This note contains our comments on the following areas: (i) the Annex on the methodology for the calculation of active (business/end) users; (ii) key Art.5 and Art. 6 obligations that need to be revisited (iii) whether or not ancillary services should be in scope, and (iv) examples showcasing the need for additional safeguards on Art. 7.

1. Annex on the methodology for the calculation of active business/end users

Para 4: We agree that for the purpose of measuring unique end users, looking at logged-in users is the most reliable way to measure unique users. For logged-out users however, it is notoriously difficult to measure unique users. The methods mentioned in the text, for instance cookies or IP addresses are not reliable for multiple reasons, for instance because of cookie churn, multiple users using the same device, same user using multiple devices etc.

Para 6: For business users, the text notes that unique users should be measured at the account level. That is not going to be an accurate metric because the same business may have multiple accounts.

Para 7: The text notes that the undertaking has the obligation to provide accurate information that avoids undercounting or over-counting. Given the practicable difficulties mentioned above, it would be helpful to qualify this by adding "to the extent possible".

Finally the annex contains metrics for cloud and advertising services. For advertising, it is questionable whether a gatekeeper can measure the number of unique users that are exposed to ads if the user does not click, especially if third party cookies get removed.

2. Article 5 and Article 6 obligations that require refinement

Article 5(a)- Personal data combination: We support rigorous protection of personal data. The proper legal instrument for that protection is the GDPR, which already provides for a high level of protection. Introducing rules on the protection of personal data in the DMA is liable to give rise to tension with the GDPR and create legal uncertainty. For example, the GDPR allows combining data across services on grounds other than user consent, such as legitimate interests or a contract. One option for a reasonable outcome would be to limit the requirement for consent to use of personal data in a service that is functionally unrelated to the core platform and where that use cannot reasonably be anticipated by a user:

- "*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, **where the service in question is functionally unrelated to the core platform service and the user cannot reasonably anticipate the data combination,** unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679*"

Article 6.1.d - Search ranking: We support principles that ensure ranking is free from artificial manipulation and provides users with relevant results. A crucial element to provide useful and relevant results is for a service to have the ability to use different formats and different algorithms for different results. A categorical ban on differentiation could lead to unintended consequences for business users, shifting for instance disproportionately web traffic from end business users (hotels, restaurants, retailers) to a handful

of aggregators. We would therefore welcome a clarification that Article 6.1.d does not apply to legitimate differentiation but rather unjustified preferencing.

- *"refrain from **unjustifiably** treating more favorably in ranking services any **distinct** products offered by the gatekeeper itself or by any third party belonging to the same undertaking compared to similar services or products of **a** third party **in a** and apply fair and non-discriminatory **and disproportionate manner.** conditions to such ranking. "*

Article 6.1.f- Interoperability and access: As developers of interoperable systems, we know that enabling interoperability can pose difficult questions and tradeoffs in terms of functionality, quality assurance, user safety, and intellectual property, for example. Critically, enabling interoperability presents different challenges for an operating system (which by design is meant to interoperate with third-party products) and application level services. We suggest clarifying Article 6(1)(f) in line with Recital 52 and provide for consideration of legitimate interests as follows:

- "***In relation to operating systems** allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features **provided or mediated by the operating system** that are available or used in the provision by the gatekeeper of any ancillary services, **provided that (i) there are no substantial technical obstacles to interoperability, and (ii) such interoperability does not unduly prejudice other legitimate interests, such as functionality, quality, product improvements, system integrity, user safety, or intellectual property.***"

Article 6.1.g- Access to search data: Anonymization alone does not necessarily protect against privacy violations (*see* a study in *Nature* by Yves Alexandre de Montjoye, one of the author's of the Commission's report into 'Competition Policy for the Digital Era'). And disclosure of search data may have other serious, harmful consequences including exposing a search service to ranking manipulation and copying of its results and search algorithms. Article 6.1.g should provide due consideration for legitimate interests that may be unduly harmed by disclosures along the following lines:

- *"provide to any third party providers of online search engines, upon their request, with access on fair, reasonable and non-discriminatory terms to **aggregated** 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 **due safeguards to protect legitimate interests, including user privacy, the integrity and security of the search service, and the protection of intellectual property.** anonymisation for the query, click and view data that constitutes personal data."*

3. Broadening of the scope of various Art.5 and Art. 6 obligations to capture "ancillary services"

The rationale of the DMA, as indicated in Article 1.2 and Article 3.1.b, is to lay down rules that apply to a gatekeeper's core platform services which "*serve as an important gateway for business users to reach end users*". Therefore it is this "*gateway function*" which is an essential element of the application of the DMA. By definition, ancillary services do not play this role.

Moreover, it is questionable whether a comprehensive definition of ancillary services can be laid down. Article 2.2(14) merely provides some examples by pointing, for instance, to payment services. Broadening the scope of the Article 5 and Article 6 provisions to an unidentified group of services will likely chill innovation as potential gatekeepers would be reluctant to roll out new features or services as they might be captured by the stringent DMA rules.

Finally, existing case law on tying provides a basis for identifying when a separate 'service' (as opposed to a mere product feature) exists. We suggest including a definition for "service" to provide guidance as to how to delineate different services in Article 2:

- "***'Service' means a standalone functionality offered by a provider that is unrelated to other***

functionalities offered by the same provider, such that there is separate, independent demand for the functionality in question. By contrast, a mere 'feature' of a product will not constitute a distinct 'service' if there is no separate demand for that feature, independent

of the main product ."

4. Examples showcasing the need for additional safeguards on Art. 7

We support comments made by Luxembourg and numerous member States that introduce additional safeguards in the implementation of the Art.5 and Art.6 obligations. Specifically, we believe that Art. 7.1 should explicitly mention that implementing measures shall be *necessary* and effective in achieving the objectives of the relevant obligation. These measures shall take into account the quality, integrity and functionality of the gatekeeper's services.

4a. Example showcasing why we need the quality of the service to be explicitly mentioned - Article 6.1.d

The implementation of a prohibition of differentiated treatment can take different forms. In Turkey, where the competition authority outlawed any differentiated treatment on search results, Google had to remove the Shopping Units. This had detrimental consequences for countless Turkish merchants, which lost traffic and now pay higher prices for promoting their offers, and harm to users for whom it is now more difficult to find relevant product offers.

Even if the regulator doesn't impose a strict prohibition on differentiated treatment, product designs can take various forms such as carousels on top or below the gatekeeper's results, choice screens, one single unit that sources information from various sources etc. An explicit mention of the "quality of the service" will force the regulator and the gatekeeper to propose flows that preserve the gatekeeper's offer while applying the DMA rule in a timely fashion.

4b. *Example showcasing why we need the integrity of the service to be explicitly mentioned - Article 6.1.j*

A high level of transparency or granularity on datasets might create a risk of reverse engineering in certain circumstances. This could be the case, for instance, if a search engine based outside of the EU (and the US) has access to specific and sensitive datasets. This case wouldn't fall under Art. 9.2.c as it doesn't not relate to *public* security but merely to the integrity of the gatekeeper's service.

4c. *Example showcasing why we need the integrity of the service to be explicitly mentioned - Article 6.1.f*

Enabling interoperability presents different challenges for an operating system (which by design is meant to interoperate with third-party products) and application level services. Allowing *any* third party provider of ancillary services -which encompasses a wide range of services- to have access and interoperate with any hardware, software or OS features could have unintended consequences in the smooth operation of the gatekeeper's service. Therefore, Article 6.1.f would require additional safeguards, akin to those under Article 6.1.c.