# A Telecoms Industry View on the Digital Services Act

Joint Position Paper by the GSMA and ETNO



**About the GSMA**

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators and nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at **gsma.com**

Follow the GSMA on Twitter:
**@GSMA**
**@GSMAEurope**

**About ETNO**

ETNO is the European Telecommunications Network Operators' Association. We proudly represent Europe's main telecom operators, who innovate and invest in the continent's digital backbone. Our companies are the providers of Europe's most advanced digital networks and services. ETNO's mission is to develop a positive policy and regulatory environment empowering the delivery of world-class services for European citizens and businesses.

**www.etno.eu** | **@ETNOAssociation**

# Introduction and Executive Summary

In this digital age, the future of our democracies, societies and economies depends on digital ecosystems that are open, fair, competitive, and respectful of the rule of law.

The adoption of digital technology brings the promise of addressing some of the biggest challenges of our times: climate change, inclusion, socio-economic growth – just to name a few. However, progress will only happen if digital industries are able to advance a purpose that goes beyond just delivering for narrow categories such as "users" or "consumers". Digital technology needs to serve citizens.

For this reason, we believe that the European Commission's efforts in shaping a "Digital Services Act" (DSA) has the potential to be one of the most relevant tech policy exercises of our generation. Not only it will be relevant to millions of European citizens and businesses, but also has the potential to inspire a new global approach to digital markets.

In this context, the GSMA and ETNO take a view that the digital economy is a broad, diverse ecosystem. One in which innovation thrives through collaboration and competition, but also through shared responsibility and accountability across global value-chains.

The DSA approaches two fundamental aspects of today's digital markets. On the one hand, we must address the balance between ensuring fundamental freedoms and preventing illegal and socially toxic activity online. On the other hand, we should tackle the effects of excessive market power in the digital space, taking a European perspective on practices that might unfairly disadvantage European companies and innovation.

The Commission will no doubt embark on this feat guided by Europe's long-standing values and principles, enshrined in the *acquis communautaire*: the freedom of thought and of expression, the principles of open and fair competition, as well as the key principles of the eCommerce Directive.

On behalf of the European mobile and fixed telecom operators, the GSMA and ETNO propose that the Commission consider the following recommendations when designing the DSA:

## Review of the eCommerce Directive

- **Put the European single market and European values at the core of the review** by maintaining the main principles enshrined in the existing eCommerce Directive: country of origin; limited liability for targeted online intermediaries; prohibition of general monitoring obligations;

- **Recognise the diversity of the digital ecosystem** and promote regulatory intervention in areas where specific harm is recognised: not all platforms are the same;

- **Direct the regulatory focus to those hosting services that play an 'active' role** in the dissemination of content online or share such content with a broad audience or have the technical means to swiftly identify and remove users' specific content on a piece-by-piece basis;

- **Be mindful of internet freedoms** by emphasising the use of "notice-and-action" at the hosting providers' level for the removal of illegal content, while limiting the use of "blocking injunctions" at the network level and using it as a last resort;

• **Consider further strengthening and harmonising the use of reliable notifiers**, such as trusted flaggers, to identify the presence of illegal content online and ensure a more effective enforcement against such content;

• **Ensure legal certainty, proportionality, and the preservation of fundamental rights** by applying a clear distinction between illegal content and content that is harmful, but legal. In our view, the DSA is not the appropriate tool for addressing harmful content.

## Regulation of Digital Gatekeepers

• **Support new measures to promote fair competition in digital markets**. Where competition law is insufficient to provide effective solutions to problems arising from entrenched and durable dominance in digital markets, it should be complemented by a new ex-ante regulatory framework tailored to large online platforms acting as gatekeepers.

• **Advocate for a dynamic case-by-case approach:** a careful and targeted approach should identify the digital gatekeepers that must be subject to ex-ante regulation, testing them against specific criteria that reflect the competitive dynamics of each digital market.

• **Support targeted, proportionate, and dynamic remedies:** a framework based on a case-by-case assessment should entail the application of specific remedies, which allow for dynamic adjustments addressing harm and market structures. Proportionality will be key in reflecting the nature and the gravity of the specific threats to competition and to contestability in a targeted market.

• **Consider introducing a list of prohibited unfair commercial practices** that digital gatekeepers should always be prevented from deploying, as a complementary safeguard against the most frequent and harmful abusive behaviours.

• **Promote harmonisation through supervision and enforcement of the new rules at the EU level:** large online platforms operate in global ecosystems and competition concerns arising in digital markets have an important cross-border dimension. In parallel, ensure coordination of authorities across Member States.

# Review of the eCommerce Directive

Since the adoption of the eCommerce Directive in 2000, the use of digital services has increased considerably. Almost 85 percent of all individuals in the EU-28, aged between 16 and 74 years, are using the internet regularly[1]. At the same time, the variety of online services has also grown exponentially, and new business and value creation models have emerged. In particular, the importance of online platforms that allow the wide dissemination of user content to individuals and society has drastically increased.

The members of GSMA and ETNO provide a broad range of information society services, as defined in the eCommerce Directive. Predominantly these services consist of the provision of connectivity and internet access (falling within the liability regime provided for 'mere conduits' within the eCommerce Directive). However, GSMA and ETNO members also provide a variety of services such as those falling in the categories of caching or hosting within the definitions of the eCommerce Directive.

In recent years, as part of the Digital Single Market Strategy, the legal framework regulating responsibilities for, or otherwise governing the provision of, digital services was complemented by legislation to deal with specific issues.

However, there remain areas for improvement, specifically with regard to ensuring legal certainty and cross-border harmonisation vis-à-vis intermediary liability and the safety of consumers. In the light of new economic realities, new threats and issues in our society, an update to the legal framework on the liability of online intermediaries is needed. The ambition of the von der Leyen Commission, and the issues brought sharply into focus by the COVID-19 crisis, offers an opportunity to achieve a coherent set of rules for digital services.

GSMA and ETNO support the aim of harmonising rules across Member States, limiting fragmentation, to foster a digital single market for citizens and enterprises. This also requires that harmonised rules be proportionate, targeted and do not create excessive regulatory burdens. The choice of a Regulation as the legislative instrument in this regard can support this objective.

## Preserving the fundamental principles of the eCommerce Directive

The review of the eCommerce Directive by way of the Digital Services Act should take account of technical developments and capabilities, considering additional targeted provisions to address specific issues while preserving the fundamental principles of the eCommerce Directive.

**Country of Origin Principle:** The country of origin principle is a cornerstone of the liability framework of the Digital Single Market and, as such, any new regulatory framework should maintain this principle. This should go hand in hand with the effort to further harmonise obligations across Member States. All service providers offering services in the EU should be subject to the EU rules, irrespective of their place of main establishment. Therefore, undertakings in third countries that provide services to EU users should be required to have a representative within the EU and follow the legal requirements of at least this Member State. This would be in line with recent EU regulatory developments, including the Commission's proposal for a Regulation on Terrorist Content Online, the General Data Protection Regulation (GDPR), and the Regulation on Platform-to-Business Relations, which explicitly require providers to have a legal representative within the EU territory.

1. Digital Economy and Society Statistics, Eurostat, 2019

**Liability Exemptions:** The underlying legal principle that certain online intermediaries (such as ISPs and other network access, caching and cloud services providers) are not liable for content they transmit or store at the request of users should be preserved. Services categorised as 'mere conduit', in particular, access services – covered by Article 12 the e-Commerce Directive – are subject to the Open Internet Regulation that prohibits to block, slow down, alter, restrict, interfere with, degrade or discriminate specific content, applications or services and only allows blocking (e.g. of unlawful content) if that is based on "Union legislative acts, or national legislation that complies with Union law" (Telecoms Single Market Regulation, Art. 3(3) a). Similarly, caching providers and hosting services providers – covered by Articles 13 and 14 the e-Commerce Directive – should continue to benefit from the exemption from liability for user content to the extent that they do not play an active role in the dissemination of such content. We reiterate that providers of internet access services should not be under any obligation to monitor traffic over their networks since these digital services have no knowledge, control or management activity over the content that users upload and exchange when using their services.

**Prohibition on general monitoring:** The prohibition on imposing a general monitoring obligation set out in Article 15 of the eCommerce Directive should be maintained under the Digital Services Act. Furthermore, and in line with Article 15, hosting service providers should benefit from more legal certainty when taking targeted pro-active measures to detect and remove illegal content as indicated by the jurisprudence of the CJEU[2].

## An update to the legal framework is needed on the scope and responsibilities of hosting services

While the above-mentioned principles have proven fit for purpose and should therefore be maintained also in the DSA, we acknowledge that new business models have emerged, and an update of the current legal framework is needed. In order to do so, specific problems should be addressed through targeted legislative intervention focused on the areas where harm occurs.

In our view, this centres around the scope of hosting services, where an important clarification needs to be introduced, distinguishing **'active'** and **'passive'** hosting service providers. We believe the provisions of Article 14 of the eCommerce Directive should be amended consistently with the jurisprudence of the CJEU[3], which elaborated on 'hosting services' by introducing this crucial distinction. While the liability exemption enshrined by Article 14 is still reasonably applicable to passive hosting providers, it is essential to redefine the categorisation and the responsibilities of online services that play an active role in the dissemination of content online.

The categorisation as **'active hosting provider'** should apply where that provider has actual knowledge of, or exerts control over the content made available by its users, for example by tagging, organizing, promoting, optimizing, personalizing, recommending, presenting or otherwise curating specific content[4]. In relation to those (active) intermediaries, a new liability regime could be designed in order to ensure a more trustworthy use of the internet. On the contrary, it

2. CJEU Case Eva Glawischnig-Piesczek v Facebook Ireland Limited from October 2019. In its ruling, the Court held that a platform could be ordered by a national court to remove information which it stores, the content of which is identical or equivalent to information which was previously declared to be unlawful.

3. In its Google France and L'Oréal v. eBay decisions, the CJEU formulates the distinction between active and passive hosts.

4. For the purpose of the Digital Services Act, dissemination to the public is understood as the practice of making available a given item of content, at any time to any internet user, without the need to be granted specific access rights by a content owner or administrator.

is unreasonable to impose obligations that aim at reducing broad dissemination of illegal content to services that do not reach a broad audience or to require detection from hosting providers that do not have the technical means to identify users' specific content (e.g. GSMA and ETNO members' cloud services that strictly protect users' content).

We suggest the following non-cumulative criteria to establish additional liabilities for specific hosting service providers, going beyond current provisions applicable to all hosting services providers:

**1. Interaction with user-generated content:** building on the distinction between active and passive hosting providers established in the eCommerce Directive and developed by the CJEU, where platforms that have actual knowledge of, or exert control over, the content including activity or information.

**2. Impact:** where the actual risk results from a specific online platform, such as the sharing of illegal user-generated content with a broad audience.

**3. Available technical capabilities:** where platforms retain (or can easily put in place) the means to address the problem in the most expedient and proportionate manner, closest to its source. This may include the abilities to identify and remove users' specific content on a piece-by-piece basis.

## Additional obligations for active hosting service providers

From our perspective, the current system disincentivises hosting service providers from taking more proactive steps to prevent illegal activities: the less a service provider knows about illegal activity on its platform, the clearer its liability defence. This is a perverse incentive, and one that could be corrected in the scope of the DSA.

**Pro-active measures:** Should a new set of binding legal requirements be introduced, these need to be strictly limited to active hosting service providers. Legal requirements could include the taking of proactive steps to prevent the dissemination of illegal content, which is particularly relevant for hosting service providers that allow sharing of user-generated content with a broad audience. In addition, it should be considered whether the provider actually has the technical capability to identify or remove specific end-user content. The application of such proactive measures should not confer upon the hosting service provider primary liability for illegal material or the illegal activity of its users but would function rather as a legal obligation/Duty of Care to consider the safety of users on its platform, and take action to mitigate these risks with appropriate sanctions for failure to do so. Such requirements and enforcement regimes should be reasonable and proportionate.

**Stay-down & put-back obligations:** We believe that responsibilities beyond current provisions applicable to any hosting service provider should be legally required only in a targeted way to ensure legal clarity and avoid infringement on fundamental rights and freedoms. If stay-down and put-back obligations are considered to reinforce the fight against illegal content online, these provisions should be strictly limited to providers that qualify as 'active' hosting service providers, which share user-generated content with a broad audience and which have the technical capability to identify or remove specific end-user content. Moreover, these measures should remain targeted so as to not contradict the underlying principle of Article 15 of the eCommerce Directive whereby general monitoring obligations are prohibited. In particular, should mandatory detection tools be introduced to identify illegal content, such obligations must be limited to targeted measures for defined types of content or specific services, so as to not constitute general monitoring as indicated by the jurisprudence of the CJEU[5].

5.. CJEU Case Eva Glawischnig-Piesczek v Facebook Ireland Limited from October 2019. In its ruling, the Court held that a platform could be ordered by a national court to remove information which it stores, the content of which is identical or equivalent to information which was previously declared to be unlawful.

**Transparency & reporting:** Online platforms that impose particularly high risk by allowing the sharing of user-generated content with a broad audience or the public should provide competent authorities with transparency reports including statistics on content removed on a regular basis and an explanation on how automated systems apply in practice. These reports should be easily understood by the public, allow for comparison across different online platforms in scope in the different Member States, and include data about the actions taken in response. Trust can also be built using other means, including regulatory codes of practice and standards to which companies must adhere.

The consequence for failing to apply these obligations should be sanctions, in order to incentivise compliance, without necessarily subjecting the service provider to direct liability for the illegal activity of their users. However, in the case of persistent non-compliance with these obligations, increasing levels of sanctions should be foreseen (e.g. fines as in the GDPR), ultimately resulting in the loss of the liability exemption if the infringement of the obligation of removal constitutes a systemic failure.

## Notice-and-action should remain the primary instrument for the removal of illegal content

When it comes to the removal of illegal content, the Digital Services Act should reinforce the cascade of responsibilities, emphasising that the **notice-and-action mechanism** should be the primary instrument in the removal of illegal content, addressing the hosting service providers who are best placed to act to remove such content.

The removal of illegal content should happen as close to the source as possible. Blocking injunctions, issued to Internet Service Providers by a competent authority to prevent access to illegal content, should only be considered as a last resort, where any reasonable and proportionate action closer to the content owner is not possible. From a technical perspective, the blocking of websites is challenging (even more so with encryption) and costly. Whereas content removal may be determined by terms of service or other conditions, Internet Access Providers do not assess the content related to blocking injunctions and simply execute the received order. Therefore, when issuing blocking injunctions, public authorities should be obliged to cover internet access providers' resulting costs, and indemnification against potential claims for the action taken as ordered should be foreseen.

## Tackling illegal content could be reinforced by third parties such as trusted flaggers

As proposed in the Commission's Recommendation on Tackling Illegal Content Online, we believe that reliable notifiers could be helpful to identify the presence of illegal content online and ensure a more effective enforcement against such content, in the context of hosting service providers that allow the sharing of user-generated-content with the public or broad audience.

These third parties – such as **Trusted Flaggers** – should be duly accredited and independent, and could be public or private organisations, whose role would be to identify illegal online content,

goods and services and inform competent authorities. After direct notification of the content by the trusted flagger, the platform would remove the content, or the competent authority would order its removal. The various national administrations should share their official list of trusted flaggers with the other Member States so that their actions are valid and legitimate when they act at European level.

EU Member States should further improve cooperation, both between EU Member States and with third parties in order to contribute to swift action against illegal content. This acknowledges that hosting service provider's effective actions strongly depend on an effective interplay with authorities and other involved stakeholders.

## A clear distinction is needed between illegal and harmful content

For the sake of legal certainty, proportionality and the preservation of fundamental rights, a clear distinction should be made between rules applicable to illegal content, in contrast to content which is harmful but legal. We believe that the DSA should not aim at establishing rigid definitions for harmful content, which will in any event be determined at the national level and/or addressed more comprehensively in other instruments, including the Democracy Action Plan. The DSA should possibly subject relevant hosting service providers (e.g. online platforms that allow sharing of user-generated content with the public or a broad audience) to fully harmonised obligations such as on transparency.

We support concerted action from all relevant stakeholders to swiftly address systemic threats to society. Even in emergency situations, providers of digital services require legal certainty when taking specific actions. While we fully support that relevant providers take responsibility when required, this must not result in severe legal risks for these providers when dealing with harmful content that more often lacks generally agreed definitions. Any potential obligation in that context must be clearly defined and strictly limited to specific systemic threats in order to not spur misuse (e.g. political purposes).

A recent example is the disinformation campaigns falsely linking the COVID-19 pandemic to 5G deployment. The fast spread of this content over social media platforms motivated arson attacks against hundreds of telecom masts and the harassment of hundreds of maintenance workers and engineers. Moreover, the ensuing misinformation that spread among activist groups and among broader communities has caused confusion around the health and safety of networking technologies. Beyond being criminal offenses, these attacks on critical infrastructure threatened to undermine the fundamental rights of access to information and freedom of expression, as well as the digital economy.

The dis/misinformation around 5G and COVID-19 needs to be strictly distinguished and differentiated from existing health concerns about electromagnetic fields from communications equipment, particularly now with the deployment of 5G. The Commission and Member States must educate the public at all levels around the international public safety standards followed in the EU and the fact-based science that supports them.

# Regulation of Digital Gatekeepers

Electronic communication services and connectivity underpin people's digital lives and consumer behaviours. At the same time, as markets and technologies converge, connectivity becomes increasingly entwined with wider consumer propositions and larger ecosystems. Indeed, digital ecosystems have themselves become more complex and multi-layered, with the ever-critical role of online gatekeepers such as search engines, operating systems and voice assistants, in shaping users' relationship with digital services and in governing the relationship between the different parties in the whole ecosystem.

Large online platforms are thus the centrepiece of digital environments. They hold the key to the user experience online, and they are the strategic partners for all businesses along the value chain that want to participate in economic and social activity. Large online platforms should consequently exert their essential role in a manner that promotes fairness, competition, and innovation for all users, competitors, and partners.

Large online platforms acting as gatekeepers can also exploit their crucial gatekeeper role to stifle digital markets and ecosystems, rather than nurturing them. These platforms frequently engage in behaviours which include the imposition of unfair terms and conditions; prominence given to a platform's own content, service, or advertising (self-preferencing); entrenching a platform's position in adjacent markets by bundling its services, typically with 'must have' services and apps; restrictions to service interoperability and to access to key components, software or hardware; restrictions to data portability due to a lack of interoperability of application programming interfaces (APIs); etc. The exclusionary effect of such behaviours is exacerbated by a lack of transparency.

As a result of their vast network effects, key data assets, and their unequal bargaining power on business counterparts, large online platforms acting as gatekeepers that engage in abusive practices have a very severe impact on competition across their digital environment. These winner-take-all tactics raise high barriers to entry, marginalise traditional players, exclude potential competitors, and reinforce user lock-in, resulting in prejudice to market contestability. Ultimately, this translates into a chilling effect on consumer choice and innovation in alternative digital services.

Competition policy can tackle failures in digital markets and recent European cases have demonstrated that the Commission is able to act strongly in certain cases. Even so, we recognise that there are limits to what competition law can achieve to address the gatekeeper role of large online platforms in digital markets. The current competition framework is not always sufficient to tackle competition issues arising from large digital platforms with cross-market activity in an efficient and timely manner, due to the specificities of these platforms. Dedicated rules targeted at large online platforms acting as gatekeepers would be an appropriate instrument to avoid competition distortion, before entrenched and durable dominance materialises in digital markets.

# What are digital gatekeepers?

Digital platforms cover various business models and operate in different segments of the online ecosystem.

They all have in common some key characteristics that contribute to cementing their market power. Large online platforms acting as gatekeepers typically enjoy a **very large user base**, have **cross-market activity** over a wide geographic footprint, play a gatekeeping role by controlling the access to markets or to users, leverage **strong network effects**, raise **barriers to entry** in their markets and are readily able to enter **adjacent markets** thanks to their considerable physical and intangible assets. Consumer behavioural biases such as consumers' preference for default options, the size of a company, and its financial and innovation capabilities strengthen these companies' market power and constitute barriers for their competitors.

This affects several telecommunications markets, where these players are accelerating the disintermediation of telecom operators, for instance reaching unconnected populations with aerial-based solutions using satellites and drones on unlicensed spectrum or laying down their own fibre network infrastructure. This trend will only increase in the race towards 5G, where some of these players are moving towards the edge to leverage their cloud, hosting and storage capabilities.

The role of data is particularly pivotal in growing a firm into a digital gatekeeper. Online platforms collect and generate huge amounts of valuable data, which have increasing marginal returns that enable significant economies of scale and which can be easily leveraged across diverse markets, facilitating large economies of scope and creating barriers to entry. However, it is extremely challenging to tap into the wealth of data generated and held by online platforms, due to the lack of interoperability and common APIs which makes it difficult for competitors to compete effectively, and for users to port or multi-home their own information. Furthermore, the accumulation of a huge amount of non-rivalrous data from large user bases and different markets allows large platforms to produce highly personalised user profiles that can be leveraged by the platform itself (for instance affording e-commerce platforms more information about user demand and a competitive edge over sellers on its marketplace who do not have this data) or sold to third parties for targeted advertising. This further exacerbates the disadvantage of competing platforms in the valuable online advertising business.

A new ex-ante regulatory framework should target the large online gatekeepers that exhibit the key characteristics that allow them to rapidly enter a new market and capture it by creating barriers to marginalise their competitors and jeopardise future market contestability. These characteristics are common to major players in B2B and B2P2C digital environments that are prone to becoming gatekeepers and to concentration such as operating systems, online advertising and ad exchanges, web search engines, voice assistants, and cloud computing.

For regulatory purposes, it is difficult to capture all these digital gatekeepers in a single blanket definition that describes the complex nature of their competitive dynamics in an exhaustive manner. These platforms should be identified through a methodology that allows for a dynamic, case-by-case assessment of the companies that should be subject to ex-ante regulation, testing them against the relevant criteria that reflect the competitive dynamics of digital markets. Several criteria and tests have been proposed in the literature and in various expert reports to identify large online platforms acting as gatekeepers that should be subject to targeted legislative intervention. We recommend that the choice of the appropriate test and combination of criteria to define the scope of application of the new legal framework be guided by the following objectives:

• The criteria to identify gatekeepers should be simple enough to enable quick intervention and guarantee legal certainty. They should be objectively set, with reference to well-established economic principles

• Analysis should consider the relationships between the different sides of the market, when looking at multi-sided markets

• Analysis should consider the size and nature of the company's direct and indirect network effects

• The scale of the platform should be evaluated according to the ways it is able to leverage data and user base, its financial and innovation capabilities, its size in relation to its user base and geographic reach

• The gatekeeper role should be established when the company manages to control access to a group of users or markets and sets the rules of the market. Other forms of gatekeeper positions can emerge due to control of data that is difficult to replicate. In all of these cases, other businesses participating in the same ecosystem will depend on this platform, with no real possibility to bypass it or to create an alternative offering, and will suffer from significant imbalances in negotiations with the gatekeeper

## Need for regulation

The chief objective of the new regulation should be to ensure that markets and ecosystems characterised by large platforms acting as gatekeepers remain fair and contestable for innovators, businesses, and new market entrants, ultimately for the benefit of consumers. The new legal framework should consider the high variety of online platforms' business models and digital services and products they provide, as well as the specific harms to be addressed.

Therefore, we support a framework based on a **case-by-case assessment and application of tailored remedies** allowing dynamic adjustments and that are proportionate to the nature and the seriousness of the specific threats to competition and contestability in a targeted market. Following identification of gatekeepers through a multi-criteria test, competent authorities should be empowered to assess the specific competition problems and select the most appropriate remedies to address market failures and abusive practices, ensure contestability in affected markets, and promote consumer choice.
Remedies imposed on individual gatekeepers through a case-by-case assessment should be attuned to the specific competition dynamics associated with the company concerned. As problems arise, remedies will have to be designed, tested, and adjusted by competent authorities in an iterative process. For instance, they could include:

• Access to non-rivalrous data

• Non-discriminatory access to certain key facilities (software/hardware, APIs) which are critical to compete

• Prohibition of restricting content/service interoperability (e.g. allowing multiple app platforms on an Operating System and the possibility to provide services in different Operating Systems)

• Obligation of interoperability of datasets and application programming interfaces (e.g., of customer data for advertising), to facilitate data portability and data exchanges (such as between Operating Systems)

• Enhanced transparency and non-discrimination, e.g. via prohibition of self-preferencing

• Prohibition of bundling/tying with 'must have' services and apps that leads to anti-competitive behaviours

• Prohibition of unfair terms and conditions of a contract (e.g. predatory pricing, non-price terms, requirements to share data, restrictions on use, exclusivity clauses, etc.)

• Separation (accounting, functional, structural) where justified in very exceptional cases (e.g. where there has been persistent failure to achieve effective non-discrimination and where it is unlikely to achieve fair competition after recourse to other remedies)

An additional tool consisting in a **list of prohibited unfair commercial practices** that digital gatekeepers should always be prevented from employing would represent a reasonable complementary safeguard against their basic abusive behaviours by gatekeepers. The prohibited practices enumerated in the list could for instance ban exploitative and unfair terms and conditions in contracts (e.g. obligation to use the platform's own ancillary services or harmful contract modifications with retroactive effect).
It should be noted that relying on general prohibitions alone would be insufficient to address market failures related to a digital gatekeeper in a targeted and proportionate manner. A list of prohibited practices would be based on a static assessment of the behaviours and problems that need addressing today and would not allow for a future-proof, dynamic adjustment to all emerging issues in the competitive landscape of digital economy. As a result, one size fits all rules would not be flexible enough to guarantee competition and contestability in continuously evolving digital ecosystems. Additionally, situations of very specific abusive behaviours might require structural remedies that cannot be contemplated as part of a blanket list of behavioural prohibitions, irrespective of the actual and specific harms caused to platform's competitors.

A list of prohibited practises for large online platforms would therefore have its greatest value only as a complement to a framework that empowers competent authorities to adopt tailor-made remedies addressed to individual gatekeepers on a case-by-case basis, where necessary and justified.

Finally, the GSMA and ETNO believe that a single properly defined instrument that provides for a case-by-case imposition of targeted remedies on individual large online platforms with gatekeeper power would be sufficient to tackle asymmetries and solve issues when the current competition framework is not enough. In this regard, we see the risk that the New Competition Tool would overlap with an ex-ante regulatory framework for digital gatekeepers articulated through the DSA.

## Institutional set-up

Imposition, supervision and enforcement of these new rules would be best undertaken at EU level, since large online platforms operate in global ecosystems and competition concerns arising in digital markets have an important cross-border dimension. Nevertheless, as the effects of platforms' abusive conducts may differ across Member States or emerge only in single Member States, coordination with and among national competent authorities remains crucial.

An adequately resourced EU body should be primarily responsible for monitoring markets and enforcing dedicated rules for major digital gatekeepers. This body should be vested with adequate investigative powers, as well as with oversight and monitoring powers that would enable it to collect relevant information from digital firms to fully appreciate the competitive dynamics of digital ecosystems.

The EU body would also coordinate and advise national authorities and facilitate cross-border cooperation among them, to guarantee a harmonised implementation of rules. Where a single decision is made affecting the EU single market, a single right of appeal at an EU level should be provided.