Digital Services Act

Joint Position by the GSMA and ETNO

April 2021

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**

Policy Contact:
Pierantonio Rizzo
Senior Manager, EU Affairs, GSMA
Prizzo@gsma.com

Policy Contact:
Ross Creelman
Public Policy Manager, ETNO
Creelman@etno.eu

Since the adoption of the eCommerce Directive (eCD) in 2000, the use of digital services has increased considerably. Last year, almost 85 percent of all individuals in the EU-28, aged between 16 and 74 years, were 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-uploaded content to society has drastically increased.

Digital infrastructure, tools and technologies have proved to be extremely resilient throughout the Coronavirus crisis. The speed and scale at which all aspects of life and commerce have shifted online as a result of the crisis has been a huge success story. However, this digital dependency also presents us with some challenges. Risks that already existed in the digital ecosystem have intensified because of the increased reliance on digital services and platforms, for example: exposure to illegal content, services and goods online, as well as the dissemination of viral misinformation. The GSMA and ETNO believe the Digital Services Act (DSA) has the potential to restore citizens' trust and increase consumer protection online by creating a harmonised EU legal framework applicable to all service providers offering their content, goods or services within the European Union.

We believe it is possible to achieve this goal while respecting internet freedoms and protecting the basic principles enshrined in the eCD. In particular, we welcome the fact that the key principles of the existing legal framework for online intermediaries have been preserved, namely the country-of-origin principle, conditional liability exemptions for online intermediaries and the prohibition of general monitoring. At the same time, new proposals included in the DSA, such as the appointment of a legal representative, will improve the effectiveness of the Regulation.

Subject-matter, Scope and Definitions

This legislative initiative is of high importance for GSMA and ETNO since it regulates and affects a range of information society services provided by our members. Predominantly, these services consist in the provision of connectivity and internet access ('mere conduit') but it also includes a variety of cloud services ('hosting').

In this context, we welcome the Commission's recognition that not all platforms impact citizens in the same way and some digital actors should have an increased responsibility to keep digital services free from illegal material and ensure that the Rule of Law is respected online with the same rigour as it is offline. However, there remains room for improvement, and a more nuanced approach regarding the new obligations should be considered. With specific regard to cloud services, more precise distinctions should be introduced to take full account of the nature of these services. Relevant in this regard is the providers' technical capability to identify and, potentially, remove specific material as well as the extent to which the service disseminates such material to the public or the level of activity exercised by the provider in organising and presenting the material to the recipient[2].

The DSA is meant to create a horizontal framework for all categories of content, products, services and activities on intermediary services. To achieve this objective, it is key to set clear definitions that would allow the DSA to be a future-proof and agile legal instrument. In this respect, we wish to draw attention on the following definitions that we believe should be better clarified in the course of the co-legislative procedure:

1. Digital Economy and Society Statistics, Eurostat, 2020.
2. For example by organising, promoting or otherwise curating the material in a way which goes beyond merely passive hosting.

• Information Society Services (Article 2(a)):
The definition of Information Society Services does not sufficiently clarify that services provided against users' data, which do not require monetary payment but are only apparently 'free', should be considered as being provided against remuneration. The Digital Services Act should take this element into account, in line with other recent EU legislation, including the Digital Content Directive[3], the Platform-to-Business Regulation and the Omnibus Directive, which explicitly introduce the principle of data as counter-performance.

• Recipient of the Service (Article 2(b)):
We note that the term 'recipient of the service' is used indistinctly throughout the Regulation to indicate a number of different actors along the chain, ranging from the business-customer to the end-user of the service. We believe that the DSA should be more punctuated and make more readily understandable whether the notion addresses any potential recipients (around the world) or a specific recipient of the service. This distinction appears to be particularly relevant for a number of provisions such as Articles 9(2)(a), 15(1), 15(2)(f), 17, 22 and 31(5).

• Illegal Content (Article 2(g)):
We welcome the Commission's approach to focus the provisions of this Regulation on illegal content. For the sake of proportionality and the preservation of fundamental rights, it is necessary to maintain different regimes applicable to content that is illegal from content that is harmful but legal. In this respect, we believe that the co-regulatory[4] framework designed by the European Democracy Action plan, which builds on the risk mitigation measures established in Articles 26 to 28 of the draft DSA and will be enhanced by the Code of Practice on Disinformation, is a balanced and needed European response.

• Online Platform (Article 2(h)):
We support the distinction between a traditional hosting service, on the one hand, and an online platform service as a different category of intermediary, on the other hand. The DSA should distinguish between platforms aggregating different on-demand content services (such as a platform assembling a number of (third-party) VoD services) from video-sharing platforms[5] which are driven primarily by UGC where users have the possibility to interact. For the first category, the risks highlighted under the DSA (and corresponding obligations) are much less likely to arise.

• Dissemination to the Public (Article 2(i)):
The definition of 'dissemination to the public' and its interpretation in the corresponding Recital 14 should be consistent with the agreed wording of the Terrorist Content Regulation[6].

3. Recital 24 and Article 3(1) of the Digital Content Directive, Directive (EU) 2019/770
4. See also the GSMA views on the European Democracy Action Plan
5. Definition of 'video-sharing platform service' in Article 1(b) of the AVMSD, Directive (EU) 2018/1808
6. Definition of 'dissemination to the public' in Recital 14 of the TCO Regulation adopted by the Council of the EU on 18 March 2021

Mere Conduit and Provisions Applicable to All Intermediary Services

GSMA and ETNO welcome the maintenance of the definition of 'mere conduit' and 'caching' services and the fact that, overall, the new obligations applicable to all intermediaries aim at harmonising rules and procedures across the EU to ensure greater legal predictability and consistency for business users. In particular, we highlight the following aspects:

• Mere Conduit (Article 3):
Internet access services (IAS) are subject to the 'Open Internet' Regulation[7] that prohibits to block, slow down, alter, restrict, interfere with, degrade or discriminate against specific content, applications or services and only allows blocking if that is based on Union legislative acts, or national legislation that complies with Union law. Today, providers of IAS remove illegal content based on blocking injunctions issued by competent authorities at the Member State level. This is an effective system for providers of IAS and should remain in place. We would welcome more clarity and guidance on the role of Internet Service Providers in blocking illegal content, particularly considering the interplay between the so-called "net neutrality" rules and voluntary measures aimed at removing content foreseen in Article 6.

• Monitoring (Article 6 & 7):
As a cornerstone of the open Internet, we fully agree that the principle of "no general monitoring" should be maintained in order to protect users' privacy and freedom of expression and information. At the same time, intermediary services should be encouraged to take voluntary and targeted measures to detect and remove illegal content without losing their liability exemption when doing so, as long as these measures remain targeted and do not constitute general monitoring.

• Orders to act against illegal content (Article 8):
Orders must be proportionate and justified and should always consider the technical feasibility of the measures being ordered. In particular, this is relevant for Internet Access Service (IAS) Providers that simply execute the order received and do not assess the content subjected to blocking. Therefore, when issuing blocking injunctions, public authorities should be obliged to cover IAS providers' resulting costs, and indemnification against potential claims for the action taken as ordered should be foreseen. Furthermore, the relationship of such orders and notice-and-action requests should be clarified. The competence to issue orders should be aligned with the country-of-origin principle. Particularly in cross-border situations, it will be necessary to foresee procedural safeguards to have the legality of orders checked.

• Legal Representatives (Article 11):
We strongly support that all service providers offering services in the EU should be subject to the EU rules, irrespective of their place of main establishment. Undertakings in third countries that provide services to EU users should be required to have a representative and a legal point of contact 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 Terrorist Content Online Regulation, 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.

• Transparency Reporting (Article 13):
We find that the reporting obligations in Article 13 and Recital 39 essentially duplicate the requirement of Article 44(2)(b) which obliges a Digital Services Coordinator to provide annual reports on the number of removal orders issued by judicial and administrative authorities. We reiterate that providers of IAS do not monitor traffic over their networks and providers of these services have no knowledge, control or management activity over the content that users upload and exchange when using their services. Consequently, we believe such a reporting requirement is unnecessarily burdensome and disproportionate for the intermediaries in question and should be limited to 'online platforms'.

7. Article 3(3)(a) of the Telecoms Single Market Regulation (EU) 2015/2120

Hosting Service Providers

The definition and responsibilities attributable to hosting services providers have long been debated since the adoption of the eCD, while the emergence of new digital services with different characteristics has added further complexity to this issue. In this respect, the proposal falls short in designing an effective and proportionate approach to content removal, which recognises the diverse technical characteristics of hosting services in the digital ecosystem and targets new obligations at service providers that contribute to the dissemination of illegal content online, and at those service providers that are best placed to act.

In order to ensure effectiveness and proportionality, **the removal of illegal content should happen as close to the source as possible. New rules should also have due regard to the underlying technical capabilities of a given service provider in order to avoid imposing obligations that are not proportionate or not technically feasible.** The DSA should take into account the principle of **'available technical capabilities'** of the hosting service provider, namely where platforms retain (or can easily put in place) the means to address the problem in the most expedient and proportionate manner, including the abilities to identify and remove users' specific content on a piece-by-piece basis, or to demand, based on contractual obligations, that its customer should remove notified illegal content.

This is particularly relevant for Cloud Service Providers (and other non-hosting intermediaries such as Domain Name Systems or Content Delivery Networks) that do not have visibility of or control over content, nor can offer granularity in removing specific content or suspend individual end-user accounts. In our members' experience, customer traffic circulating on the cloud is encrypted and, as a result, the only option at their disposal is to block the entire service provided to a customer, when requested by a competent authority. Therefore it should be explicitly mentioned that application of Articles 14 and 15 should be limited to hosting services provider, including online platform, that have the technical and contractual possibility to act on specific content.

Moreover, we would welcome an explicit acknowledgement in the DSA Regulation of the importance of cascading responsibilities to tackle illegal content. Notice and action at the level of the hosting service level should be the principal mechanism for removing illegal content, with blocking injunctions being the last resort.

• Notice & Action (Article 14):
We support a standardised and harmonised form of reporting so as to empower users, ensure transparency, and increase the possibility for redress for wrongly flagged content. However, Article 14 should clarify that the notifying individual or entity should at first direct its notice to the entity that has a clear view about the illegal activity. Moreover, regarding identification of the person who sends the report, some disclosure of identity is important for the sake of tackling potential misuse (e.g. attempts to "silence other users") but it should remain voluntary.

• Statement of Reasons (Article 15):
Considering the different characteristics and roles in managing the content among hosting service providers, the provision in Article 15(4) is disproportionally burdensome, as it requires the publication of the decisions and the statements of reasons in a publicly accessible database managed by the Commission. This requirement should be limited to 'online platforms'. Nevertheless, the hosting service provider's obligation to inform recipients of the service about the removal of content should not compromise criminal investigations e.g. in case the reported/removed illegal content involves serious crime.

Online Platforms

The distinction between hosting services and 'online platforms' which store and disseminate information to the public at the request of the recipient of the service is of paramount importance to properly attributing responsibilities and liability in the value chain.

GSMA and ETNO find as a positive step the European Commission's intention to preserve the eCD's definition of 'hosting' while distinguishing hosting services in the broad sense from 'online platforms' (and 'very large online platforms'). Nevertheless, consideration should also be given to qualitative criteria to achieve a proportionate and future-proof framework, while rendering the distinction with mere passive hosting services clearer.

When going beyond provisions applicable to all hosting service providers, we suggest the following cumulative criteria to establish obligations for 'online platforms':

1. Dissemination to the Public:
the test for dissemination to the public should take into account where the actual risk results from a specific online platform, such as the sharing of illegal user-generated content to the public and how a service is actually being used. Recital 13 of the DSA outlines that providers of hosting services should not be considered as online platforms where the dissemination to the public is merely a minor and purely ancillary feature of another service. Moreover, Recital 14 provides a helpful clarification specifying the concept of 'dissemination to the public' as the making available of information to a potentially unlimited number of persons without further action by the recipient of the service. This element is of paramount importance for cloud storage services where content is shared (if at all) within a closed group subscribed to the service but it can also be further disseminated, or access provided, to a broader audience outside the control of the cloud provider[8]. We consider that the DSA should provide clear guidance as to what obligations apply for hyperlinking by clarifying that cloud service providers do not perform an act of communication to the public within the meaning of the DSA when a user makes content hosted by the cloud provider available through the provision of a hyperlink.

2. Interaction with user-generated content:
building on the notion of active hosting service provider developed in the jurisprudence of the CJEU[9], regulatory focus should be given to those online platforms that play an active role in the dissemination of material, uploaded by their users, to the final recipient/end-user. We believe this criteria is particularly helpful to determine providers that are best placed to take action to address illegal content, and it should be taken into account at least when defining, and establishing additional obligations for, online platforms and very large online platforms.

8. E.g. if the hyperlink generated by the cloud service provider is subsequently shared by the user on a social media platform.

9. In its Google France and L'Oréal v. eBay decisions, the CJEU formulates the distinction between active and passive service providers. It should be considered active that provider that 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.

Concerning the obligations applicable to online platforms, we recommend the following suggestions:

• Out-of-court settlement (Article 18):
Bodies established by Member States to solve out-of-court disputes should always be impartial, independent and have expertise in issues arising from illegal content, goods or services, and must be certified by a valid entity to do so. A recipient of the service, who wishes to raise a case, should be obliged to pay a basic fee to avoid a misuse of the system. Article 18(3) should be amended accordingly.

• Trusted flaggers (Article 19):
Reliable notifiers could be helpful to identify the presence of illegal content online and ensure a more effective enforcement against those online platforms that allow the sharing of user generated-content with the public. These Trusted Flaggers should be public or private entities (not individuals) and must be duly accredited and independent. If public entities are at hand, the relationship between their capacity as Trusted Flagger, on the one hand, and issuer of injunctions or orders, should be clarified. In any event, in essence the same level of procedural and substantive rights' protection should be secured irrespective of the role eventually assumed by a public authority or other State body. The various national administrations should share their official list of trusted flaggers with the other EU Member States and update them regularly, so that their actions are valid and legitimate when they act at European level. EU Member States should further improve cooperation, both among themselves, and with third parties in order to contribute to swift action against illegal content. This acknowledges that hosting service providers' effective actions strongly depend on an effective interplay with authorities and other involved stakeholders.

• Notification of suspicions of criminal offences (Article 21):
The hierarchy proposed in Article 21 fails to take into account that not all online platforms have the same resources to deal with enforcement and judicial authorities. In our view, where an online platform becomes aware of any suspicions of criminal offences, it shall inform the authorities of the Member State(s) concerned or one of the Member State in which it is established or the provider has its legal representative, or inform Europol. This proposed approach will equally preserve the possibility for online platforms to directly inform the authority of the Member State concerned of the suspicion if they have the capacity to do so without hampering the Country of Origin principle.

• Traceability of traders (Article 22):
We welcome the introduction of Know Your Business Customer (KYBC) obligations that should apply to online platforms that primarily deal with the selling of goods online (such as online marketplaces). However, it should be noted that online platforms are not always in the position of assessing or obtaining updated and verified information about the traders. In this respect, we support the 'reasonable efforts' approach provided in Article 22(2). It should also be noted in the legislative process that an unintended expansion of the KYBC provisions on all digital services - beyond online platforms - would impact on existing cloud providers' scalability of their cloud services and create significant barriers to the delivery of cloud services in Europe.

Regulatory Oversight and Transposition

GSMA and ETNO support effective law enforcement and the establishment of better market intelligence. Overlapping competencies that lead to legal uncertainty and bureaucracy must be avoided, while stronger cooperation of the relevant authorities should be ensured. In particular:

• Penalties (Article 42):
The aim of this Regulation should be to achieve maximum harmonisation. Therefore, Member States should lay down the same rules on penalties applicable to same infringements, as per Article 83 of the GDPR. The imposition of penalties should be limited to hosting services where there is communication to the public (i.e. online platforms as well as VLOPs). Providers of mere conduit and caching services are prevented from actively searching for illegal content and would instead react to injunctions issued by public authorities. We recommend that the wording of the provision in Article 20 of eCD on sanctions be preserved for the categories of mere conduit, caching and hosting service providers other than (very large) online platforms.

• Right to lodge complaints (Article 43):
The provisions on the right to lodge a complaint appear to duplicate the rights of recipients of a service. Under articles 14 and 15, recipients already have the right to lodge a complaint to the intermediary, as well as request an out-of-court dispute resolution (Article 18).

• Fines (Article 59(2)):
Fines applicable to the persons referred to in Article 52(1) other than VLOPs should be limited to intentional infringements and do not cover negligent behaviours.

• Digital Coordinators powers (Articles 61 and 62):
More clarity regarding the limitation and enforcement powers of Digital Services Coordinators should be provided. In addition, we believe that more guidance should be given on what are 'proportionate and necessary remedies' (Article 41(2) b) (e.g. a list of proposed remedies).

• Entry into force (Article 74):
An appropriate extension of the starting date of application of the Regulation, i.e. to 12 months following its publication, should be considered due to the complex requirements foreseen by it, including the administrative bodies that would need to be established, as opposed to the three months currently foreseen in the proposed Regulation.

GSMA EUROPE
Regent Park, 1st Floor,
Boulevard du Régent 35,
1000 Brussels, Belgium
www.gsma.com/gsmaeurope

ETNO
Boulevard du Régent 43-44,
1000 Brussels, Belgium
www.etno.eu