

**Compromise Amendment E**

**on compliance replacing all relevant amendments, including AM 7-18, 51-65, 592-838,  
951-970, 971-976**

*Article 5*

*Obligations for gatekeepers*

In respect of each of its core platform services identified pursuant to Article 3(7), a gatekeeper shall:

- (a) refrain from combining ***and cross-using*** 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 ***in a explicit and clear manner***, and has provided consent in the sense of ~~*Article 6 (1) point (a) of Regulation (EU) 2016/679;*~~ ***alternatively, the gatekeeper may rely on the legal basis provided for in included under Article 6 (1) of that Regulation (EU) 2016/679 with the exception of lit points (b) and (f) thereof of Article 6 (1) of Regulation (EU) 2016/679.***
- (b) ~~***allow refrain from applying contractual obligations that prevent business users to offer from offering***~~ the same products or services to end users through third party online intermediation services ***or through their own direct online sales channel*** at prices or conditions that are different from those offered through the online intermediation services of the gatekeeper;
- (c) allow business users to ***communicate and promote different*** offers ***including under different purchasing conditions*** to end users acquired via the core platform service ~~***with which business user is in contractual relationship and for which the core platform service has been remunerated or through other channels***~~, and to conclude contracts with these end users ***or receive payments for services provided outside regardless of whether they use for that purpose*** the core platform services of the gatekeeper, ~~***and allow end users to access and use, through the core platform services of the gatekeeper, content, subscriptions, features or other items by using the software application of a business user, where these items have been acquired by the end users from the relevant business user without using the core platform services of the gatekeeper;***~~
- (ca) ***allow end users to access and use, through the core platform services of the gatekeeper, content, subscriptions, features or other items by using the software application of a business user, even where these items have been acquired by the end users from the relevant business user without using the core platform services of the gatekeeper, unless the gatekeeper can demonstrate that such access undermines the fulfilment of the obligations set out under EU law on end users data protection and/or cybersecurity.***

- (d) refrain from *directly or indirectly* preventing or restricting business users *or end users* from ~~*directly or indirectly*~~ raising issues with any relevant public authority, *including national courts*, relating to any practice of gatekeepers;
- (e) refrain from requiring business users to use, offer or interoperate with an identification service *or any other ancillary service* of the gatekeeper in the context of services offered by the business users using the core platform services of that gatekeeper;
- (f) ~~refrain from requiring~~ *not require* business users or end users to subscribe to or register with any other core platform ~~services identified pursuant to Article 3 or which meets the thresholds in Article 3(2)(b)~~ as a condition *for being able to use*, access, sign up *for* or registering *with* to any of their core platform services identified pursuant to that Article ~~nor seek to achieve the same result through product design~~;
- ~~(fa) not distort, alter or impair manipulate end users' and business users' autonomy, decision making, or choice via the structure, design, function or manner of operation of their online interface or any part thereof;~~
- (g) provide ~~individual~~ advertisers and publishers *or third parties authorised by the advertisers or publishers*, to which it supplies *digital* advertising services, ~~upon their request~~ *with free of charge, high-quality, effective, continuous and real-time access to full information on the visibility and availability of advertisement portfolio as well as*, including:
  - (i) *the pricing conditions concerning the bids placed by advertisers and advertising intermediaries* ~~with information concerning~~;
  - (ii) *the price-setting mechanisms and schemes for the calculation of the fees including the non-price criteria in the auction process*;
  - (iii) the price *and fees* paid by the advertiser and publisher, *including any deductions and surcharges*; ~~as well as~~
  - (iv) the amount ~~of~~ *and* remuneration paid to the publisher, for the publishing of a given advertisement; and
  - (v) *the amount and remuneration paid to the publisher* for each of the relevant advertising services provided by the gatekeeper.
- ~~(g)a~~ refrain from using, in competition with business users, any data not publicly available, which is generated through *or in the context of activities by those business users, including by the end users of these business users, of its the use of the relevant* core platform services or *ancillary services provided* by those business users *including by the end users of these business users of its core platform services or ancillary services or provided by those business users of its core platform services or ancillary services* or by the end users of these business users; [Moved from Article 6 as this obligation does not seem susceptible of being further specified.]
- ~~(g)b~~ allow *and technically enable* end users to un-install any pre-installed software applications on ~~its~~ core platform service *an* operating system *that the gatekeeper provides or effectively controls as easily as any software application installed by end users at any stage, and to change default settings on an operating system that direct or steer end users to services or products offered by the gatekeeper*, 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;

[Moved from Article 6 as this obligation does not seem susceptible of being further specified.]

2. **For the purposes of point (g)a of paragraph 1 data that is not publicly available shall include any aggregated and non-aggregated data generated by business users that can be inferred from, or collected through, the commercial activities of business users or their customers on the core platform service or ancillary services of the gatekeeper.**[moved from Article 6]

#### Article 6

##### *Obligations for gatekeepers susceptible of being further specified*

1. In respect of each of its core platform services identified pursuant to Article 3(7), a gatekeeper shall:
  - (a) ~~refrain from using, in competition with business users, any data not publicly available, which is generated through activities by those business users, including by the end users of these business users, of its core platform services or provided by those business users of its core platform services or by the end users of these business users;~~ [Moved to Article 5 as this obligation does not seem susceptible of being further specified.]
  - (b) ~~allow end users to un-install any pre-installed software applications on its core platform service 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;~~ [Moved to Article 5 as this obligation does not seem susceptible of being further specified.]aa) *refrain from combining personal data for the purpose of delivering targeted or micro-targeted advertising, except if a clear, explicit, renewed and-informed consent has been requested by the gatekeeper in line with the procedure foreseen in the Regulation (EU) 2016/679.*
  - (c) allow *and technically enable* the installation and effective use ~~and interoperability~~ of third party software applications or software application stores using, or interoperating with, operating systems of that gatekeeper and allow these software applications or software application stores to be accessed by means other than the *relevant* core platform services of that gatekeeper. The gatekeeper shall *prompt where relevant the end user to decide whether the downloaded application or application store should become the default. The gatekeeper shall* not be prevented from taking *measures that are both necessary and* proportionate ~~measures~~ to ensure that third party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the *gatekeeper or undermine end-user to ensure the fulfilment of obligation set out under EU law on data protection and-or cyber security provided that such necessary and proportionate measures are duly justified by the gatekeeper;*
  - (d) ~~refrain from treating not treat~~ more favourably in ranking ~~or display other settings~~, services and products offered by the gatekeeper itself or by any third party belonging to the same undertaking compared to similar services or products of third party and apply *transparent*, fair and non-discriminatory

~~conditions to such *third party services or products* ranking; *where a gatekeeper's online search engine results page includes the display of separate products or services third parties shall be afforded equal opportunity to provide this product or services in exchange for remuneration; to avoid any conflicts of interest, the gatekeeper's product or service shall be treated as a separate commercial entity and shall be commercially viable as a stand-alone service;*~~

- (e) ~~not refrain from restrict~~ technically or ~~otherwise restricting~~ the ability of end users to switch between and subscribe to different software applications and services ~~to be accessed using the operating system of the gatekeeper, including as regards the choice of Internet access provider for end users; refrain from practices that obstruct the possibility for the end-user to unsubscribe from a core platform service.~~
- (f) allow business users, ~~and~~ providers of services ~~and providers of hardware ancillary~~ *free of charge* access to and interoperability with the same *hardware and software features accessed or controlled via an* operating system, ~~hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services~~ *provided the operating system is identified pursuant to Article 3(7), that are available to services that are available to services or hardware provided by the gatekeeper; access and interoperability conditions shall be fair, reasonable and non-discriminatory; allow business users and providers of ancillary services to interoperate with the gatekeeper core platform service in a functionally equivalent manner as the gatekeepers own products or services; Providers of ancillary services shall further be allowed access to and interoperability with the same operating system, hardware or software features, regardless of whether the latter are part of an operating system, that are available to ancillary services provided by a gatekeeper. 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.* [wording proposed by the Commission]
- fa *allow any providers of equivalent core platform services upon their request and free of charge to interconnect with the gatekeepers number independent interpersonal communication services [or social network services core platform services] identified pursuant to Article 3(7). Interconnection shall be provided with the same conditions 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.*
- (g) provide advertisers and publishers, ~~or third parties authorised by advertisers and publishers~~ upon their request and free of charge, with access to the performance measuring tools of the gatekeeper and the information necessary for advertisers and publishers to carry out their own independent verification of the ad inventory *including aggregated data and performance data in a manner that would allow advertisers and publishers to run their own verification and*

*measurement tools to assess performance of the core services provided for by the gatekeepers;*

- (h) provide *end users or third parties authorised by an end user, upon their request and free of charge, with* effective portability of data provided by the end user or generated through ~~his or her their~~ ~~the activity of a business user or end user in the context of the use on the relevant core platform service and shall, in particular, including by~~ *providing free of charge tools for end users* to facilitate the *effective* exercise of ~~effective exercise of such~~ data portability, in line with Regulation EU 2016/679, *and* including by the provision of continuous and real-time access;
- (i) provide business users, or third parties authorised by a business user, *upon their request*, free of charge, with ~~effective, high quality~~, continuous and real-time access and use of aggregated ~~and or~~ non-aggregated data, that is provided for or generated in the context of the use of the relevant core platform services *or ancillary services offered by the gatekeeper* by those business users and the end users engaging with the products or services provided by those business users; *This shall include, at the request of the business user, the possibility and necessary tools to access and analyse data “in-situ” without a transfer from the gatekeeper.* 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 service, and when the end user opts in to such sharing with a consent in the sense of the Regulation (EU) 2016/679;
- (j) provide to any third party providers of online search engines, upon their request, with access on fair, reasonable and non-discriminatory terms to 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 ~~ranking~~, query, click and view data that constitutes personal data;
- (k) apply *transparent, fair, reasonable* and non-discriminatory general conditions of access *and conditions that are not less favourable than the conditions applied to its own service* for business users to *its core platform services* ~~software application store~~ designated pursuant to Article 3 of this Regulation.

~~2. For the purposes of point (a) of paragraph 1 data that is not publicly available shall include any aggregated and non aggregated data generated by business users that can be inferred from, or collected through, the commercial activities of business users or their customers on the core platform service of the gatekeeper. [moved this to Article 5]~~

## Article 12

### Obligation to inform about concentrations

1. A gatekeeper shall inform the Commission ~~and competent national authorities~~ of any intended concentration within the meaning of Article 3 of Regulation (EC) No 139/2004 involving another provider of core platform services or of any other services provided in the digital sector irrespective of whether it is notifiable to a Union competition authority under Regulation (EC) No 139/2004 or to a competent national competition authority under national merger rules.

A gatekeeper shall inform the Commission of such a concentration prior to its implementation and following the conclusion of the agreement, the announcement of the public bid, or the acquisition of a controlling interest.

***The Commission shall inform competent national authorities of such notifications***

2. The notification pursuant to paragraph 1 shall at least describe for the acquisition targets their EEA and worldwide annual turnover, for any relevant core platform services their respective EEA annual turnover, their number of yearly active business users and the number of monthly active end users, as well as the rationale of the intended concentration.
  3. If, following any concentration as provided in paragraph 1, additional core platform services individually satisfy the thresholds in point (b) of Article 3(2), the gatekeeper concerned shall inform the Commission thereof within three months from the implementation of the concentration and provide the Commission with the information referred to in Article 3(2).
- 4a The competent national authorities may use the information received under paragraph 1 to request the Commission to examine the concentration pursuant to Article 22 of Regulation (EC) No 139/2004.***

*Article 13*

*Obligation of an audit*

Within six months after its designation pursuant to Article 3, a gatekeeper shall submit to the Commission **and the High Level Group of Digital Regulators** an independently audited description of any techniques for profiling of consumers that the gatekeeper applies to or across its core platform services identified pursuant to Article 3. This description shall be updated at least annually. ***The Commission shall develop, in consultation with the EU Data Protection Supervisor, the European Data Protection Board, civil society and experts, the standards and process of the audit.***

***The gatekeeper shall make publicly available an overview of the audited description referred in previous paragraph, taking into account business secrets.***

**RECITALS 33 - 57**

(33) [covered under CA D]

- (34) The combination of these different mechanisms for imposing and adapting obligations should ensure that the obligations do not extend beyond observed unfair practices, while at the same time ensuring that new or evolving practices can be the subject of intervention where necessary and justified.
- (35) The obligations laid down in this Regulation are necessary to address identified public policy concerns, there being no alternative and less restrictive measures that would effectively achieve the same result, having regard to need to safeguard public order, protect privacy and fight fraudulent and deceptive commercial practices.

- (36) The conduct of combining end user data from different sources or signing in users to different services of gatekeepers gives them potential advantages in terms of accumulation of data, thereby raising barriers to entry. To ensure that gatekeepers do not unfairly undermine the contestability of core platform services, they should enable their end users to freely choose to opt-in to such business practices by offering a less personalised **but equivalent** alternative. ***The less personalized alternative should not be different or of degraded quality compared to the service offered to the end users who provide consent to the combining of their personal data.*** The possibility should cover all possible sources of personal data, including own services of the gatekeeper as well as third party websites, and should be proactively presented to the end user in an explicit, clear and straightforward manner.
- (36)a ***The treatment of personal data for advertising purposes should not contain indications on peculiarities of individuals such as racial or ethnic origin, the political opinions, the religious or philosophical beliefs, the trade union membership, the health, the sex life or the sexual orientation, The processing shall be in line with the requirements of data minimisation under Article 5 (1)(c) of Regulation (EU) 2016/679.***
- (37) Because of their position, gatekeepers might in certain cases, ***through the imposition of contractual terms and conditions***, restrict the ability of business users of their online intermediation services to offer their goods or services to end users under more favourable conditions, including price, through other online intermediation services ***or through direct business channels***. Such restrictions have a significant deterrent effect on the business users of gatekeepers in terms of their use of alternative online intermediation services ***or direct distribution channels***, limiting inter-platform contestability, which in turn limits choice of alternative online intermediation channels for end users. To ensure that business users of online intermediation services of gatekeepers can freely choose alternative online intermediation services ***or other direct distribution channels*** and differentiate the conditions under which they offer their products or services to their end users, it should not be accepted that gatekeepers limit business users from choosing to differentiate commercial conditions, including price. Such a restriction should apply to any measure with equivalent effect, such as for example increased commission rates or de-listing of the offers of business users.
- (38) To prevent further reinforcing their dependence on the core platform services of gatekeepers, the business users of these gatekeepers should be free in promoting and choosing the distribution channel they consider most appropriate to interact with any end users that these business users have already acquired through core platform services provided by the gatekeeper ***or through other channels***. ***An acquired end user is an end user who has already entered into a contractual relationship with the business user. Such contractual relationships may be on either a paid or a free basis (e.g., free trials, free service tiers) and may have been entered into either on the gatekeeper's core platform service or through any other channel.*** Conversely, end users should also be free to choose offers of such business users and to enter into contracts with them either through core platform services of the gatekeeper, if applicable, or from a direct distribution channel of the business user or another indirect distribution channel such business user may use. This should apply to the promotion of offers, ***communication*** and conclusion of contracts between business users and end users. Moreover, the ability of end users to freely acquire content, subscriptions, features or other items outside the core platform services of the gatekeeper should not be undermined or restricted. In particular, it should be avoided that gatekeepers restrict end users from access to and

use of such services via a software application running on their core platform service. For example, subscribers to online content purchased outside a software application download or purchased from a software application store should not be prevented from accessing such online content on a software application on the gatekeeper's core platform service simply because it was purchased outside such software application or software application store.

- (39) To safeguard a fair commercial environment and protect the contestability of the digital sector it is important to safeguard the right of business users **and end users, including whistleblowers** to raise concerns about unfair behaviour by gatekeepers with any relevant administrative or other public authorities. For example, business users **or end users** may want to complain about different types of unfair practices, such as discriminatory access conditions, unjustified closing of business user accounts or unclear grounds for product de-listings. Any practice that would in any way inhibit **or hinder** such a possibility of raising concerns or seeking available redress, for instance by means of confidentiality clauses in agreements or other written terms, should therefore be prohibited. This should be without prejudice to the right of business users and gatekeepers to lay down in their agreements the terms of use including the use of lawful complaints-handling mechanisms, including any use of alternative dispute resolution mechanisms or of the jurisdiction of specific courts in compliance with respective Union and national law. This should therefore also be without prejudice to the role gatekeepers play in the fight against illegal content online.
- (40) **Gatekeepers offer a range of ancillary—Identification services. To ensure contestability, it is crucial that for business users are free to choose such ancillary services without having to fear any detrimental effects for the provision of the core platform service and to** conduct their business, as these can allow them not only to optimise services, to the extent allowed under Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council<sup>1</sup>, but also to inject trust in online transactions, in compliance with Union or national law. Gatekeepers should therefore not use their position as provider of core platform services to require their dependent business users to **use, offer or include any ancillary service provided by the gatekeeper or a particular third party, where other ancillary services are available to such business users.** ~~include~~ Gatekeepers should **eventually** not use their position as provider of core platform services to require their dependent business users to include any identification services provided by the gatekeeper itself as part of the provision of services or products by these business users to their end users, where other identification services are available to such business users.
- (41) Gatekeepers should not restrict the free choice of end users by technically preventing switching between or subscription to different software applications and services. Gatekeepers should therefore ensure a free choice irrespective of whether they are the manufacturer of any hardware by means of which such software applications or services are accessed and should not raise artificial technical barriers so as to make switching **more difficult impossible** or ineffective. The mere offering of a given product or service to end users, including by means of pre-installation, as well the improvement of end user offering, such as better prices or increased quality, would not in itself constitute a barrier to switching.

---

<sup>1</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).



- (42) The conditions under which gatekeepers provide online advertising services to business users including both advertisers and publishers are often non-transparent and opaque. This opacity is partly linked to the practices of a few platforms, but is also due to the sheer complexity of modern day programmatic advertising. The sector is considered to have become more non-transparent after the introduction of new privacy legislation, and is expected to become even more opaque with the announced removal of third-party cookies. This often leads to a lack of information and knowledge for advertisers and publishers about the conditions of the advertising services they purchased and undermines their ability to switch to alternative providers of online advertising services. 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 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 free of charge, effective, high-quality, continuous and real-time*** when requested and to the extent possible, 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 ***and the availability and visibility of advertisement***.
- (43) A gatekeeper may in certain circumstances have a dual role as a provider of core platform services whereby it provides a core platform service to its business users, while also competing with those same business users in the provision of the same or similar services or products to the same end users. In these circumstances, a gatekeeper may take advantage of its dual role to use data, generated from transactions by its business users on the core platform, for the purpose of its own services that offer similar services to that of its business users. This may be the case, for instance, where a gatekeeper provides an online marketplace or app store to business users, and at the same time offer services as an online retailer or provider of application software against those business users. To prevent gatekeepers from unfairly benefitting from their dual role, it should be ensured that they refrain from using any aggregated or non-aggregated data, which may include anonymised and personal data that is not publicly available to offer similar services to those of their business users. This obligation should apply to the gatekeeper as a whole, including but not limited to its business unit that competes with the business users of a core platform service.
- (44) Business users may also purchase advertising services from a provider of core platform services for the purpose of providing goods and services to end users. In this case, it may occur that the data are not generated on the core platform service, but are provided to the core platform service by the business user or are generated based on its operations through the core platform service concerned. In certain instances, that core platform service providing advertising may have a dual role, as intermediary and as provider of advertising services. Accordingly, the obligation prohibiting a dual role gatekeeper from using data of business users should apply also with respect to the data that a core platform service has received from businesses for the purpose of providing advertising services related to that core platform service. ***Moreover the gatekeeper should refrain from disclosing any commercially sensitive information obtained in connection with one of its advertising services to any third party belonging to the same undertaking and from using such commercially sensitive information for any purposes other than the provision of the specific advertising service unless this is necessary for carrying out a business transaction.***

- (45) In relation to cloud computing services, this obligation should extend to data provided or generated by business users of the gatekeeper in the context of their use of the cloud computing service of the gatekeeper, or through its software application store that allows end users of cloud computing services access to software applications. This obligation should not affect the right of gatekeepers to use aggregated data for providing ancillary data analytics services, subject to compliance with Regulation 2016/679 and Directive 2002/58/EC as well as with the relevant obligations in this Regulation concerning ancillary services.
- (46) A gatekeeper may use different means to favour its own services or products on its core platform service, to the detriment of the same or similar services that end users could obtain through third parties. This may for instance be the case where certain software applications or services are pre-installed by a gatekeeper. To enable end user choice, gatekeepers should not prevent end users from un-installing any pre-installed software applications on its core platform service and thereby favour their own software applications. ***The gatekeeper may restrict such un-installation when such applications are essential to the functioning of the operating system or the device.***
- (47) The rules that the gatekeepers set for the distribution of software applications may in certain circumstances restrict the ability of end users to install and effectively use third party software applications or software application stores on operating systems or hardware of the relevant gatekeeper and restrict the ability of end users to access these software applications or software application stores outside the core platform services of that gatekeeper. Such restrictions may limit the ability of developers of software applications to use alternative distribution channels and the ability of end users to choose between different software applications from different distribution channels and should be prohibited as unfair and liable to weaken the contestability of core platform services. ***To ensure contestability, the gatekeeper should prompt where relevant the end user to decide whether the downloaded application or app store should become the default.*** In order to ensure that third party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper the gatekeeper concerned may implement proportionate technical or contractual measures to achieve that goal if the gatekeeper demonstrates that such measures are necessary and justified and that there are no less restrictive means to safeguard the integrity of the hardware or operating system.
- (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. ***Such preferential or embedded display of a separate online intermediation service shall 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.* 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 *leading to conflicts of interest.* 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.

- (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 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. *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.* The guidelines adopted pursuant to Article 5 of Regulation (EU) 2019/1150 should also facilitate the implementation and enforcement of this obligation.<sup>2</sup>
- (50) Gatekeepers should not restrict or prevent the free choice of end users by technically preventing switching between or subscription to different software applications and services. This would allow more providers to offer their services, thereby ultimately providing greater choice to the end user. Gatekeepers should ensure a free choice irrespective of whether they are the manufacturer of any hardware by means of which such software applications or services are accessed and shall not raise artificial technical barriers so as to make switching impossible or ineffective. The mere offering of a given product or service to consumers, including by means of pre-installation, as well as the improvement of the offering to end users, such as price reductions or increased quality, should not be construed as constituting a prohibited barrier to switching.
- (51) Gatekeepers can hamper the ability of end users to access online content and services including software applications. Therefore, rules should be established to ensure that the rights of end users to access an open internet are not compromised by the conduct of gatekeepers. Gatekeepers can also technically limit the ability of end users to effectively switch between different Internet access service providers, in particular through their control over operating systems or hardware. This distorts the level playing field for Internet access services and ultimately harms end users. It should therefore be ensured that gatekeepers do not unduly restrict end users in choosing their Internet access service provider.
- (52) Gatekeepers may also have a dual role as developers of operating systems and device manufacturers, including any technical functionality that such a device may have. For example, a gatekeeper that is a manufacturer of a device may restrict access to some of the functionalities in this device, such as near-field-communication technology and the software used to operate that technology, which may be required for the effective

---

<sup>2</sup> Commission Notice: Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council (OJ C 424, 8.12.2020, p. 1).

provision of an ancillary service by the gatekeeper as well as by any potential third party provider of such an ancillary service. Such access may equally be required by software applications related to the relevant ancillary services in order to effectively provide similar functionalities as those offered by gatekeepers. If such a dual role is used in a manner that prevents alternative providers of ancillary services or of software applications to have access under equal conditions to the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services, this could significantly undermine innovation by providers of such ancillary services as well as choice for end users of such ancillary services. The gatekeepers should therefore be obliged to ensure access under equal conditions to, and interoperability with, the same operating system, hardware or software features that are available or used in the provision of any ancillary services by the gatekeeper.

**52 a** *The lack of interconnection features among the gatekeeper services may substantially affect users choice and ability to switch due to the incapacity for end user to reconstruct social connections and networks provided by the gatekeeper even if multi-homing is possible. Therefore, it should be allowed for any providers of equivalent core platform services to interconnect with the gatekeepers number independent interpersonal communication services or social network services upon their request and free of charge. Interconnection shall be provided with at least the same conditions that are available or used by the gatekeeper, while ensuring a high level of security and personal data protection. In the particular case of number-dependant intercommunication services, interconnection requirements should mean giving the possibility for third-party providers to request access and interconnection for features such as text, video, voice and picture, while it should provide access and interconnection on basic features such as posts, likes and comments for social networking services. Interconnection measures of number-independent interpersonal communication services should be imposed in accordance with the provisions of the Electronic Communications Code and particularly the conditions and procedures foreseen in Article 61 thereof.*

(53) The conditions under which gatekeepers provide online advertising services to business users including both advertisers and publishers are often non-transparent and opaque. This often leads to a lack of information for advertisers and publishers about the effect of a given ad. To further enhance fairness, transparency and contestability of online advertising services designated under this Regulation as well as those that are fully integrated with other core platform services of the same provider, the designated gatekeepers should therefore provide advertisers and publishers **for entire disclosure and transparency of the parameters and data used for decision making, execution and measurement of the intermediation services**, *A gatekeeper shall further provide* when requested, with free of charge access to the performance measuring tools of the gatekeeper and the information necessary for advertisers, advertising agencies acting on behalf of a company placing advertising, as well as for publishers to carry out their own independent verification of the provision of the relevant online advertising services. (54) Gatekeepers benefit from access to vast amounts of data that they collect while providing the core platform services as well as other digital services. To ensure that gatekeepers do not undermine the contestability of core platform services as well as the innovation potential of the dynamic digital sector by restricting the ability of business users to effectively port their data, business users and end users should be granted effective and immediate access to the data they provided or generated in the

context of their use of the relevant core platform services of the gatekeeper, in a structured, commonly used and machine-readable format. This should apply also to any other data at different levels of aggregation that may be necessary to effectively enable such portability. It should also be ensured that business users and end users can port that data in real time effectively, such as for example through high quality application programming interfaces. Facilitating switching or multi-homing should lead, in turn, to an increased choice for business users and end users and an incentive for gatekeepers and business users to innovate.

- (55) Business users that use large core platform services provided by gatekeepers and end users of such business users provide and generate a vast amount of data, including data inferred from such use. In order to ensure that business users have access to the relevant data thus generated, the gatekeeper should, upon their request, allow unhindered access, free of charge, to such data. Such access should also be given to third parties contracted by the business user, who are acting as processors of this data for the business user. Data provided or generated by the same business users and the same end users of these business users in the context of other services provided by the same gatekeeper may be concerned where this is inextricably linked to the relevant request. To this end, a gatekeeper should not use any contractual or other restrictions to prevent business users from accessing relevant data and should enable business users to obtain consent of their end users for such data access and retrieval, where such consent is required under Regulation (EU) 2016/679 and Directive 2002/58/EC. Gatekeepers should also facilitate access to these data in real time by means of appropriate technical measures, such as for example putting in place high quality application programming interfaces.
- (56) The value of online search engines to their respective business users and end users increases as the total number of such users increases. Providers of online search engines collect and store aggregated datasets containing information about what users searched for, and how they interacted with, the results that they were served. Providers of online search engine services collect these data from searches undertaken on their own online search engine service and, where applicable, searches undertaken on the platforms of their downstream commercial partners. Access by gatekeepers to such ranking, query, click and view data constitutes an important barrier to entry and expansion, which undermines the contestability of online search engine services. Gatekeepers should therefore be obliged to provide access, on fair, reasonable and non-discriminatory terms, to these ranking, query, click and view data in relation to free and paid search generated by consumers on online search engine services to other providers of such services, so that these third-party providers can optimise their services and contest the relevant core platform services. Such access should also be given to third parties contracted by a search engine provider, who are acting as processors of this data for that search engine. When providing access to its search data, a gatekeeper should ensure the protection of the personal data of end users by appropriate means, without substantially degrading the quality or usefulness of the data.
- (57) In particular gatekeepers which provide access to *core platform services* serve as an important gateway for business users that seek to reach end users. In view of the imbalance in bargaining power between those gatekeepers and business users of their *core platform services*, those gatekeepers should not be allowed to impose general conditions, including pricing conditions, that would be unfair or lead to unjustified differentiation. Pricing or other general access conditions should be considered unfair if they lead to an imbalance of rights and obligations imposed on business users or confer an advantage on the gatekeeper which is disproportionate to the service provided

by the gatekeeper to business users or lead to a disadvantage for business users in providing the same or similar services as the gatekeeper. The following benchmarks can serve as a yardstick to determine the fairness of general access conditions: prices charged or conditions imposed for the same or similar services by other providers of *core platform services* ; prices charged or conditions imposed by the provider of the software application store for different related or similar services or to different types of end users; prices charged or conditions imposed by the provider of the software application store for the same service in different geographic regions; prices charged or conditions imposed by the provider of the software application store for the same service the gatekeeper offers to itself. This obligation should not establish an access right and it should be without prejudice to the ability of providers of *core platform services* to take the required responsibility in the fight against illegal and unwanted content as set out in Regulation [Digital Services Act].

#### **Recital on Article 12**

- (31) To ensure the effectiveness of the review of gatekeeper status as well as the possibility to adjust the list of core platform services provided by a gatekeeper, the gatekeepers should inform the Commission ~~and the competent national authorities~~ of all of their intended and concluded acquisitions of other providers of core platform services or any other services provided within the digital sector. Such information should not only serve the review process mentioned above, regarding the status of individual gatekeepers, but will also provide information that is crucial to monitoring broader contestability trends in the digital sector and can therefore be a useful factor for consideration in the context of the market investigations foreseen by this Regulation. ***The Commission should inform competent national authorities of such notifications. The information gathered may be used to trigger the referral system set out in article 22 of the Regulation (EC) no. 139/2004.***

#### **Recital on Article 13 - recital 61**

- (61) The data protection and privacy interests of end users are relevant to any assessment of potential negative effects of the observed practice of gatekeepers to collect and accumulate large amounts of data from end users. Ensuring an adequate level of transparency of profiling practices employed by gatekeepers facilitates contestability of core platform services, by putting external pressure on gatekeepers to prevent making deep consumer profiling the industry standard, given that potential entrants or start-up providers cannot access data to the same extent and depth, and at a similar scale. Enhanced transparency should allow other providers of core platform services to differentiate themselves better through the use of superior privacy guaranteeing facilities. To ensure a minimum level of effectiveness of this transparency obligation, gatekeepers should at least provide a description of the basis upon which profiling is performed, including whether personal data and data derived from user activity is relied on, the processing applied, the purpose for which the profile is prepared and eventually used, the impact of such profiling on the gatekeeper's services, and the steps taken to enable end users to be aware of the relevant use of such profiling, as well as to seek their consent. ***The Commission should develop, in consultation with the EU Data Protection Supervisor, the European Data Protection Board, civil society and experts, the standards and process of the audit.***