DMA – Questions raised by Article 5 and 6

Evidence and effect of the obligations

Many of the obligations appear to be inspired by learnings derived from specific antitrust cases, developed in a very specific context pursuant to extensive market analysis related to conduct adopted by a specific company. Some of these obligations relate even to conduct subject to current investigations that have not been finalised, let alone tested in court. Has the EC sufficiently assessed the effect of imposing these obligations on a broader set of services providers, delivering different services and operating different business models? Should the EC preclude the ending of such investigations – which could equate to take sides in a commercial dispute – and apply these conclusions to a broader set of actors?

It is highly questionable to qualify, as the EC proposes to do, these obligations in a "*per se*" manner, with automatic applicability. Whilst arguably raising issues of contestability and fairness, each of the listed conduct may also generate positive effects on several other fronts. It is thus unclear whether the EC has taken into consideration the impact of each obligation beyond its (sometimes untested) effect on contestability and "fairness", such as the effect on:

- consumers: will it impact user preference, user safety, user privacy, security?
- business users: will the obligation help all business users or only a subsection of those? Will it impact SMEs more than bigger business users?
- the platform: does the obligation fit all services and business models? How will the obligations impact the platform's incentives? Will the obligations lead to service providers choosing alternative business models and will these models be preferable?
- innovation: will the obligation create the right incentives for entrepreneurs to innovate and to invest in improving existing and future assets?

For each obligation, the EC should clarify its intention, and explain that *on balance*, the public interests in general will be better served by imposing such *per se* obligations. Specific questions linked to specific obligations can be find below.

Difference between article 5 and 6

The EC expects the gatekeeper to comply with all the obligations outlined in Articles 5 and 6 ex ante. The DMA offers the possibility to specify how gatekeepers can comply with article 6, but only in the context of its investigative powers, where the EC can impose a specific solution on the gatekeeper.

Some of the obligations, particularly those outlined in article 6, are highly intrusive, may lead to very complex technical changes, or are very difficult if not impossible to comply with upfront. Proportionality to the policy goals is mentioned briefly in Recital 33, yet Recital 35 stresses that no other measure would achieve the same result. Recital 23 explicitly rejects the use of economic grounds to demonstrate efficiencies to justify a specific behaviour. In effect, the gatekeeper has very limited if no opportunity to demonstrate the user and consumer benefits – include economic efficiencies – of its legitimate business practices.

- Does the EC expect that many gatekeepers will seek specification under Article 7.2?
- Given the diversity of business models, services and user interests, should there be a clearer differentiation between article 5 – focused on evidence-based, undeniable unfair commercial practices, where contestability objectives clearly and unquestionably outweigh any other objectives – and article 6 – to be applied in a tailored manner on a case-by-case basis?

- Does the need to ensure a certain degree of speed, given the frustration with antitrust enforcement, be at the expense of a more detailed, reasoned analysis of the effect of an obligation? Does this run the risk of unintended consequences in the market? Could a case-by-case analysis, bolstered by regulatory dialogue, not achieve more proportionate effects, within an appropriate time-frame to avoid the downsides of existing antitrust enforcement?
- Why does the EC reject even the possibility of gatekeepers to provide objective justifications, in order for gatekeepers to clarify trade-offs and incentives? On what basis does the EC have sufficient comfort and certainty that the listed conduct should always, in all circumstances, be either prohibited or required?
- Is the reference to proportionality recital 33 sufficient to ensure legal certainty, and should it only be linked to the objectives of Article 1.1? Shouldn't the gatekeeper be able to clarify how the practice meets or is relevant to pursue other EU policy objectives, such as user safety, privacy, security, avoiding harmful or illegal online content, and innovation?

The draft proposal mentions the importance of regulatory dialogue to specify the application of obligations, particularly those outlined in article 6. However, the parameters and principles framing such dialogue are not defined in the draft regulation. Yet, given the complexity of targeted markets, the asymmetric nature of the regulation and the clear potential for unintended harmful consequences of certain of these obligations, developing effective proportionate and predictable procedures and an environment of trust will be key ensuring positive regulatory outcomes.

- How does the EC foresee such regulatory dialogue to take place in practice? Should there be space to continuous dialogue, outside investigatory proceedings outlined in Article 18, to create a more participative approach to regulation?

Questions raised by specific Article 5 obligations:

5(a) Limits on Personal Data Tracking:

- What specific harm this obligation seeks to address? Does the reference to user consent refer to both parts of the sentence? In such case, would a reliance on consent be sufficient to address this harm?
- Very specific instances of personal data tracking can be positive for consumers in order to support customer services across an ecosystem. Will these instances be impacted by this obligation?

5(c) Prohibition of anti-steering:

- What specific harm this obligation seeks to address?
- Anti-circumvention clauses are a regular feature of commission-based business models, in order to prevent free-riding. This model does not prevent the business user from offering better offers or advertise them outside of the platform in question. Should the DMA allow free-riding, regardless of the size of the service-provider and the market strength of the business user?
- Certain platforms review all third-party service/content before distributing it, in ways that fulfill the goals of the DSA (reduce exposer to illegal content, impact on fundamental rights). What would be the responsibility of the core service provider, if the business user sells illegal content/services or fraudulent services to a consumer found through the core service but steered outside of the platform? How will that impact consumer behaviour?

- Given the potential impact of this obligation on user safety and on a company's incentive to invest, should this obligation be moved to article 6?
- What is illegal offline, should be illegal online. Conversely, what is legal offline, should be legal online. Why would it be appropriate to consider the article 5 c obligation also a binding per se requirement in the offline world? Would it not be appropriate for a brick and mortar retail store to not allow its business supplier to encourage customers in the retail store to purchase its products elsewhere, outside of the store?

Questions raised by specific Article 6 obligations:

6.1(b) un-install pre-install apps

- Most OS provides allow pre-installed apps to be uninstalled. However, some apps are essential to the functioning of the software and hardware or are key to ensure that it remains functional during the device's life-cycle – even when these services are offered by third parties.
- The caveat around apps that are essential to the functioning of the OS and device is useful. Can the EC clarify what it means by "which cannot technically be offered on a standalone basis by third-parties"? What does "technically offered" mean?

6.1(c) Side-loading and alternative app stores

- Has the EC fully considered the effect of this obligation from a security, privacy and user experience perspective? Does this take into consideration existing competitive pressure and alternative modes of distribution both on and off the core service provider?
- An app store review usually goes beyond protecting the integrity of the platform, to enable high levels of security, privacy and protect the overall performance of the platform. They can support data minimisation and ensure high levels of user control over the data generated by their devices. Can EC offer concrete examples of appropriate measures to protect the integrity of an OS? Are such "appropriate measures" sufficient to protect user data privacy and security and device performance?
- Why would the EC preclude the possibility for a gatekeeper to refuse side-loading or the installation of alternative app stores when this installation would harm the privacy, security and safety interests of the gatekeeper's customers?
- Shouldn't such intrusive and difficult to balance remedy be left to antitrust enforcement?

6.1(e) Consumer Switching

- What specific harm this obligation seeks to address?
- "Internet access provider" is not defined in the law. Does the EC refer to "internet access service" as defined in the contest of article 2.2 of Regulation (EU) 2015/2120?

6.1(f) Ancillary service interoperability

- Providing access to technical functionalities can raise complex engineering challenges, in order to ensure that the functionality in question is sufficiently stable to be used as an economic opportunity by third parties, does not impact the integrity of the operating system, and delivers the necessary user protection in terms of security and privacy.
- Has the EC taken into consideration these challenges when including this obligation?

6.1(h) Data portability and 6.1(i) Business user data access.

- Can the EC clarify what it means by “continuous” and “real time access”, and what is the goal of such access? Is this approach proportionate to all instances of user data portability and business user data access outlined in the relevant obligations?
- GDPR requires service providers to verify the identity of the user before processing data access request. How will obligation 6.1(h) work in practice?
- Giving access to non-aggregated data and data that is generated in the context of the use of the relevant core platforms services may raise privacy and IP challenges. Furthermore, some platforms only gather that data on an anonymised basis. Has the EC considered those challenges, and the effect of such data access may have on good privacy practices?
- Is the definition of business user in Article 2.17 sufficiently precise, given that it could cover business user that have no formal relationship with the core service provider?

6.1(k) Fair and non-discriminatory access to application stores.

- What is fair to one set of users may be perceived as unfair to others. How will the EC assess fairness, beyond the guidance provided in recital 57? Shouldn’t legal certainty be better promoted by clearly defining unfair commercial practices?
- Has the EC considered how a gatekeeper could, from a practical perspective, be expected to realistically comply with this obligation – which traditionally is very often the subject of heated debates and views? How will the EC determine whether the measures implemented by the gatekeeper to ensure compliance with this specific obligation laid down in Article 61(k) will be effective in achieving the objective of the relevant obligation to provide ‘fair’ and ‘non-discriminatory’ access?
- Can the EC clarify what it means by “conditions that lead to an imbalance of rights and obligations on the business user”, as referred to in Recital 57?
- Recital 57 points to the fact that similar access conditions are provided by other providers of application stores. Does this run the risk of reducing competition in the market, notably around quality, security and privacy?