

# DMA - Comparative table of EC, EP and Council positions

- **Recitals 48 and 49 of the EP text, and EP Art. 6(1)(d) on equal treatment - support the Council / Commission position**
  - The EP text in Recital 48 suggests that providing equal treatment between 3P vs. gatekeeper services would not be sufficient for an equal treatment duty under Art. 6(1)(d). This addition could cause serious harm to European users and businesses by forcing gatekeepers to remove helpful results. It's also unnecessary because Art. 6(1)(d) already creates equal treatment.
  - EP proposal in Art 6(1)(d) is to extend the rule not to self-preference to "other settings" beyond ranking. This would expand the scope of the rule and mean that the rule would cover more CPSs (not just those that rank content like search engines or social media). The EP edit would fundamentally change the nature of the obligation beyond its intent – preventing manipulation in ranking – and, in turn, call into question any form of product integration.
- **Inclusion of Article 6(1)(aa) that limits ads personalization - support the Council / Commission position**
  - The determination of whether minors are able to consent to ad targeting should be addressed by privacy regulations, not rules concerned with gatekeeper practices. Pursuing social policy objectives creates a risk of misalignment and possibly conflicting rules with privacy laws. Also, any restraints on targeted ads will disadvantage publishers as their main revenue stream will be undercut (if asked, 70% of users say they are not willing to pay for news online so paywalls are not an alternative for the ads-based business model). Finally, European SMEs and consumers will also be disadvantaged. The former will struggle to reach the right audience, the latter will see less relevant ads.
- **Art. 6(1)(f) - interoperability requirements - support the modified EP position (to ensure art. 6(1)(f) applies to OSs as originally intended). Failing that, support the Council position**
  - We think the focus of this provision should be targeted at Operating Systems (OSs) which was its original intention. To this end, we propose to align the article with the corresponding recital (rec. 52). We think interoperability makes sense for specific services such as OS and communications services (please see below for more). That said, extending this provision to possibly cover all CPSs will create unintended consequences. As the CMA recognized recently, promoting interoperability is not costless: "*Interventions to require greater interoperability will involve balancing a number of considerations including the competitive and consumer benefits of overcoming network effects and the potential costs of greater homogenisation of services and risks to privacy*".
  - Currently, all 3 texts (Council, EC EP) can be interpreted to go beyond OSs. However, the EP text provides that interoperability and access must be provided for free. Providing interoperability to a large number of core services operated by the biggest platforms would come at a cost that platforms should be able to -at least partly- recuperate.
- **Art. 6(1)(k) - support the Council / Commission position:** The EP proposes to include a general access obligation (on FRAND terms) for all CPSs, not just app stores (which was in the EC's version). This is a significant extension of the obligation and may have far-reaching implications. There is also no safeguard beyond the qualifier associated with FRAND. A general access obligation risks significantly harming user safety and security (e.g., by not allowing gatekeepers to limit access to apps that contain malware in their app stores). The general access obligation also risks conflicting with the interoperability obligation in Art. 6(1)(f) and other EU legislative acts (e.g. DSA) that will require gatekeepers to moderate content (e.g. prevent misinformation / disinformation, take down illegal content, etc.).
- **Art. 5(e) - support Council / Commission position:** The EP text substantially amends Art. 5(e) so that it is no longer just about ID services, but extends it to be a straightforward ban on bundling CPSs with ancillary services. This could have severe negative consequences. F.ex. a gatekeeper operating an app store would not be able to run security checks on apps that are available in the store. It's because these checks are usually performed by an ancillary security service which is also operated by a gatekeeper. An absolute ban would cause harm, given the well-recognised efficiencies that can arise when services are provided together. In the EC's words, providing products together is a: "*common practice intended to provide customers with better products or offerings in more cost effective ways.*"
- **Art. 5(gb) - support the EP position and choice screens for all.** A last minute change in the EP draft included a provision requiring default choice screens for gatekeeper services preinstalled on operating systems (Art. 5(gb)). We see it as an amendment offering more consumer choice and therefore is something we support.
- **Art. 6(1)(fa) - support the EP position requiring interoperability for comms. services:** We can support the EP's new obligation for messaging interoperability (Art. 6(1)(fa)). The [CMA's Mobile Ecosystems Market Study Interim Report](#) supports this line of advocacy by arguing that there are currently significant barriers to switching between Android and iOS, which could be remedied by an interoperability obligation.
- **Art. 5(a) - consider introducing safeguards:** We would advocate adding the following sentence at the end of Article 5(a): "*This requirement does not apply to gatekeepers combining such data for the purposes of detecting/combatting fraud, abuse, or other safety-related activity, or where compelled by law.*" This ensures gatekeepers can perform data combinations aimed at protecting consumers' security online.

- **Support a general proportionality clause.** While there was a proposal for a proportionality clause in the ECON Committee draft, it did not make it into the final EP version. Although none of the EC, Council, or EP texts include a safeguard, there is still support from academics, judges, practitioners, and industry. Given the value that a proportionality clause would have, this is the one area where we think it is worth continuing to push.

	EC text	Council text	EP text	Our Recommendations
<b>Recital 48</b>	<p>(48) Gatekeepers are often vertically integrated and offer certain products or services to end users through their own core platform services, or through a business user over which they exercise control which frequently leads to conflicts of interest. This can include the situation whereby a gatekeeper offers its own online intermediation services through an online search engine. When offering those products or services on the core platform service, gatekeepers can reserve a better position to their own offering, in terms of ranking, as opposed to the products of third parties also operating on that core platform service. This can occur for instance with products or services, including other core platform services, which are ranked in the results communicated by online search engines, or which are partly or entirely embedded in online search engines results, groups of results specialised in a certain topic, displayed along with the results of an online search engine, which are considered or used by certain end users as a service distinct or additional to the online search engine. Other instances are those of software applications which are distributed through software application stores, or products or services that are given prominence and display in the newsfeed of a social network, or products or services ranked in search results or displayed on an online marketplace. In those circumstances, the gatekeeper is in a dual-role position as intermediary for third party providers and as direct provider of products or services of the gatekeeper. Consequently, these gatekeepers have the ability to undermine directly the contestability for those products or services on these core platform services, to the detriment of business users which are not controlled by the gatekeeper.</p>	<p>(48) Gatekeepers are often vertically integrated and offer certain products or services to end users through their own core platform services, or through a business user over which they exercise control which frequently leads to conflicts of interest. This can include the situation whereby a gatekeeper offers its own online intermediation services through an online search engine. When offering those products or services on the core platform service, gatekeepers can reserve a better position to their own offering of <b>online intermediation services, online social networking services or video-sharing platform services</b>, in terms of ranking, as opposed to the products of third parties also operating on that core platform service. This can occur for instance with products or services, including other core platform services, which are ranked in the results communicated by online search engines, or which are partly or entirely embedded in online search engines results, groups of results specialised in a certain topic, displayed along with the results of an online search engine, which are considered or used by certain end users as a service distinct or additional to the online search engine. Other instances are those of software applications which are distributed through software application stores, or products or services that are given prominence and display in the newsfeed of a social network, or products or services ranked in search results or displayed on an online marketplace. In those circumstances, the gatekeeper is in a dual-role position as intermediary for third party providers <b>undertakings</b> and as <b>direct provider of undertaking directly providing</b> products or services of the gatekeeper. Consequently, these gatekeepers have the ability to undermine directly the contestability for those products or services on these core platform services, to the detriment of business users which are not controlled by the gatekeeper.</p>	<p>(48) Gatekeepers are often vertically integrated and offer certain products or services to end users through their own core platform services, or through a business user over which they exercise control which frequently leads to conflicts of interest. This can include the situation whereby a gatekeeper offers its own online intermediation services through an online search engine. When offering those products or services on the core platform service, gatekeepers can reserve a better position to their own offering, in terms of ranking, as opposed to the products of third parties also operating on that core platform service. This can occur for instance with products or services, including other core platform services, which are ranked in the results communicated by online search engines, or which are partly or entirely embedded in online search engines results, groups of results specialised in a certain topic, displayed along with the results of an online search engine, which are considered or used by certain end users as a service distinct or additional to the online search engine. <b>Such preferential or embedded display of a separate online intermediation service should constitute a favouring irrespective of whether the information or results within the favoured groups of specialised results may also be provided by competing services and are as such ranked in a non-discriminatory way.</b> Other instances are those of software applications which are distributed through software application stores, or products or services that are given prominence and display in the newsfeed of a social network, or products or services ranked in search results or displayed on an online marketplace. In those circumstances, the gatekeeper is in a dual-role position as intermediary for third party providers and as direct provider of products or services of the gatekeeper <b>leading to conflicts of interest.</b> Consequently, these gatekeepers have the ability to undermine directly the contestability for those products or services on these core platform services, to the detriment of business users which are not controlled by the gatekeeper.</p>	<p><b>Recommendation: Support the Council / Commission position</b></p> <ul style="list-style-type: none"> <li>• The EP Recital is disproportionate. This objective of equal treatment and avoiding artificial manipulation can be achieved by implementing equal treatment of 1P and 3P services within units.</li> <li>• The Recital could cause serious harm. If GKs cannot create equal treatment by giving business users equal access, then it may damage users and businesses who lose helpful designs that help them find information and send valuable traffic to businesses.</li> <li>• The DMA's objective of preventing artificial manipulation of ranking can be achieved without the EP's additions to Recital 48. Art 6(1)(d) will still set out an obligation of equal treatment.</li> </ul> <p>In terms of the Recital to support, the Council version is better than the EP version because it refers to favoring of distinct OISs, social networks, and video-sharing platform services, rather than the vaguer "offering".</p>
<b>Recital 49</b>	<p>(49) In such situations, the gatekeeper should not engage in any form of differentiated or preferential treatment in ranking on the core platform service, whether through legal, commercial or technical means, in favour of products or services it offers itself or through a business user which it controls. To ensure that this</p>		<p>(49) In such situations, the gatekeeper should not engage in any form of differentiated or preferential treatment in ranking on the core platform service, whether through legal, commercial or technical means, in favour of products or services it offers itself or through a business user which it controls. To ensure that this obligation is effective, it should also be ensured that the conditions that apply to such</p>	<p><b>Recommendation: Support the Council / Commission position</b></p> <p>The EP's text seeks to require gatekeepers to treat their services as commercially viable standalone services. That could have negative consequences for GKs in terms of</p>

	obligation is effective, it should also be ensured that the conditions that apply to such ranking are also generally fair. Ranking should in this context cover all forms of relative prominence, including display, rating, linking or voice results. To ensure that this obligation is effective and cannot be circumvented it should also apply to any measure that may have an equivalent effect to the differentiated or preferential treatment in ranking. The guidelines adopted pursuant to Article 5 of Regulation (EU) 2019/1150 should also facilitate the implementation and enforcement of this obligation. 34		ranking are also generally fair. Ranking should in this context cover all forms of relative prominence, including display, rating, linking or voice results. To ensure that this obligation is effective and cannot be circumvented it should also apply to any measure that may have an equivalent effect to the differentiated or preferential treatment in ranking. <b>In addition, to avoid any conflicts of interest, gatekeepers should be required to treat its own product or services, as a separate commercial entity that is commercially viable as a stand-alone service.</b> The guidelines adopted pursuant to Article 5 of Regulation (EU) 2019/1150 should also facilitate the implementation and enforcement of this obligation.	launching and showing new services.  The objective of equal treatment can be achieved without the requirement for separate products or services to be treated as a “ <i>separate commercial entity that is commercially viable as a standalone service</i> ”. That could have unintended consequences by unintentionally outlawing any kind of vertical integration, which benefit users.  In particular, the requirement for commercial viability could severely hamper innovation. Many new products and companies that consumers value are not “ <i>commercially viable as a standalone entity</i> ” for many years, like AirBnB, Uber, DropBox, Lyft, Peloton, Snap. This Rectial would risk banning gatekeepers from launching useful innovations that would benefit users.
<b>Article 5 - Obligations for gatekeepers</b>	In respect of each of its core platform services identified pursuant to Article 3(7), a gatekeeper shall:	In respect of each of its core platform services identified in the <b>designation decision</b> pursuant to Article 3(7), a gatekeeper shall:	In respect of each of its core platform services identified pursuant to Article 3(7), a gatekeeper shall:	
<b>Article 5 (a)</b>	(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 and provided consent in the sense of Regulation (EU) 2016/679. ;	(a) <del>refrain from combining</del> <b>not combine</b> personal data sourced from <del>these any of its these</del> core platform services with personal data from any <del>other further core platform service or other services further services</del> offered by the gatekeeper or with personal data from third-party services, and <del>not from signing in</del> 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 and provided consent in the sense of <b>Article 6(1) point (a)</b> of Regulation (EU) 2016/679. <b>The gatekeeper may also rely on the legal basis included under Article 6(1) points (c), (d) and (e) of Regulation (EU) 2016/679, where applicable;</b>	(a) refrain from combining <b>and cross-using</b> 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 <b>in a explicit and clear manner</b> , and <b>has</b> provided consent in the sense of Regulation (EU) 2016/679;	<b>Recommendation: Support the Council position</b>  The Council text offers a clearer legal basis for data processing.  If possible we'd like to add the following sentence at the end of Article 5(a) which would ensure that data processing aiming at protecting users online is not compromised: “ <b><i>This requirement does not apply to gatekeepers combining such data for the purposes of detecting/combatting fraud, abuse, or other safety-related activity, or where compelled by law.</i></b> ”
<b>Article 5 (e)</b>	(e) refrain from requiring business users to use, offer or interoperate with an identification service of the gatekeeper in the context of services offered by the business users using the core platform services of that gatekeeper;	(e) refrain from requiring business users <b>or end users</b> to use, <b>and in the case of business users, also to</b> offer or interoperate with, an identification <b>or payment</b> service of the gatekeeper in the context of services offered by the business users using the core platform services of that gatekeeper;	(e) refrain from requiring business users to use, offer or interoperate with an identification service <b>or any other ancillary service</b> of the gatekeeper in the context of services offered by the business users using the core platform services of that gatekeeper;	<b>Recommendation: Support the Commission / Council text</b>  The Council and EP texts expand the obligation to payment services (Council) and ancillary services (EP). These amendments seem to introduce an absolute ban on bundling ancillary services vis-à-vis businesses, which would have serious implications.  The EP version imposes an absolute ban on bundling any service together with a CPS. Such an absolute ban could have serious downsides for consumers because it is well recognized that selling services as a bundle is, in the EC's words, a “ <i>common practice intended to provide customers with better products or offerings in more cost effective ways.</i> ” An absolute ban on bundling would severely harm competition and innovation by overlooking the benefits that arise when companies bundle their

				<p>services.</p> <p>Also, services sometimes need to be distributed together to ensure the functioning of the CPS and to protect user safety. F. ex. an app store operator would also run an ancillary security service that would perform security checks on apps listed in the store. If the rule would be expanded, it would need to include safeguards to protect against security and privacy risks.</p>
<b>Article 5 (gb)</b>			<p><b>(ga) from the moment of end users' first use of any pre-installed core platform service on an operating system, prompt end-users to change the default settings for that core platform service to another option from among a list of the main third-party services available, and allow and technically enable end users to uninstall pre-installed software applications on a core platform service at any stage without prejudice to the possibility for a gatekeeper to restrict such un-installation in relation to software applications 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;</b></p>	<p><b>Recommendation: support the EP position and move the proposed provision to art. 6 to allow for regulatory dialogue about implementation</b></p> <p>We support the EP new obligation requiring gatekeepers to prompt end-users to offer default setting prompts for pre-installed apps. It offers more consumer choice which is a positive development. That said, we would suggest moving this provision to art. 6 to allow for a regulatory dialogue about how exactly this provision should be implemented.</p>
<b>Article 6 - Obligations for gatekeepers susceptible of being further specified</b>	Obligations for gatekeepers susceptible of being further specified	Obligations for gatekeepers susceptible of being further specified <b>under Article 7</b>	Obligations for gatekeepers susceptible of being further specified	
			<p><b>aa) for its own commercial purposes, and the placement of third-party advertising in its own services, refrain from combining personal data for the purpose of delivering targeted or micro-targeted advertising, except if a clear, explicit, renewed, informed consent has been given to the gatekeeper in line with the procedure foreseen in the Regulation (EU) 2016/679 by an end-user that is not a minor.</b></p>	<p><b>Recommendation: Support the Council / Commission position (i.e. no restraints on targeted ads)</b></p> <p>This new rule conflates competition and privacy objectives. The determination of whether minors are able to consent to ad targeting should be addressed by privacy regulations, not rules concerned with gatekeeper practices. Pursuing social policy objectives creates a risk of misalignment and possibly conflicting rules with privacy laws.</p> <p>It has also been shown that the ability to show targeted ads can enhance consumer welfare by incentivising platforms to deliver greater value to users and enabling platforms to offer lower prices and transaction costs (e.g., Langus and Lipatov, "<a href="#">Value creation by ad funded platforms</a>," p.10).</p>
<b>Article 6 (1) d</b>	(d) refrain from treating more favourably in ranking services and products offered by the gatekeeper itself or by any third party belonging to the same undertaking compared to similar	(d) refrain from treating more favourably in ranking services and products offered by the gatekeeper itself <del>or by any third party belonging to the same undertaking</del> compared to similar services or products of third party and apply fair and non-discriminatory	(d) <del>refrain from treating</del> <b>not treat</b> more favourably in ranking <b>or other settings</b> , services and products offered by the gatekeeper itself or by any third party belonging to the same undertaking compared to similar services or products	<b>Recommendation: Support the Council / Commission position</b>

	<p>services or products of third party and apply fair and non-discriminatory conditions to such ranking;</p>	<p>conditions to such ranking;</p>	<p>of third party and apply <b>transparent</b>, fair and non-discriminatory conditions to such <b>third party services or products</b> ranking;</p>	<p>The EP's proposal to extend the rule to not self-preference to "other settings" beyond ranking obligation significantly widens the scope of Article 6(1)(d). This may extend the rule to cover default settings on CPSs that are not ranking services.</p> <p>It risks dramatically changing the scope and intention of the Article. The rule is about favoring in ranking: when the purpose of the service is to present a non-manipulated list to users so they can choose. By contrast, a broad ban on any form of different treatment in "other settings" is so vague as to be almost impossible to understand. And it risks causing harm by calling into question any form of vertical integration that benefits consumers.</p> <p><b>On top of that, we'd like to put forward the following amendment that would clarify the scope of Article 6(1)(d)</b></p> <p>"Gatekeepers shall "refrain from treating, <b>without justification</b>, more favourably in ranking services any 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 <b>in a and apply fair and non-discriminatory and disproportionate manner. conditions to such ranking.</b>"</p> <p>The proposed amendments allows for legitimate and justified differentiated treatment of results, which has been proved to tremendously improve user experience while providing a solution compliant with the general principles of proportionality.</p>
<p><b>Article 6 (1) f</b></p>	<p>(f) allow business users and providers of 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 ancillary services;</p>	<p>(f) allow business users and <del>providers of</del> <b>undertaking providing</b> 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 ancillary services. <b>In these cases, access and interoperability conditions shall be fair, reasonable and non-discriminatory. The gatekeeper shall not be prevented from taking to the extent strictly necessary and proportionate measures to ensure that third party ancillary services do not endanger the integrity of the operating system, hardware or software features provided by the gatekeeper, provided that such proportionate measures are duly justified by the gatekeeper;</b></p>	<p>(f) allow business users, <del>and</del> providers of services <b>and providers of hardware ancillary free of charge</b> access to and interoperability with the same <b>hardware and software features accessed or controlled via an</b> operating system, <del>hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services</del> <b>provided that the operating system is identified pursuant to Article 3(7), that are available to services or hardware provided by the gatekeeper. Providers of ancillary services shall further be allowed access to and interoperability with the same operating system, hardware or software features, regardless of whether those software features are part of an operating system, that are available to ancillary services provided by a gatekeeper.</b> The gatekeeper shall not be prevented from taking indispensable measures to ensure that interoperability does not compromise the integrity of the operating system, hardware or software features provided by the gatekeeper or undermine end-user data protection or cyber security provided that such indispensable measures are duly justified by the gatekeeper.</p>	<p><b>Recommendation: Support the EP position provided the sentence that extends the obligation beyond OSs (highlighted in yellow) is removed . Failing that, support the Council position.</b></p> <p>The EP final text (a) goes beyond OSs, and (b) mandates that access and interoperability must be free. Those shortcomings can be rectified by removing the sentence highlighted in yellow which will revert the scope of this provision to OSs as originally intended.</p> <p>The original focus of this provision is on OSs which is also reflected in the corresponding recital (Recital 52)</p> <p>A rule encouraging interoperability, accompanied by reasonable safeguards, for OSs makes sense. As currently phrased, all 3 texts (Council, EC, EP) might be interpreted to provide interoperability for all CPSs. This risks causing serious harm:</p> <ul style="list-style-type: none"> <li>○ "Interventions to require greater interoperability will involve balancing a number of considerations including the</li> </ul>

				<p>competitive and consumer benefits of overcoming network effects and the potential costs of greater homogenisation of services and risks to privacy” (<a href="#">CMA Online Platforms and Digital Advertising Market Study Final Report</a>)</p> <ul style="list-style-type: none"> <li>○ “the policy objective should not be full or maximum interoperability, but rather an optimal degree of interoperability that balances benefits and costs” (<a href="#">Article</a> by Prof. Dr. Wolfgang Kerber and Prof. Dr. Heike Schweitzer)</li> </ul> <p>The EP text helpfully includes the widest safeguards (integrity of the service, data protection, and cybersecurity). That said, the EP text stipulates that interoperability and access must be provided for free. Providing interoperability to a large number of core services operated by the biggest platforms would come at a cost that platforms should be able to -at least partly- recuperate.</p>
			<p><b>(fa) allow any providers of number independent interpersonal communication services upon their request and free of charge to interconnect with the gatekeepers number independent interpersonal communication services identified pursuant to Article 3(7). Interconnection shall be provided under objectively the same conditions and quality that are available or used by the gatekeeper, its subsidiaries or its partners, thus allowing for a functional interaction with these services, while guaranteeing a high level of security and personal data protection. [PROPOSED ADDITION: In addition, to the extent that a service can be used as both a number-based interpersonal communication service and a number-independent interpersonal communication service, the entirety of the service shall be subject to the interoperability obligations].</b></p>	<p><b>Recommendation: support the EP position with the proposed addition to close possible loopholes</b></p> <p><b>Support the EP text including an obligation for providers of number independent comms. services (NIICs) to provide interoperability.</b></p> <p>Recently published <a href="#">CMA’s Mobile Market Study Interim Report</a> supports interoperability of NIICs. The CMA notes that:</p> <p>“Users may have a worse experience of interacting with friends’ and family’s Apple devices after switching. For instance, Android users sending number-based interpersonal messages to iOS users will reach the iOS device via Short Message Service (SMS) / Multimedia Messaging Service (MMS) technology, because Apple has not adopted the Rich Communications Standards (RCS) protocol for iMessage. By contrast, iOS users may send number-based messages to other iOS users via a faster, encrypted iMessage service that permits functionality (eg message effects) unavailable when communicating with an Android user. In response to the CMA’s questions, we heard that Apple’s practices impair communications sent between non-iOS device users and iMessage users via SMS / MMS. Apple suggested that it has not adopted the RCS protocol for number-based messaging because RCS is a new technology and it is unclear how effective it will be. Apple noted that alternative third-party messaging services are available on Android and iOS. Parties also reported that iOS users may also need to manually disable iMessage, via their iOS device or online, to be able to receive messages sent to their number on an Android</p>

				<p>device”</p> <p>The CMA went on to suggest this this locks in users to iOS which can harm users:</p> <ul style="list-style-type: none"> <li>• “the unavailability of apps such as iMessage on other operating systems is likely to contribute to other barriers to switching, set out below”</li> <li>• “The diminished experience of interacting with friends’ and family’s Apple devices after switching – and features of iMessage in particular – also pose barriers to switching”</li> </ul> <p>The CMA proposed that a potential remedy would be “allowing Apple’s first-party apps (eg iMessage) and connected devices (eg the Apple Watch) to interoperate fully with equivalent features of Android devices.”</p>
<p><b>Article 6 (1) k</b></p>	<p>(k)apply fair and non-discriminatory general conditions of access for business users to its software application store designated pursuant to Article 3 of this Regulation.</p>	<p>(k)apply fair, <b>reasonable</b> and non-discriminatory general conditions of access for business users to its software application store designated pursuant to Article 3 of this Regulation.</p>	<p>(k) apply <b>transparent</b>, fair, <b>reasonable</b> and non-discriminatory general conditions of access <b>and conditions that are not less favourable than the conditions applied to its own service</b> for business users to <b>its core platform services</b> <del>its software application store</del> designated pursuant to Article 3 of this Regulation</p>	<p><b>Recommendation: Support the Council / Commission position</b></p> <p><b>The EP text that creates a general access obligation for all CPSs.</b> The EP proposes to include a general access obligation (for FRAND) for all CPSs, not just app stores (which was in the EC’s version). This is a significant extension of the obligation and may have far-reaching implications. There is also no safeguard beyond the qualifier associated with FRAND.</p> <p>A general access obligation proposed by the EP risks significantly harming user safety and security. Gatekeepers should be able to limit access to their services to ensure a safe environment for their users (e.g., by limiting access to the app store when an app contains malware).</p> <p>Additionally, this new obligation potentially is likely to be in conflict with EU legislation requiring tech companies to curtail dis- / mis-information, take down illegal content, etc. An unlimited fair access requirement would legally oblige certain platforms such as search engines and social media to carry all kinds of content, no matter its quality, social impact or trustworthiness.</p> <p>Finally, a fair access / must-carry obligation would be a de-facto revision of the copyright (EUCD) directive which already specifies the conditions for carrying publishers’ content by Internet companies. The EUCD should be fully transposed by all EU countries and its effectiveness rigidly assessed before new laws are proposed.</p>