six, not necessarily consecutive, months ~~***the largest part***~~ of the financial year; (c) [..] 3. Where a provider of core platform services meets all the thresholds in paragraph 2, it shall notify the Commission without undue delay and at the latest 30 days ~~***thereof within three months***~~ after those thresholds are satisfied and provide it with the relevant information identified in paragraph 2. That notification shall include the relevant information identified in paragraph 2 for each of the core platform services of the provider that meets the thresholds in paragraph 2 point (b). The notification shall be updated whenever other core platform services individually meet the thresholds in paragraph 2 point (b). A failure by a relevant provider of core platform services to notify the required information pursuant to this paragraph shall not prevent the Commission from designating these providers as gatekeepers pursuant to paragraph 4 at any time.
Article 3	4. The Commission shall, without undue delay and at the latest 60 days after receiving the complete information referred to in paragraph 3, designate the provider of core platform services that meets all the thresholds of paragraph 1 and 2 as a gatekeeper. ~~***, or decide that the provider has presented sufficiently substantiated arguments to demonstrate that, in the circumstances in which the relevant core platform service operates, and taking into account the elements listed in paragraph 6, the provider does not satisfy the requirements of paragraph 1.***~~ ~~***Where the gatekeeper presents such sufficiently substantiated arguments to demonstrate that it does not satisfy the requirements of paragraph 1, the Commission shall apply paragraph 6 to assess whether the criteria in paragraph 1 are met.***~~ 5. ~~***The Commission is empowered to adopt delegated acts in accordance with Article 37 to specify the methodology for determining whether the quantitative thresholds laid down in paragraph 2 are met, and to regularly adjust it to market and technological developments where necessary, in particular as regards the threshold in paragraph 2, point (a).***~~ 6. The Commission may identify as a gatekeeper, in accordance with the procedure laid down in Article 15, any provider of core platform services that meets each of the requirements of paragraph 1, but does not satisfy each of the thresholds of paragraph 2~~***, or has presented sufficiently adequately substantiated arguments in accordance with paragraph 4***~~. For that purpose, the Commission shall take into account the following elements: (a) the size, including turnover and market capitalisation, operations and position of the provider of core platform services; (b) the number of business users depending on the core platform service to reach end users and the number of end users;

	(c) entry barriers derived from network effects and data driven advantages, in particular in relation to the provider's access to and collection of personal and non-personal data or analytics capabilities; (d) scale and scope effects the provider benefits from~~**, including**~~ with regard to data; (e) business user or end user lock-in; (f)-other structural systemic market characteristics. In conducting its assessment, the Commission shall take into account foreseeable developments of these elements. Where the provider of a core platform service that satisfies the quantitative thresholds of paragraph 2 fails to comply with the investigative measures ordered by the Commission in a significant manner and the failure persists after the provider has been invited to comply within a reasonable time-limit and to submit observations, the Commission shall be entitled to designate that provider as a gatekeeper. Where the provider of a core platform service that does not satisfy the quantitative thresholds of paragraph 2 fails to comply with the investigative measures ordered by the Commission in a significant manner and the failure persists after the provider has been invited to comply within a reasonable time-limit and to submit observations, the Commission shall be entitled to designate that provider as a gatekeeper based on facts available. 7. For each gatekeeper identified pursuant to paragraph 4 or paragraph 6, the Commission shall within 3 months identify the relevant undertaking to which it belongs and list the relevant core platform services that are provided within that same undertaking and which individually serve as an important gateway for business users to reach end users as referred to in paragraph 1(b). 8. The gatekeeper shall comply with the obligations laid down in Articles 5 and 6 without undue delay but no later than three ~~**six**~~ months after a core platform service has been included in the list pursuant to paragraph 7 of this Article.

CHAPTER III – PROHIBITED PRACTICES

While far from comprehensive, the identified harmful practices largely echo the concerns of commercial broadcasters and other content providers active in digital markets**.** The Commission rightly points to the fact that several prohibited practices are interrelated, and that it is necessary for all of them to be banned in tandem for meaningful changes.

2.1. Obligations for gatekeepers *in*susceptible of being further specified (Article 5)

2.*1.1. Article 5 (a) – opt-in for personal data combination*

Overall approach to relevant data

ACT members are active in the advertising business and other areas where data is a key determinant. They are fully aware that gathering relevant data regarding end users' preferences and needs can be an effective tool to increase the relevance of advertising. Data is essential to generate positive indirect network effects between the user group of end users and the user group of advertisers, thereby improving the overall quality of the medium. Data can also be crucial to develop and add further helpful services. Innovation can and does come from all quarters. Therefore, all operators, not just companies controlling ecosystems, should be enabled to use data to innovate and enhance their offerings, including broadcasters.

Accordingly, ACT members do not condemn the accumulation and combination of data as such. Rather, they would recommend focussing on creating a level playing field for all companies active in the advertising industry as regards the gathering of and the access to relevant data.

To start off with, business users need to gain no less access to the data generated in the process of transactions with their end customers than the intermediary. It should be a matter of course, that gatekeepers make all the data available to business users that relate to their transactions. If a platform intends to combine data collected from a business user with other data sets, the business user should have the option to either prohibit such combination or to get access to the combined data itself. Moreover, in case a (hybrid) platform also competes with the business user, it should be prohibited from using such data to outcompete the business user, e.g. by algorithmically adjusting its own offerings to that of the business user. Where the collection, combination or sharing of data with business users requires consumer consent, the gatekeeper shall be obliged to make the same effort, using the same methods and prompts, for obtaining such consent as it applies for obtaining consent for its own service.

We understand that these issues of fairness are addressed generally by Article 6 (a) and (i) and specifically for ad inventory in (f) (see further below on this). In contrast, Article 5 (a) is not concerned with equal access and use by the intermediary and the business user of data relating to the latter. It has the goal of levelling the commercial advantages that a gatekeeper obtains from being part of a broad ecosystem with various other services that collect data – a "data collection eco-system" that rivals can hardly challenge. It is less about fairness and more about ensuring contestability of Gatekeepers.

The current version of Article 5 (a) should be revisited to meaningfully restrain the data collection powers of gatekeepers.

Opt-in option annuls benefits of Article 5 (a)

Article 5 (a) prohibits the bundling of data from various sources only if the user does not consent to such combination in the sense of an opt-in. When dealing with Gatekeepers, such solution is rather meaningless.

Under the GDPR, consent to the combination of personal data is required in any event. Article 5 (a) does not add any further hurdle for Gatekeepers in this regard. This is surprising given that, over recent years, experience has shown that the GDPR is inherently beneficial for large platforms to the detriment of smaller platforms.

By definition, given the lack of alternatives, end users are dependent on a gatekeeper as described in Article 3. Thus, by definition, Gatekeepers will find it easier than any other platform to obtain end user consent for data usage as a pre-condition for the use of their platforms. Consequently, for the DMA to reduce barriers to entry vis-à-vis digital gatekeepers, Article 5 (a) needs to be stricter than the GDPR requirement. This is why we believe that the obligation should not be attached to end users' consent, not even through an opt-in clause. The co-legislators should underline that by default, gatekeepers shall separate their data pools into separate data silos. There must be a high hurdle for combining such data. This could be based upon an end user's explicit request to combine data in order to obtain a significantly improved service. In such a case, the provider should bear the burden of proof that the combination of data indeed (i) improves the service, (ii) allows the end user a fair share of the resulting benefits, (iii) is indispensable for such improvement and (iv) does not eliminate competition.[23] Moreover, in order to ensure that the gatekeeper remains contestable, the end user's consent should only justify the gatekeeper's combination of data if the consent is equally given to the business users involved in the intermediation pursuant to Article 6 (1) (i).

Article #	**Proposed Regulation, suggested deletion (~~strike through~~) and new insertions**
Article 5 (a)	refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice between a less personalised alternative and a more personalised alternative that allows a measurable benefit for the end user which may only be achieved by combining the data and provided consent in the sense of Regulation (EU) 2016/679 to both the combination of data by the gatekeeper and the sharing of the relevant data according to Article 6 (1) (i).

2.1.2. Article 5 (b) – prohibition of parity clauses

Article 5 (b) contains an important prohibition for broadcasters as well, for instance where a gatekeeper does not allow a broadcaster to offer end users better conditions on different content platforms. The current version is limited to the offering of better conditions on other intermediation services (a "broad" most-favoured nation clause). However, broadcasters and other content providers also offer their services directly through their own websites or apps. Accordingly, the prohibition should be expanded to disallowing better conditions through the business users directly (a "narrow" most-favoured nation clause). In its *Booking.com* decision of May 2021, the German Federal Supreme Court confirmed that also such narrow clauses typically restrict competition without being objectively justified or required to prevent any 'free-riding'.[24]

[23] This method of justification is based upon the well-established principles and case law developed under Article 101 para. 3 TFEU, which ensures legal certainty.

[24] German Federal Supreme Court, 18 May 2021, KVR 54/20 – *Booking.com*

Article #	Proposed Regulation, suggested deletion (~~strike through~~) and new insertions
Article 5 (b)	*allow business users to offer the same products or services to end users through third party online intermediation services or own platforms or other distribution channels at prices or conditions that are different from those offered through the online intermediation services of the gatekeeper.*

2.1.3. Article 5 (d) – prohibition of contact with enforcement institutions

In ACT's view, it is important that the obligations laid down by Article 5 and 6 are also enforceable in civil courts by means of private enforcement (see below at Chapter IV). Accordingly, Article 5 (d) should be expanded to also cover conduct that penalises business users for enforcing the DMA before national courts. This is necessary because the DMA and the DSA distinguish between "authorities" and "courts".

Article #	Proposed Regulation, suggested deletion (~~strike through~~) and new insertions
Article 5 (d)	*refrain from preventing or restricting business users from raising issues with any relevant public authority, including national courts, relating to any practice of gatekeepers.*

2.1.4. Article 5 (e) – requiring business users to use ID service (and other ancillary services)

Overall approach to tying and bundling practices

ACT members are very concerned about the bundling and tying practices of digital gatekeepers, such practices are used to leverage market power into new markets and to foreclose competition. The ban on bundling/tying addresses a well-established category of abusive conduct in technology markets[25]. Such bans have also been successfully imposed by sector-specific regulation in network industries, in particular as regards telecoms providers with significant market power[26]. Vertically integrated gatekeepers have particular incentives to engage in such tying practices. In lack of any regulatory obligation to separate their services (at least in terms of accounting), they can easily cross-subsidise any service with profits generated through tying practices.

Economists have recommended that tying and bunding practices be presumed anti-competitive and that a general ban be included in the list of Article 6 DMA-A[27]. However, we assume that the current lack of such general ban in the DMA is linked to the fact that, in some (rare) cases, bundling and tying conducts may benefit consumers and that the need to assess such "defence" may be inconsistent with the per-se illegality approach pursued by the DMA (with a view to distinguishing it from competition law that shall not be harmonised).

The DMA therefore appears to target specific types of bundling and tying for which there is no plausible efficiency defence (Article 5 (e) and (f)). Such a selective approach does not come without risks. Gatekeepers

[25] See the cases of *Microsoft Windows Media Player (*Case T-201/04); *Microsoft – Tying (Internet Explorer)* (Case AT.39530), *Intel* (Case C-413/14 P) and *Google Android* (Case AT.40099).

[26] See Article 83 Directive (EU) 2018/1972 and previously Article 17 Universal Service Directive (EU) 2002/22/EC according to which "*national regulatory authorities shall impose appropriate regulatory obligations on undertakings identified as having significant market power on a given retail market […]. The obligations imposed may include requirements that the identified undertakings [..] show undue preference to specific end-users or unreasonably bundle services."*

[27] *Cabral/Haucap/Parker/Petropoulus/Valletti,Van Alstyne*, The EU Digital Markets Act: A Report from a Panel of Economic Experts, 2021, p. 13.

may argue that the list of explicit tying/bundling practices imply in turn that any other such practices are not prohibited, but permitted. This would lead to unbearable outcomes if, contrary to the current wording, the DMA would ultimately block any national competition laws dealing with Gatekeepers. Accordingly, it should be clarified that the list of obligations in Article 5 and 6 is without prejudice to the legality of equivalent Gatekeeper practices because the list does not allow any conclusion that other practices are less problematic.

Prohibiting the tying of gatekeeper services to video streaming or to advertising services

In line with the DMA's focus on particularly obvious and harmful types of tying and bundling, ACT members believe that further such practices may be identified and included in Article 5 or 6. In particular, ACT is concerned about the tying of video streaming services (such as Amazon Prime) with online intermediation services (such as sales on Amazon Marketplace) by granting monetary discounts (such as no delivery costs) for the purchase of goods if a user subscribes to any such video streaming service.

Equally harmful is the condition imposed by operating systems (such as Android connected TV) or content intermediation services (such as IMDB TV) that that content providers will only be displayed (and hence only reach the audience) if the content provider also uses the advertising intermediation service provided by that gatekeeper – instead of the content provider's own or a competing advertising service. Today, such practices can be seen as *per se* harmful tying conduct, not least since they are identical to the practice prohibited in the Commission's case of Google *AdSense*[28].

Article 5 (e) should be expanded to all types of ancillary services

Article 5 (e) only prohibits making the use of a core platform service dependent on the use of an identification service of the Gatekeeper. According to recital (14) and Article 2 (14), an identification service is a sub-category of an ancillary service. "Ancillary services" means any "*service provided in the context of or together with core platform services, including payment services [..], fulfilment, identification or advertising services*". There is no apparent reason as to why a Gatekeeper should be prohibited from bundling its core platform service with an identification service, but allowed to bundle it with another ancillary services. In line with the uniform treatment elsewhere in the DMA, Article 5 (e) should also pursue a uniform approach to ancillary services.

Article #	**Proposed Regulation, suggested deletion (~~strike through~~) and new insertions**
Article 5 (e)	*refrain from requiring business users to use, offer or interoperate with any ancillary service ~~an identification service~~ of the gatekeeper in the context of services offered by the business users using the core platform services of that gatekeeper;*

2.1.5. Article 5 (f) – prohibition of making access to CPS conditional on use of another service

[28] Decision of 20 March 2019, Case AT.40411 – *Google Search (AdSense).* The Decision found that Google abused its dominance on the market for online search advertising intermediation by requiring from its business users (website publishers seeking to use this service) (i) "to source all of their search ads requirements from Google", (ii) "to reserve the most prominent and therefore most profitable space on their search results pages for Google search ads" and (iii) "to refrain from placing competing search ads in a position immediately adjacent to or above Google search ads". In other words, Google's search advertising intermediation service was in effect tied to Google's search ads service. If publishers integrated a Google search service, they needed to display the search ads provided by Google instead of any search ads by another ad intermediary; see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020AT40411(03)&from=EN

Article 5 (f) is limited to prohibiting a Gatekeeper from making the "*access, sign up or regist[ration]*" to any core platform service dependent on the "*subscription*" or "*registration*" with any "*other core platform service identified pursuant to Article 3 (2)(b)*". Considering the detrimental effects of tying / bundling practices in digital markets described above (see 2.1.4), such prohibition appears too narrow in four ways.

First, it only applies to conditions for the "*access, sign up and registration*" to Gatekeeper services, while it should apply to any conditions for the use of a Gatekeeper service.[29]

Second, in addition to any need to "subscribe" or "register" with any core platform service, also the need to "use" such a service as a pre-condition to access, sign-up, register or use another service must be prohibited.

Third, to prevent leveraging, it makes little sense to only prohibit the tying of one Gatekeeper service with another gatekeeper service, while permitting the making of the use of a Gatekeeper service dependent on the use of another service for which the undertaking does not yet enjoy such position. Should the tying prohibition be limited to two Gatekeeper services together, the prohibition arrives too late, because the markets have likely already tipped and the users have become dependent on both services in any event. So, at the very least the scope of unfairly tied services must be extended to any core platform service (not just those with a gatekeeper status). In fact, since there is no justification for making the use of a gatekeeper service dependent on the use of any other service the provision should by extended to the tying to any digital service. In particular, as seen in the case of Amazon Prime (see above), under the current wording, a gatekeeper could make the use of its identified core platform service dependent on the subscription to its own video on demand platform - but not to its own video sharing platform. There is no plausible reason for such differentiation. Put differently: the reasons for limiting the scope of core platform services to multi-sided intermediation services do not apply (make little/no) sense when it comes to identifying the markets/services that should be protected from unfair leveraging or trading practices.

Forth, the prohibition should also cover cases of a mixed bundling, often referred to as multi-product rebates. While in the case of a 'pure' bundling the products are only sold jointly in fixed proportions, in the case of mixed bundling, the products are also made available separately, but the sum of the prices when sold separately is higher than the bundled price[30]. The Commission's "Guidance on the [..] enforcement priorities in applying Article [102] TFEU to abusive exclusionary conduct"[31] treats pure and mixed bundling equally[32]. Accordingly, a multi-product rebate is seen as abuse of dominance, "*if it is so large that equally efficient competitors offering only some of the components cannot compete against the discounted bundle*"[33]. The DMA should follow the same holistic approach. This would prevent circumventions, such as the current practice of Amazon to grant significant discounts if an end user purchases goods on the Amazon Marketplace and agrees to also subscribe to Amazon's video-on-demand service Amazon Prime.

Article #	**Proposed Regulation, suggested deletion (~~strike through~~) and new insertions**
Article 5 (f)	*refrain from requiring from business users or end users to subscribe to, ~~**or**~~ register or use any other [digital] service ~~**core platform services identified pursuant to Article 3 or which meets the thresholds in Article 3(2)(b)**~~ as a condition to access, sign up, ~~or~~ register to, use any of*

[29] An end user's use of a search engine or market place, for instance, does not require any "access, sign up or registration".

[30] Communication from the Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, 2009/C 45/02, para. 48.

[31] *Ibid*.

[32] See *ibid*, paras 48-62.

[33] *Ibid*, para. 59.

	their core platform services identified pursuant to that Article 3 or meeting the thresholds of Article 3 (2) (b) or as a condition for obtaining a better price for the use of such core platform services or any product or services offered through such core platform."
Article 5 (x)	*refrain from making the indexing, ranking or display of a business user in a core platform service dependent on this business user's subscription to, registration to or use of any core platform service identified pursuant to Article 3 or meeting the thresholds in Article 3 (2) (b)*

2.1.6. Article 5 (g) – price transparency in advertising intermediation

Overall approach to practices in advertising markets

ACT welcomes the fact that the DMA-P considers advertising services, including intermediation services, as core platform services, if they are offered by a provider of any other core platform service (Article 2(2)(h). This is in line with the qualification of advertising services as an "ancillary service" pursuant to Article 2(14). However, given that several of the largest tech undertakings are primarily advertising companies, and having regard to the high level of concentration along the entire digital advertising value chain, it comes as a surprise that, with Article 5 (g) and 6 (1)(g), the DMA-A only contains two specific requirements dealing specifically with online advertising services. This is even more astonishing because the obligations are limited to (narrow) transparency obligations that hardly exceed the obligations applicable to all online platforms regardless of their size or position pursuant to the Platform-to-Businesses Regulation (EU) 2019/1150.

As active advertising industry participants, ACT members are frequently faced with restraints caused by the highly concentrated online advertising markets. Even for the largest media companies, the advertising environment is highly opaque, given the discretionary activities/opaqueness of Gatekeepers. The latter can use their entrenched position to impose their Terms & Conditions to limit the disclosure of information on costs, effectiveness and profits of ad placements. As recital (42) rightly points out, "*the costs of online advertising are likely to be higher than they would be in a fairer, more transparent and contestable platform environment. These higher costs are likely to be reflected in the prices that end users pay for many daily products and services relying on the use of online advertising*". However, while the concerns have been rightly identified, the proposed transparency obligations are unlikely to effectively address them. A great deal more will have to be done to render such markets contestable, or at least to sufficiently discipline the incumbents.

Transparency vs fairness – need to eliminate conflicts of interests

The central issue of the advertising value chain is the close vertical integration of the dominating players. With their search, video-sharing and social media sites, Google and Facebook do not simply provide some of the most relevant mediums to place ads. They also provide the leading advertising intermediation platforms services for both the supply side of competing publishers (namely through Supply Side Platforms (SSPs) and the demand side of advertisers (through Demand Side Platforms (DSPs).

This creates nearly irresolvable conflicts of interests that inevitably lead to acts of self-preferencing. In addition, in an industry defined by data-driven network effects, given the lack of any regulation, such a conglomerate market structure also gives rise to extremely high barriers to entry. Transparency obligations are incapable of solving such issues because, given the lack of competition, transparency alone neither prevents exploitation nor increases contestability. Instead, regulation must neutralise the competitive advantages resulting from the unhindered vertical integration and bundling of relevant bidding data.

One way to achieve this objective is to prohibit a Gatekeeper from using data that is relevant for advertising purposes and that was collected via one advertising service (e.g., an SSP) in another advertising service, with

the objective of gaining a competitive advantage vis-á-vis competing bidders. Such use of data that the intermediary could only obtain from another intermediation service of the same undertaking should be considered to be unlawful "insider bidding" and prohibited - akin to insider trading in the banking sector.

Minimum scope of transparency

Even for the limited purpose of creating greater transparency, Article 5 (g) provides little assistance. The obligation is limited to providing "*information concerning the price paid by the advertiser and publisher*" and the "*amount or remuneration paid to the publisher*" and for each of the relevant advertising services provided. It should be a matter of course that a business partner is informed of the price that it is meant to pay.

However, a company is not helped if it is informed of the price it has to pay once that price has been (unilaterally and possibly unfairly) determined. Publishers and advertisers are far more interested in how such a price was determined, i.e., on the basis of which parameters and premises the price or the remuneration was calculated. To be able to assess whether a Gatekeeper with a conflict of interest has calculated a price fairly and reasonably, a business user needs to know which criteria and which calculation methodology the Gatekeeper used, in particular as regards any biddings in algorithmic auction processes. In other words, regulation must shed some light into the price finding mechanisms used by the algorithm-driven black boxes of digital advertising Gatekeepers.

Article #	**Proposed Regulation, suggested deletion (~~strike through~~) and new insertions**
Article 5 (g)	provide advertisers and publishers to which it supplies advertising services, upon their request, with a comprehensive set of information concerning: (i) the price and its components, including any fees, surcharges or deductions, paid by the advertiser and publisher, as well as the amount or remuneration paid to the publisher, for the publishing of a given ad and for each ~~**of the relevant**~~ advertising service~~**s**~~ provided by the gatekeeper; (ii) the methodology for the calculation of fees and surcharges, including its application to any bids submitted by the advertiser and publisher for each of the advertising service used, (iii) the outcome of an [annual] independent audit of the auctions for any matching of supply and demand for advertising.
Article 5 (g1new)	in addition to the obligations pursuant to Regulation (EU) 2019/1150, ensure that the full chronology of the contracts concluded between the gatekeeper and a business user as well as any corresponding terms and conditions is easily available to that business user at all stages of the commercial relationship, including for at least five years following the end of the relationship.
Article 5 (g2new)	refrain from making available any data not publicly available, which may influence the outcome of advertising intermediation services, sourced from one advertising service of the gatekeeper to any other advertising service belonging to the same undertaking at a different level of the advertising value chain.
Recital (42)	The conditions under which gatekeepers provide online advertising services to business users including both advertisers and publishers are often non-transparent and opaque. [..] Furthermore, the costs of online advertising are likely to be higher than they would be in a fairer, more transparent and contestable platform environment. These higher costs are likely to be reflected in the prices that business and end users pay for many daily products and services relying on the use of online advertising. Transparency

	obligations should therefore require gatekeepers to provide advertisers and publishers to whom they supply online advertising services, with information that allows both sides to understand the price paid for each of the different advertising services provided as part of the relevant advertising value chain. This should include comprehensive information regarding the methodology for calculating any prices and fees and its application in relation to the respective bids submitted by an advertiser or publisher for each of the advertising intermediation services provided. Furthermore, the gatekeeper shall subject the auction-based matching of advertising demand and supply to regular independent audits to ascertain that the outcome of such auctions corresponds with the bids made and the fees charged reflect the pricing information provided by gatekeeper.

2.2. Obligations for gatekeepers susceptible of being further specified (Article 6)

2.2.1. Article 6 (1) (a) – prohibition of using non-public data generated by competing business users

ACT strongly welcomes Article 6 (1) (a), in particular because it applies to all types of core platform services, including, for instance, app stores, operating services or ancillary advertising services. In particular, i our proposal for a new Article 5 (g2) (see above) is not adopted, Article 6 (1) (a) may play a crucial role in the advertising industry. Gatekeepers have routinely used data generated by the consumption of audio-visual content on their platforms for their own commercial gains, including for advertising in competition with the providers of the content. To enhance the effectiveness of the prohibition, its wording should be aligned with that of Article 6 (1) (i) as regards the type of data that may not be used. It should also be clarified that the prohibition also applies where the gatekeeper uses the data of one business user ("A") to compete not against such particular user, but with another business user ("B"). In both cases competition is unfairly distorted.

Article #	**Proposed Regulation, suggested deletion (~~strike through~~) and new insertions**
Article 6(1)(a)	refrain from using, in competition with any business users, any data not publicly available, which is provided for or generated through or in the context of activities by ~~**those**~~ business users, including by the end users of ~~**these**~~ business users, of its core platform service or provided by those business users of its core platform services or by the end users of these business users;

2.2.2. Article 6 (1) (b) – app un-installing

Article 6 (1) (b) addresses an extreme form of self-preferencing, namely the pre-installation of apps on mobile devices by undertakings controlling the app store or the operating system. As observed in the Commission's *Android* case[34], such pre-installations can foreclose any competition as end users are subject to a "status quo bias"[35] that keeps them from switching to alternative, more relevant apps.

Against this background, we are surprised that Article 6 (1) (b) diverts from remedies developed under competition law. Article 6 (1) (b) only obliges Gatekeepers to allow end users to un-install any pre-installed

[34] Case AT.40099 – *Google Android*.

[35] In behavioural economics, a "status quo bias" describes the phenomenon that end users prefer that things stay as they are or that the current state of affairs remains the same.

apps. It does not prohibit such pre-installations in the first place. Neither are Gatekeeper obliged to actively provide a choice to end users. Due to the strong "status quo bias", it is very unlikely that end users will switch and make well-informed choices if such choices are not presented and explained to them in the first place. This was a key learning from the Commission's *Android* case.

Moreover, gatekeepers should not be enabled and incentivised to circumvent the prohibition by integration functionalities in another way than through a software application. End users should be enabled to un-install any functionality on a device, irrespective of its technical labelling, as long as this does not jeopardise the security or other functionalities[36]. The gatekeeper should bear the burden of proof that such risks exist.

Article #	**Proposed Regulation, suggested deletion (~~strike through~~) and new insertions**
Article 6(1)(b)	~~allow end users to un-install any pre-installed software applications~~ refrain from pre-installing own services on its core platform service without prejudice to the possibility for a gatekeeper to ~~***restrict such un-***~~install such services that are essential for the functioning of the operating system or of the device and which cannot technically be offered on a standalone basis by third-parties or to present end users with a significant choice of alternative services that may be installed, where such choice screen provides sufficient information about the service and the selection mechanism is automatically repeated at least every six months. .

2.2.3. Article 6 (1) (c) – enabling of side-loading

The obligation pursuant to Article 6 (1) (c) regarding the installation and effective use of third-party apps or app stores is also relevant for ACT members seeking to reach users through different distribution channels. Gatekeepers have various options to technically hamper or complicate the uploading of competing software. They may also try to penalise any such installation by reducing the scope or demoting the quality of other services used by the end user. In particular where a gatekeeper needs to implement technical steps to enable a side-loading, it is not enough to merely oblige it to "allow" such side-loading.

Moreover, in contrast to Articles 6 (1) (d) and (e) that ensure the use of any third-party service, Article 6 (1) (c) is limited to "software applications" or "software application stores". End users should also be allowed to install other services where this is technically feasible, such as a video-streaming service.

In addition to being entitled to install such other services, end users should also be enabled to easily set their side-loaded app or service as the new default[37]. Otherwise the gatekeeper may undermine the installation of any further apps or services by automatically and continuously providing its own service as the default – burdening the end user to click or access the side-loaded app or service each time they wish to use it.

Finally, while in general end users should have a choice, the gatekeeper should still be entitled to reject the installation of any service that would that does not comply with legal requirements or facilitates illegal practices such as copyright infringing video streaming. The Gatekeeper should bear the burden of proof that any side-loaded app or service endangers the integrity of its system.

[36] BEUC, Digital Markets Act Proposal, Position Paper, 2021, p. 10 with reference to the pre-installed health service on iPhones, which may or may not be considered as an app.

[37] BEUC, ibid., p. 10.

Article #	Proposed Regulation, suggested deletion (~~strike through~~) and new insertions
Article 6(1)(c)	allow and technically enable the effective installation, ~~and~~ effective use, full interoperability of third-party software applications and services or software application stores using, or interoperating with, operating systems of that gatekeeper and allow and enable these software applications, ~~or~~ software application stores or services to be accessed by means other than the core platform services of that gatekeeper and to serve as the new default. The gatekeeper shall not be prevented from taking proportionate measures to ensure that third party software applications, ~~or~~ software application stores or services do not endanger the integrity of the hardware or operating system provided by the gatekeeper or enable or facilitate any illegal activities by end users such as copyright infringements;

2.2.4. Article 6 (1) (d) - prohibition of self-favouring in ranking

Overall approach to self-preferencing practices

An effective ban on self-preferencing is one of the most important provisions in the DMA. ACT has identified several self-preferencing practices that impair end users' ability to find and access high quality content online and thereby deprive them of the cultural and linguistic wealth that defines Europe.[38] This does not just relate to the ranking of our members' offerings in Google Search, on YouTube or on Facebook. We have observed that, more generally, Gatekeepers deploy self-preferencing practices to establish and control new market entry points through which end users may access digital content.

Self-preferencing bears the risk that such new access points are then used to primarily push the Gatekeeper's own offerings to the detriment of competing content providers. For example, Google and Amazon are in the process of developing new smart devices and interfaces that provide a curated audio-visual experience.[39] Embedded in their omnipresent ecosystems, it is highly likely that such interfaces will constitute crucial market entry points for broadcasters in the future. Self-preferencing practices may then be deployed to allow the Gatekeepers to steer consumers towards their own services and away from more relevant sources, including the content/services of broadcasters.

The intermediation power of Gatekeepers could allow them to determine the "winners and losers" on any interface they control and in any market that they intermediate. Accordingly, a strict ban on unjustified preferencing of own services or those of partners is an indispensable precondition for a well-functioning internal market.

[38] See Annex - ACT Perspectives on the New Competition Tool - www.acte.be/publication/act-perspectives-on-the-new-competition-tool/

[39] In particular, Google (Android TV) and Amazon have ambitions, through arrangements with OEMs, to become the default provider of operating systems for a potentially wide range of connected (IoT) devices: connected TVs, soundbars and speakers etc.

By now, the detrimental effects of such practices, if carried out by Gatekeepers, have been well understood. There is a global consensus that they seriously harm competition between business users[40]. At the same time, Gatekeepers have repeatedly demonstrated that they are highly creative and capable of exploiting their technological means and existing information asymmetries vis-à-vis authorities in order to evade obligations and remedies imposed on them.[41] Accordingly, the DMA needs to focus on getting such prohibitions "right".

The current version of Article 6 (1) (d) leaves significant loopholes that need to be closed.

Self-preferencing through other means than ranking

Article 6 (1) (d) only addresses favourable "rankings". Article 2 (18) defines a "ranking" as "*relative prominence given to goods or services offered through online intermediation services or online networking services, or the relevance given to search results by online search engines*". This narrow approach fails to sufficiently address self-preferencing

(i) by any other core platform service such as operating systems, cloud computing services, advertising systems or ancillary services, even though such practices will be equally harmful;

(ii) other than granting a more favourable graphical *display* "prominence" such as a more favourable *content* of results (e.g., more informative and less offensive descriptions[42]), a preferential crawling, indexing[43] or other "access"[44] of offerings/content to the intermediation service;

---

[40] See *Cabral/Haucap/Parker/Petropoulus/Valletti,Van Alstyne*, The EU Digital Markets Act: A Report from a Panel of Economic Experts, 2021, p. 13 "*we believe self-preferencing is a natural candidate for the 'blacklist' of practices to be deemed anti-competitive and 'per-se' disallowed*"; regarding the detrimental effects of search bias: U.S. House of Representatives Subcommittee on Antitrust report, Investigation of Competition in Digital Markets, October 2020, pp. 177 et seq., pp. 381, 395, 397; United States et al. v Google LLC, U.S. District Court for the D.C., Case No. 1:20-cv-03010, Complaint of 20 October 2020, paras. 170, 175.

[41] In November 2020 a coalition of 165 tech undertakings and associations observed that Google has failed to implement the equal treatment remedy imposed in the European Commission's Google Shopping Decision of 2017 and requested that the Commission enforce the remedy imposed (Reuters, 12 November 2020, Exclusive: Group of 165 Google critics calls for swift EU antitrust action – letter, https://www.reuters.com/article/us-eu-alphabet-antitrust-exclusive-idUSKBN27S0YQ). This was based on a study that found that Google technically evaded the Commission's remedy (see). Similarly, several industry groups and general search services have complained that Google has failed to comply with the Commission's 2018 Android decision. This was also brought to the attention of the European Parliament, see Parliamentary questions, 15 January 2021, Question for written answer E-000215/2021 https://www.europarl.europa.eu/doceo/document/E-9-2021-000215_EN.html. See also *Cabral/Haucap/Parker/Petropoulus/Valletti,Van Alstyne*, The EU Digital Markets Act: A Report from a Panel of Economic Experts, 2021, p. 13 "*in some cases self-preferencing is blatant, in most cases, it is not*".

[42] As an example, in March 2021 the French Competition Authority decided to continue investigating whether the way in which Apple requests consent for tracking end users via apps (introduced with iOS 14) can be "*regarded as a form of discrimination or 'self-preferencing, which could in particular be the case if Apple applied without justification, more binding rules on third-party operators than those it applies to itself for similar operations*". App developers and advertisers are arguing that the way Apple informs end users about a possible tracking and requests consent disadvantages rivals, given that Apple does not request such consent for the use of its own services. See https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising-apples-implementation-att-framework-autorite-does-not-issue

[43] For instance, a core platform service may index content of rival business users less frequently or less comprehensively than content from its own services.

[44] Note that while Article 6 (1) (f) and (k) prohibit the hampering of "access", conversely Article 6 (1) (d) does not mention "access". In other words, the most extreme form of self-preferencing (= excluding access of certain rival business users) is not covered by lit. (d).

(iii) by any preferential sharing of data regarding the ranking criteria and how to influence them[45];

(iv) by search engines that provide their services directly within general search results pages or exchange unbiased intermediation (via organic results) for biased intermediation (via paid results or the display of own content)[46].

Self-preferencing through preferential ranking of selected business partners

Article 6 (1) (d) only addresses a favouring of products or services that belong to the undertaking of the Gatekeeper. However, a Gatekeeper may achieve the same anti-competitive outcomes if, instead of favouring a subsidiary, it favours an external business partner with whom it has concluded an exclusivity agreement that ensures that the profits gained from such favouring are largely returned to the Gatekeeper or its subsidiaries. The recent German case[47] of Google's exclusive favouring of a third-party health portal to the economic benefit of Google itself and to the detriment of all competing health portals may serve as an example for this.

Monitoring of self-preferencing practices

In addition to the material adjustments of the ban on self-preferencing, the DMA should also pay more attention to the instruments available for the enforcement authorities to detect, evaluate and monitor such conduct. The complex algorithmic and data-driven ranking of the various types of results in search engines, app stores or marketplaces can only be effectively monitored by a highly specialised and sufficiently equipped enforcement unit, ideally on a day-to-day basis.

Such units must be able to audit and test any mechanisms underlying an intermediation process so that discrimination becomes detectable and alternative solutions can be evaluated. Against this background, we are highly sceptical of presuming that "*[t]he burden on the Commission for implementing this [DMA] initiative is low (mainly redeployment of existing job positions)*"[48]. Despite a high-profile investigation of now over eleven years into Google's favouring of various own services in general search results, we still have not seen any end to this process[49]. We do not see how the current institutional set-up for the DMA would allow a significantly more effective approach to this (see Chapter IV below).

Article #	Proposed Regulation, suggested deletion (~~strike through~~) and new insertions
Article 6(1)(d)	refrain from treating more favourably in crawling, indexing, ranking or obtaining information regarding the criteria for such measures any services and products offered by the gatekeeper itself or by any ~~**third**~~ party, with which it has entered into an agreement, ~~***belonging to the same undertaking***~~ compared to similar services or products of third-party~~y~~ies and apply fair, reasonable and non-discriminatory conditions to such crawling, indexing and ranking,

[45] If the provider of a core platform service informs its subsidiary faster, more precisely or more comprehensively about any existing or upcoming (change of) criteria for the matching of offers, the subsidiary can adjust its offerings better than competing services, which will help it to use such criteria to its advantage.

[46] According to recent study, in 2020 only every third query entered on Google led to a click on an external website; two-thirds of the queries ended on Google's site (see Business insider, 24 March 2021, Google hogs traffic for itself, according to data showing nearly two-thirds of searches ended without a click in 2020, Google Searches End Without a Click Almost Third-Thirds of the Time (businessinsider.com)). This suggests that Google is using its gatekeeper search engine to directly satisfy the demand for information by giving answers / displaying content directly in results pages.

[47] Regional Court of Munich I, Judgements of 10 February 2021, Az. 37 O 15720/20 & 15721/20 – *NetDoktor*; See *Hoppner/Nobelen*, Unhealthy Ranking Conspiracy: The German NetDoktor Judgments Banning the Favoring of a Health Portal within Google Search, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3793429

[48] DMA-A, Explanatory Memorandum, p. 11.

[49] See the request of 165 companies from various industries to bring Google's self-preferencing to an end (see footnote 31).

Article 2(X-new)	"search result" means any information presented in any format, including texts, graphics, videos, voice or other output, returned in response and related to any written, oral or equivalent search query, irrespective of whether the information constitutes an organic result, a paid result, a direct answer or any product, service or information offered in connection with, or displayed along with, or partly or entirely embedded in the results interface.
Article 6(1)(d2new)	provide sufficient space in results pages of its core platform service for organic search results generated by a purely relevance-based intermediation service as compared to paid search results or own offerings generated by the gatekeeper and clearly indicated the bias nature of the latter.
Article 6(1)(d3new)	Option 1: refrain from making the collection and combination of relevant data from end users or the obtaining of consent for the use of such data by the business user for the purposes of serving interest-based advertising within a core platform service more burdensome than for the gatekeeper itself or any party belonging to the same undertaking. Option 2: refrain from imposing mechanisms or conditions that make the collection and combination of relevant data from end users or the obtaining of consent for the use of such data by a business user for the purpose of serving interest-based advertising within a core platform service more burdensome or difficult where the business user complies with all statutory requirements for such advertising, in particular under Regulation (EU) 2016/679.

2.2.5. Article 6(1)(e) – prohibition of restricting user switching

Article 6(1)(e) addresses a very harmful conduct, namely the (artificial) technical restriction of the ability of end users to switch between competing services. An unrestrained multi-homing on the side of end users is a crucial pre-condition for competition on multi-sided markets. Considering the high relevance of keeping switching costs and hurdles low, it is difficult to see why the artificial restricting of any switching of a service should only be prohibited if it is carried out by a provider of an operating system.

Moreover, Gatekeeper providers of app stores, search engines and web browsers can implement unnecessary technical hurdles for end users in an effort to prevent switching. To maintain contestability, every provider of a gatekeeper service should therefore be prohibited from technically restricting the ability of end users to switch between services and subscribe to any other service. Since such services are multi-sided by nature, the same should apply to restrictions for business users to switch services. For example, search engines and social networks should not make it technically more difficult for advertisers to switch to alternative advertising networks in order to serve ads on their platforms or elsewhere.

Article #	**Proposed Regulation, suggested deletion (~~strike through~~) and new insertions**
Article 6(1)(e)	refrain from technically restricting the ability of end users or business users to switch between and subscribe to different online ~~*software applications and*~~services to be accessed using the core platform service ~~***operating system***~~ of the Gatekeeper, including as regards the choice of Internet access provider for end users;

2.2.6 – Article 6 (1) (f) – access to operating system and other features

Article 6(1)(f) addresses a particular type of leveraging of market power over an operating system to other markets by means of granting preferential access to certain technical features to the Gatekeeper's own services. Such leveraging practices should be prohibited, however, not just if any "ancillary service" is

favoured, as (narrowly) defined in Article 2(14). The favouring of any of the Gatekeeper's separate services should be condemned.

Article #	Proposed Regulation, suggested deletion (~~strike through~~) and new insertions
Article 6(1)(f)	allow business users and providers of other services, including ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any other service, including any ancillary services

2.2.7. Article 6(1)(g) – transparency in advertising intermediation (performance)

As outlined above in 2.1.6, the massive conflicts of interest of vertically integrated ad tech Gatekeepers cannot sufficiently be addressed by transparency obligations alone. Where business users are faced with no alternatives to penalise unfair practices that affect their performance, finding out about such practices is of limited help.

However, the obligation under Article 6 (1) (g) is a good starting point to prevent Gatekeepers from (i) obscuring the actual performance of their service to make them look more effective than competing ad intermediation services (horizontal component), and; (ii) exploiting advertising and publishing customers by charging for services or "clicks" for which no payment is merited, in particular as they were influenced by ad fraud practices that only the intermediary may detect (vertical component). To achieve such minimum objectives, the current wording of Article 6 (1) (g) is too narrow for three reasons.

First, the obligation is limited to the "performance measuring tools of the Gatekeeper". If the Gatekeeper stops using such tools, no transparency is created.

Second, the carrying out of their own "independent verification" by advertisers and publishers is limited to verifying "the ad inventory". This appears to be limited to information concerning the ad inventory of the publisher or advertiser itself. In contrast, recital (53) more adequately refers to the "independent verification of the provision of the relevant online advertising services", including the verification of the Gatekeeper's intermediation service.

Third, while it is important that publishers and advertisers may verify the service of the Gatekeeper, it is equally important that they are enabled to measure, on an individual basis, the performance of their own campaigns and to use independent Joint Industry Committees (JICs[50]) to this end. Such JICs play a significant role in verifying the reach and the usage of ad-financed media, which in turn is crucial for media outlets in setting up, scaling and pricing effective online advertising campaigns.

In this respect, it is also worth noting that each advertiser may have a different, individual definition of "performance". While some care more about the overall reach and long-term branding effects of their ads, others define success in terms of immediate returns on investment. To assess the entire breadth of the effects of an advertising campaign, an advertiser itself – not the intermediary - must be able to determine which performance parameters are to be measured and analysed. To this end, instead of merely obligating the Gatekeeper to share the performance tools it has developed for its own purposes, the Gatekeeper should be obliged to provide their business users with standardised access to the relevant raw data relating to the performance of their ad campaigns. Such an obligation would be less invasive than, for instance, the data-

[50] JIC such as agof of agma are organisations in which media companies and agencies, advertisers and media agencies come together in order to jointly, independently and neutrally research the respective media.

sharing obligation pursuant to Article 6 (1) (j) (vis-à-vis search engines), because the raw data was accumulated in the process of providing the service for the business user and directly relates to the latter's business. If such data is not shared with business users, the data advantages of the walled-off eco-systems of the Gatekeeper will only increase. Article 6 (1) (g) can be seen as a special application of the general obligation under Article 6 (1) (i) (to share data relating to business users) to the advertising industry. To maintain its independent relevance, the standard must not fall below that of Article 6 (1) (g). Accordingly, access to the relevant ad performance raw data must be provided in an "effective, high-quality, continuous and real-time" manner.

Article #	Proposed Regulation, suggested deletion (~~strike through~~) and new insertions
Article 6(1)(g)	(g) provide advertisers and publishers, upon their request and free of charge access to the performance measuring tools of the Gatekeeper and via a suitable interface high-quality, continuous and real-time access and use of all the information and data necessary for advertisers, publishers independent third parties, to effectively carry out their own independent measurement of the performance of their services and the intermediation services provided by the Gatekeeper, including the verification of the provision of the relevant advertising services, the ad inventory and the attribution.
Recital (53)	Add: "This shall include data relating to all parameters used by the Gatekeeper or services belonging to the same undertaking in the context of advertising intermediation services to determine the outcome of such intermediation and corresponding prices for ads or charges for any intermediation service provided either on the buy-side or the sell-side.

2.2.8. Article 6(1)(h) – provision of data portability

Enabling data portability is a crucial tool in rendering an established Gatekeeper platform contestable. To avoid loopholes, the wording should be aligned with that of Article 6 (1) (i), and it should be ensured that the obligation may not be relied upon by one Gatekeeper to gain access to the data of another Gatekeeper.

Article #	Proposed Regulation, suggested deletion (~~strike through~~) and new insertions
Article 6(1)(h)	provide effective portability of data provided for or generated through or in the context of the activity of a business user or end user to other services that have not been designated as gatekeepers and shall, in particular, provide free of charge tools for end users and business users to facilitate the exercise of data portability, in line with Regulation EU 2016/679, including by the provision of continuous and real-time access;

2.2.9 – Article 6 (1) (i) – access to data generated by intermediating between end users and business users

Data provides broadcasters and other providers of digital services with important insights on how audiences consume and engage with content. Such insights help in better catering to the interests of all user groups and thereby improve the quality of digital services (see above at 2.1.1).

At present, when distributing content through Gatekeeper platforms, broadcasters often fail to enhance the positive network effects of their services, as Gatekeepers decline to share with them the data allowing them to better fine-tune the offerings to the needs of all users. In particular, Gatekeepers typically refuse to share any data regarding the number of views or any interactions of end users with relevant content. As a result, while Gatekeepers can use such data to further improve their own services and enter new markets (often in competition with their business users), such data systematically reduces the ability of such business users to improve their own services (and to compete with the Gatekeeper anywhere in its eco-system). Given that the Gatekeeper is unavoidable in reaching audiences, broadcasters have no other choice but to accept this one-sided and unfair mechanism. In order to use the Gatekeeper services to reach their respective (single-homing)

audiences, broadcasters need to make their data available to the Gatekeeper and to accept its conditions as regards the free combination and use of such data.

To make matters worse, in order to enhance their superior access to data, Gatekeepers increasingly use privacy laws as an excuse to further deprive business users and competing operators of relevant data. While, given end users' dependency on Gatekeeper services, the providers of such service find it easy to collect and bundle data in a GDPR-compliant manner, they reject sharing such data with business users on the basis of alleged GDPR-non-compliance[51]. Since business users cannot equally leverage market power in order to acquire data, the data supremacy of Gatekeepers vis-à-vis their competitors and business customers will only increase.

Gatekeepers are in a unique position to facilitate the obtaining of consent. Where a user accesses a third-party service through a Gatekeeper platform, the platform is used to facilitate the obtention of consent for both the use of data by itself and the third-party service. The Gatekeeper cannot restrict the obtention of consent for its purposes alone.

Against this background, parallel to the concerns expressed against the current version of Article 5 (a) (see above at 2.2.1), we fear that the data sharing obligation pursuant to Article 6(1)(g) is rendered meaningless if it remains dependent on the end-user having opted in with a consent under the GDPR. The GDPR (and likely also the e-Privacy Regulation) inherently favour Gatekeeper platforms vis-à-vis other digital businesses. It would be counter-productive if the DMA further entrenched the imbalance created under the GDPR by automatically reducing the scope of its prohibitions to that of such laws. The data protection and privacy laws apply horizontally to any platform. The DMA, in contrast, is limited to Gatekeepers with particular market power. For such Gatekeepers stricter requirements are justified, both as regards their market conduct but also as regards the measures taken to ensure privacy.

In order to secure the independent character and approach of the DMA, the obligations it imposes should therefore not automatically be restrained by (horizontally applicable) requirements under data protection and privacy laws. Article 7 (1) clarifies explicitly that a Gatekeeper shall ensure that the measures taken ensure compliance with the obligations laid down in Articles 5 and 6 *"are implemented in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC, and with legislation on cyber security, consumer protection and product safety*". Hence, the need to adhere to data protection laws does not need to be embedded in the obligations themselves. Instead, it would be more systematic to address any conflicting interests following from the GDPR (or any other legislation) in the context of a Gatekeeper's suspension or exemption from obligations (Article 8 and 9 DMA-A) and the prohibition of circumventing the DMA obligations pursuant to Article 11 DMA-A. In so doing, Gatekeepers may only rely on privacy defences only if it has done its best (= the same as for its own service) to comply with GDPR/privacy requirements (see below at 2.2.9).

Employing hundreds of behavioural scientists, economists and programmers, Gatekeepers have many options for influencing whether or not their end users grant consent to the use of their data. They systematically use interface designs and methodologies to exploit existing consumer biases in order to influence how they behave and engage with the gatekeeper[52]. Currently, the "consent-*defence*" in Article 5 (a) creates an incentive for Gatekeepers to nudge end users into granting broad consent for the collection and combination of data by the Gatekeeper itself and the undertaking to which it belongs. In contrast, the "consent-*requirement*" in Article 6 (1)(i) creates the opposite incentive for Gatekeepers to nudge their end users into denying consent for the sharing of data with business users. This will lead to imbalance. In order to reduce barriers to entry by creating

[51] See the investigation into Apple's tracking warning referenced above in footnote 32.
[52] See BEUC, Digital Markets Act Proposal, Position Paper, 2021, p. 7-8.

a level playing field for the collection of data, the commercial interests of the Gatekeeper in obtaining consent for the use of data should be aligned with the equivalent interests of its business users.

The DMA can align such interests by introducing a simple principle - wherever the Gatekeeper fails to obtain consent from end users to share personal data that has been generated in the context of the use of the core platform service with the intermediated business user pursuant to Article 6 (1) (i)), the Gatekeeper should be prohibited from using such data for any purpose other than the original intermediation as well[53]. In particular, it must not combine the data with any data gathered from other sources or use it for the provision of another service. In other words, if the Gatekeeper does not obtain consent from end users to share their data with its business users, the Gatekeeper must also not use such data itself.

Article #	Proposed Regulation, suggested deletion (~~strike through~~) and new insertions
Article 6(1)(i)	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 by those business users and the end users engaging with the products or services provided by those business users; for personal data, provide access and use ~~***only***~~ where ~~***directly***~~ connected with the use effectuated by the end user in respect of the products or services offered by the relevant business user through the ~~***relevant***~~ core platform services~~***, and wherein the end user opts in did not opt-out to such sharing with a consent in the sense of the Regulation (EU) 2016/679***~~
Article 11(2)	Where consent for collecting~~***, or***~~ processing or sharing of personal data is required to ensure compliance with this Regulation, a Gatekeeper shall take the necessary steps to either enable business users to directly obtain the required consent to their processing and retrieval, where required under Regulation (EU) 2016/679 and Directive 2002/58/EC, or, if such consent is not obtained, to comply with Union data protection and privacy rules and principles in other ways including by providing business users with duly anonymised data~~***where appropriate***~~.
Article 11(2)(a)	The gatekeeper shall not make the obtaining of this consent by the business user more burdensome than for its own services. Neither shall the gatekeeper make it less burdensome or create stronger incentives to withdraw any such consent (opt-out) for the business user than for its own services. Where an end user has not granted or has withdrawn consent for the collection and processing of personal data required to ensure compliance with this Regulation, a gatekeeper may not itself process such data for any other purpose than the provision of the core platform service for which the data was provided by the end user.

2.2.10 – Article 6 (1) (j) – access to search data

The obligation for Gatekeeper online search engines to grant FRAND-access to relevant search data eliminates the central barrier to entry for online search services and thereby renders the market for general search

[53] Similar *Cabral/Haucap/Parker/Petropoulus/Valletti/Van Alstyne*, The EU Digital Markets Act: A Report from a Panel of Economic Experts, 2021, p. 21 "*Information flows from the platform to the separate parts [of the undertaking] are not allowed, unless that information is shared with all business users*".

services contestable. In order to render this obligation more effective, its wording should be aligned with that of Article 6 (1) (i), and it should be clarified that such data needs to be made available in real-time.

Article #	Proposed Regulation, suggested deletion (~~strike through~~) and new insertions
Article 6(1)(j)	provide any third-party providers of online search engines, upon their request, with effective, high-quality, continuous and real-time access on fair, reasonable and non-discriminatory terms as regards ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data;

2.2.11 – Article 6 (1) (k) – prohibition of unfair access conditions

App stores have become central gateways for app developers to reach end users. Providers of app stores seek to exploit this position by imposing unfair terms and conditions. For instance, without engaging in any negotiations they charge business users a standard fee of 15% to 30% of the revenues generated through an app on their store. Such charges quickly amount to an unjustified "tax" that all app developers have to pay to gain access to end users. Accordingly, Article 6 (1) (k) is generally welcomed by the ACT.

However, ACT is surprised and concerned that the obligation to apply fair and non-discriminatory general conditions is to be limited to the access of apps to app stores. The DMA's underlying rationale is that all designated Gatekeepers enjoy a particular market power that merit obligations to ensure fairness and contestability that go beyond those of general competition law. As a starting point, each Gatekeeper is to comply with the obligations laid down in Articles 5 and 6 "*in respect of each of its core platform services identified [as Gatekeeper] pursuant to Article 3(7)*" (see first sentence of Article 5 and 5). Such common approach to all Gatekeeper services is, in principle, justified as all such services should share the same characteristics of market power laid down in Article 3 (1).

If, however, as a departure from this common approach, some obligations (such as Article 6 (1) (k)) are only addressed with particular, singled-out services (such as app stores), based upon an *argumentum e contrario*, this implies that the DMA does not foresee this particular obligation for any other Gatekeeper service. Accordingly, Article 6 (1) (k) suggests that the DMA allows all other Gatekeepers to impose unfair and discriminatory general conditions for the use of their service. To make matters worse, according to Article 1 (5) "*Member States shall not impose on Gatekeepers further obligations by way of laws, regulations or administrative action*". This may even block national competition law that currently ensures fair and non-discriminatory terms and conditions of companies with Gatekeeper characteristics. Accordingly, if Article 1 (5) were taken literally, the DMA would in effect legalise such unfair practices for the large majority of Gatekeepers and hence even strengthen the position of such players vis-à-vis their business users.

There are two ways of addressing this issue. The most coherent and consistent solution would be to expand the prohibition of unfair (unreasonable) and discriminatory conditions to all designated Gatekeepers. There is no justification to allow any Gatekeeper to impose such terms and conditions. At the very least, a second option would be for the DMA to clarify that any prohibition of certain conduct that is limited to a particular service does not imply that such conduct is legitimate for any of the other Gatekeepers, and that the DMA leaves Member States free to address such conduct through national laws (see also below at Chapter IV).

Article #	Proposed Regulation, suggested deletion (strike through) and new insertions
Article 6 (1) (k)	apply fair, reasonable and non-discriminatory general conditions of access and use for business users to its core platform service ~~***software application store***~~ designated pursuant to Article 3 of this Regulation.

3. Article 7 - compliance with obligations laid down in Article 5 and 6

As stated previously, ACT urges the legislator to enact this Regulation as quickly as possible and to keep the timelines for identifying Gatekeepers and compliance as short as possible and reasonable.

Against this background, we understand Article 3 (8) in connection with Article 7 (2) as meaning that a Gatekeeper is to comply with all obligations laid down in Article 5 *and* 6 within six months after a core platform has been designated as a Gatekeeper - irrespective of whether the Commission specifies the measures that the Gatekeeper concerned should implement in order to comply. In other words, any need to take measures or any measures taken by the Commission pursuant to Article 7 (2) do not suspend the direct applicability of the obligations laid down in Article 6. This is a crucial pre-condition for the effectiveness of the DMA.

The "*regulatory dialogue*"[54] envisaged in Article 7 (2) must be limited to an *option for the Commission* to clarify some elements of the statutory obligations. It must not amount to an *option for the Gatekeeper* to postpone compliance by skilfully playing dumb in order to involve the Commission in time-consuming and staff-consuming dialogues about technicalities or other red herrings. In addition, the obligations set out in Articles 5 and 6 must continue to apply during this process.

Furthermore, we see that Article 7 (1) and (7) implies that there could be an *a priori* conversation with the European Commission before obligations set out in Article 5 and 6 apply. This does not grant sufficient legal clarity in terms of timing. As a whole, we would therefore recommend that the co-legislators clarify that all obligations are immediately applicable without any room for delay triggered by the Gatekeeper.

Finally, it is insufficient that only the Gatekeeper is entitled to request a proceeding to determine whether its measures are sufficient. It appears more important that businesses harmed by a Gatekeeper's insufficient implementation of the obligations laid down in Article 6 are entitled to request measures by the Commission.

Article #	Proposed Regulation, suggested deletion (strike through) and new insertions
Article 7	1. The measures implemented by the Gatekeeper to ensure compliance with the obligations laid down in Articles 5 and 6 shall be effective in achieving the objective of the relevant obligation. The Gatekeeper shall ensure that these measures are implemented in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC, and with legislation on cyber security, consumer protection and product safety. 2. Where the Commission finds that the measures that the Gatekeeper intends to implement pursuant to paragraph 1, or has implemented, do not ensure effective compliance with the relevant obligations laid down in Article 6, it may by decision specify the measures that the Gatekeeper concerned shall implement. The Commission shall open proceedings immediately after been made aware of any potentially inefficiencies and adopt ~~***such***~~ a decision within six months from the opening of proceedings pursuant to Article 18.

[54] See recital (29).

	3. Paragraphs 2 and 7 of this Article are ~~is~~ without prejudice to Article 3 (8) and the powers of the Commission under Articles 25, 26 and 27. 4. In view of adopting the decision under paragraph 2, the Commission shall communicate its preliminary findings within three months from the opening of the proceedings. In the preliminary findings, the Commission shall explain the measures it considers to take or it considers that the provider of core platform services concerned should take in order to effectively address the preliminary findings. 5. In specifying the measures under paragraph 2, the Commission shall ensure that the measures are effective in achieving the objectives of the relevant obligation and proportionate in the specific circumstances of the Gatekeeper and the relevant service. 6. For the purposes of specifying the obligations under Article 6(1) points (j) and (k), the Commission shall also assess whether the intended or implemented measures ensure that there is no remaining imbalance of rights and obligations on business users and that the measures do not themselves confer an advantage on the Gatekeeper which is disproportionate to the service provided by the Gatekeeper to business users. 7. Without prejudice to Article 3 (7), a gatekeeper as well as any business affected by its conduct may request the opening of proceedings pursuant to Article 18 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. A Gatekeeper may, with its request, provide a reasoned submission to explain in particular why the measures that it intends to implement or has implemented are effective in achieving the objective of the relevant obligation in the specific circumstances.

CHAPTER IV – MONITORING AND ENFORCEMENT

The competition investigations that the European Commission has carried out in the digital sphere during the previous decade have clearly demonstrated that any material duties and prohibitions are only as effective as the institution that enforces them. In this respect, ACT has identified several serious shortcomings of the DMA.

Call for a complaints proceeding and provisions on private enforcement

For reasons of effectiveness, the DMA needs to include a clear commitment to the private enforceability of the obligations laid down in Articles 5 and 6 before national courts. Currently, the DMA conveys no rights to affected business users, end users or competitors to request any investigation into any observed non-compliance. This is regrettable as experience shows that the affected market participants are best positioned and capable of identifying malpractices. Businesses harmed by non-compliance should be entitled to turn to both public enforcement authorities and national civil courts[55].

To this end, it should be clarified that, despite the "regulatory dialogue" pursuant to Article 7 (2) and the discretion of the Commission to suspend or even exempt obligations pursuant to Article 8 and 9, the obligations laid down in Articles 5 and 6 convey subjective rights to affected parties that can be enforced directly in private courts once such obligations become binding pursuant to Article 3(8) and as long as the Commission has not relieved the Gatekeeper from any such obligations pursuant to Articles 7-9. It should be

[55] BEUC, Position Paper, Digital Markets Act Proposal, 2021, p. 17; *Podszun/Bongartz/Langenstein*, ibid., p. 9; *Cabral/Haucap/Parker/Petropoulus/Valletti/Van Alstyne*, The EU Digital Markets Act: A Report from a Panel of Economic Experts, 2021, p. 14.

clarified that such private enforcement covers both claims for injunctive relief as well as damages in line with the Damages Directive 2014/104/EU[56]. In addition, it should be clarified that business users affected by any conduct of a gatekeeper have the right to submit formal complaints about gatekeepers' non-compliance with the obligations laid down in Article 5 and 6 DMA. They should also be heard in the decision-making process of the enforcement authorities[57].

Tools of the enforcement authorities

ACT would also recommend further tactical strengthening the regulatory toolkit available to the public enforcement authorities. The competition cases regarding Google's non-compliance have demonstrated the high degree of information asymmetry between digital Gatekeepers and enforcement authorities. To reduce such asymmetry the enforcement authorities must be equipped with powerful tools to create the transparency and technical know-how necessary to detect and effectively condemn acts of non-compliance. To this end, the co-legislators should consider embedding independent auditors, appointed by the regulatory authority, within the Gatekeeper in order to have continuous and direct access to the data and algorithm(s) and run behavioural experiments to evaluate the algorithm(s) and use of the data[58].

We are also cautious as regards the ability of the Commission to request information (Art. 19), conduct interviews and take statements (Art. 20) and conduct on-site inspections (Art. 21). Whether Articles 19, 20 and 21 apply exclusively to undertakings that have been designated Gatekeepers and their associations seems unclear. We encourage the co-legislators to consider limiting these actions to undertakings that have been designated as Gatekeepers. We are also cautious with regards to the potential implication of association of undertakings in this process, given the targeted nature of the Regulation.

CONCLUDING REMARKS

ACT supports the European endeavours to effectively address the serious harms caused by the largely uncontrolled intermediation power of digital Gatekeepers over end users and business users. Despite its shortcomings, in particular as regards advertising markets and the enforcement mechanism, overall the DMA is a helpful piece of legislation that can be improved to meet its stated goals, and could thus serve as an example for the international community.

[56] *Podszun/Bongartz/Langenstein*, Proposals on how to improve the Digital Markets Act, Febr. 2021, p. 9.
[57] BEUC, Position Paper, Digital Markets Act Proposal, 2021, p. 12.
[58] *Cabral/Haucap/Parker/Petropoulus/Valletti,Van Alstyne*, The EU Digital Markets Act: A Report from a Panel of Economic Experts, 2021, p. 28-29.