# ASSOCIATION OF COMMERCIAL TELEVISION IN EUROPE

# POSITION PAPER ON THE DIGITAL SERVICES ACT

## EC PROPOSAL FOR A REGULATION ON A SINGLE MARKET FOR DIGITAL SERVICES


### MEMBERS & PURPOSE - ASSOCIATION OF COMMERCIAL TELEVISION IN EUROPE (ACT)

ACT member companies finance, produce, promote and distribute content and services benefiting millions of Europeans across all platforms. At ACT we believe that the healthy and sustainable commercial broadcasting sector has an important role to play in Europe's economy, society and cultures. Commercial broadcasters are at the heart of Europe's media landscape as producers and distributors of European original content and news. We embrace the digital environment providing new services, formats and content to meet the growing European demand for quality content on various distribution models.

### FACTS & FIGURES – TV IN EUROPE (ACT)

# INITIAL REMARKS

The DSA addresses issues and areas Broadcasters are faced with on a daily basis, as players that stand at the nexus of media, technology, news and data policy. The DSA has a specific media dimension. ACT stresses the importance of seeing these proposals in light of fostering pluralism, safeguarding the rule of law whilst delivering innovative digital services, quality entertainment and trusted news.

The guiding mantra to benchmark the DSA - to ensure that **what is illegal offline should be illegal online** – requires to be further and fully reflected in the text and discussions amongst co-legislators. This is at the core of broadcasters view on the proposals to achieve an **effective level playing field for creative industries and viewer protections**.

Broadcasters and **media pluralism at large requires a strong liability regime** that can deliver a safe online and trustworthy environment, effective enforcement as well as ensuring that the Internet continues to fulfil its role as the vibrant and engaging place we all enjoy. While some players can continue benefiting from liability exemptions, the **DSA should not by any means grant additional liability privileges**.

The proposed regulation should reflect the present realities of the market, where several players have emerged that have surpassed "mere technical, automatic and passive nature" status.

Enlarging the **liability exemptions** to accommodate this new type of intermediaries will prove **detrimental to the content creation market** which needs more robust instruments to fight against the illegal dissemination of their content online and would fall short of answering market demand.

The proposed **notice and action procedures** will have to be analysed in light of existing copyright laws to ensure processes that lead to **rapid take down and stay down measures** can continue to be applied and improved.

Co-legislators may wish to assess lost opportunities to **crack down on online TV piracy**. The role and scope of trusted flaggers and Know Your Business Customer provisions are too narrow to effectively target and suspend abusive behaviour. Unless more is done in this respect, the broadcasting industry will suffer from online piracy for many years to come.

Similarly, there is no logical reason for **digital platforms** to **avoid liability for advertising content** which they select, place, promote and ultimately profit from. An effective regime should ensure that digital platforms are directly liable for all advertising content on their services and are held to account for content that falls short of generally accepted standards – as is the case for broadcasters.

We welcome the proposal's ability to **achieve more accountability regarding harmful content**, particularly as regards disinformation. Stringent codes of conduct will be required to **achieve tangible and verifiable results, commitments and oversight**. Mandatory independent audits imposed on very large platforms – essential to assess if these platforms effectively fight against illegal/harmful content and protect fundamental freedoms online – is a first, but not sufficient, step towards **much greater and needed algorithmic transparency**. In sum, while certain measures are in line with the needs of media pluralism and cultural sovereignty in Europe, others **will need to be revised to ensure the DSA presents a real upgrade for Europe's media ecosystem**.

ACT and members look forward to engaging with European institutions on both of these proposals. The diagnosis delivered by the EC is accurate. Now we must make sure the cure is effective. We will continue to advocate for **fair competition and a liability landscape that is fit for the digital age** in order to drive Europe's media strategy and support a robust, responsible and reliable media landscape.

# EXECUTIVE SUMMARY - KEY AREAS OF FOCUS FOR BROADCASTERS

## *SECTION I: CONDITIONAL LIABILITY EXEMPTIONS (Chapter II, Articles 3-9)*

### 1.1. Active/Passive distinction (Articles 3-5; 18, 20, 23)

- The requalification of articles 3-5 of the eCommerce Directive creates ambiguity and needs to better reflect the rich jurisprudence of the CJEU and national courts
- Online intermediaries that take active measures to maximise profit and consumer attention should be held liable based on criteria "optimising the presentation or promoting the content" in line with CJEU case law (L'Oréal/eBay) regardless of size
- No special regime for small players (small broadcasters have no such benefits)

### 1.2. Make the exemption of liability conditional on the compliance with due diligence obligations (Article 5; Recital 18)

- Mandatory compliance with due diligence obligations should be a necessary precondition of eligibility for liability exemptions

### 1.3. "Good Samaritan" Principle (Article 6)

- "Good Samaritan" principle goes against established EU doctrine and will create a weaker system to the detriment of the European interest and online safety of European citizens; legislators should refrain from creating new liability exemptions
- The basis for the Good Samaritan – removing alleged disincentives for platforms to proactively act against illegal content – is not supported by any factual evidence and disregards already applicable duties of care on passive hosts in the eCommerce Directive
- It is not acceptable for online intermediaries to decide by themselves which kind of illegal content they intend to track or not track

### 1.4. Orders to act against illegal content/ Catalogue wide injunctions (Article 8; Recitals 29-30)

- Preserving the standing of national orders is important, yet Member States need greater standing to issue injunctions
- Both the applicable DSA recital and 2017 Communication do not elaborate practical basis to tackle new forms of piracy such as illegal IPTV and illegal live streaming
- DSA Article should reflect practical arrangements to terminate or prevent an infringement allowing courts to issue forward looking, catalogue-wide and dynamic injunctions

### 1.5. Orders to provide information (Article 9; Recitals 31-33)

- To ensure information requests are effective, the language provided in Article 15.2 (ECD) should be mirrored in Art. 9 of the DSA ;namely requests by competent authorities enabling the identification of recipients of their service with whom information society service providers have storage agreements
- It is essential that the scope of these articles is explicitly limited to cross-border orders in order to avoid unnecessary overregulation and interference in Member States' judicial laws

### 1.6. Content moderation (Article 12; Recital 38)

- We welcome the introduction of an obligation for all providers of intermediary services to clearly describe in their terms and conditions and to enforce in a diligent manner any policies, procedures, measures and tools used for the purpose of content moderation and recommender systems

## *SECTION II: DUE DILLIGENCE OBLIGATIONS FOR A TRANSPARENT & SAFE ONLINE ENVIRONMENT (Chapter III)*

### 2.1 Notice and Action Procedures (Articles 5,14; Recitals 40,42)

- In practice, broadcasters face organisations that tend to escape their expeditious removal obligations; ACT suggests to expand the definition of the hosting services providers and simplify procedures
- Requirements proposed diminish the nature and effectiveness of the existing notice & take down procedures and need futureproofing to ensure they are not obsolete upon publication
- The title of the copyrighted content and the logo of the broadcaster are and should remain sufficient to trigger the validity of the notice as already validated by rulings

### 2.2 Trusted flaggers (Article 15,19; Recital 46)

- Trusted flagger system should become a standard for all hosting service providers; exclusion of micro and small enterprises misses sources of specific, prevalent and damaging types of pirated content
- The status should be refined in the proposal to recognise that the scope of entities needs to be wider than collective interests to allow for IP rightholders and their partners to effectively tackle illegal use of their content and continue to rely and develop existing best practices
- An obligation for hosting providers to treat notices from trusted flaggers with priority – and immediately for live content – should be combined with a fast track take-down procedure

### 2.3 Repeat infringer policy (Article 20; Recital 47)

- Repeat infringer counter-measures are welcome and to be effective need to capture micro & small entities hosting repeat infringers
- Account suspension duration (for *a reasonable period of time*) would benefit from specifications to avoid disparities in interpretations and subsequent transpositions
- The scope of suspensive measures should be widened to tackle the network of online and dynamic pirate accounts with stay down measures and termination of service for repeat infringers across all accounts
- Illegal content repeatedly uploaded should stay down

### 2.4 Know Your Business Customer (Article 22 NEW; Recitals 48-50)

- KYBC obligations should apply to providers of information society services that piracy services and other illegal operators rely on
- Requiring commercial entities to reveal their identity on the internet would automatically reduce illegal or harmful content online

### 2.5 Transparency reporting obligations for providers for online platforms & online advertising (Articles 13, 16, 23-24)

- There should not be any distinction between illegal content and manifestly illegal content
- The compliance with the due diligence obligations for a transparent and safe online environment should not be seen as burdensome
- Adapting the reach of the law to only parts of the market (digital SMEs structurally advantaged vs physical SMEs), sets a dangerous precedent and should be avoided

## *SECTION III: ADDITIONAL OBLIGATIONS FOR VERY LARGE ONLINE PLATFORMS TO MANAGE SYSTEMIC RISKS FOR ILLEGAL AND HARMFUL CONTENT*

### 3.1. Risk assessment (Article 26)

- Threshold foreseen by the Commission to qualify risk as (significantly) systemic are high. The assessment should be made in light of the prejudicial nature it has on a certain sector.
- The dissemination of illegal content, infringing property rights - fully protected by Article 17 of the Charter of Fundamental Rights - should be considered as a sufficiently prejudicial risk
- Safeguards are required to preserve media integrity and avoid oversight role over broadcasters' pre-vetted and regulated content

### 3.2. Mitigation of risks (Article 27; Recitals 56-58)

- Regulators should have a greater role and means to compel commitments, voluntary "Codes of Conducts" and "Crisis protocols" should be more robust to qualify as effective mitigation measures

### 3.3. Transparency measures for very large online platforms (Articles 28-29)

- Content providers should be informed, ideally in advance, about any modification to the algorithm and the foreseen consequences on the visibility of third party content

### 3.4. Additional online advertising transparency (Article 30)

- We welcome the obligations as foreseen in Art. 24 and 30 as the very large online platforms monetize their business through online advertising. These obligations would help creating a trusted and transparent online environment. Broadcasters already comply with a comprehensive set of legal and self-regulatory rules for their online and offline offerings. Personalized advertising, which meets the same high standards, is an increasingly crucial source of revenue for media companies that don't have the reach and massive data collection of the dominant online platforms.
- Meaningful transparency measures require verifiability and open data access for regulators
- To fully assess flows of illegal/harmful content on ad networks a self-declarative approach cannot be a substitute for independent oversight and national regulatory approaches

### 3.5. Data access and scrutiny (Article 31; Recital 64)

- Supervision of VLOP's recommendation and moderation algorithms upon request of the Digital Services Coordinator to address pro illegal or harmful content biases should be the norm
- Princle of compliance should prevail over trade secrets to prevent the dissemination of illegal content online
- Trade secrets shall not be opposed by VLOPs to the Digital Services Coordinator, and obligations like explainability, transparency by design and active collaboration with the Digital Services Coordinator (DSC) on algorithms' purposes should be included in DSA
- DSC should be entitled to have access to all data and algorithms requested for their investigation to ensure that VLOPs are DSA compliant. Vetted researchers should be able to conduct studies on the DSA and thus require data to the VLOPs.

### 3.6. Codes of conducts (Article 35; Recitals 67-68)

- To deliver a true regulatory backstop, the DSA will need to be bolstered with complementary measures
- For harmful content, and associated Code of Practice on online disinformation, there is a pressing need for guidance that delivers a step change in commitments and allows regulators powers to compel a platform to adhere in good faith to a high standard co-regulatory framework, with binding commitments and enforcement with penalties

## *SECTION IV: IMPLEMENTATION, COOPERATION, SANCTIONS AND ENFORCEMENT (CHAPTER IV)*

- The viral spread of illegal and harmful content has dramatic impact and needs immediate attention, procedures need to be streamlined to ensure the Commission can take the lead
- Relevant authorities should have the power to request and suggest commitments by VLOPs

# SECTION I: CONDITIONAL LIABILITY EXEMPTIONS (Chapter II, Articles 3-9)

## 1.1 Active/Passive distinction (Articles 3-5)

**Jurisprudence.** ACT has always stressed the need for maintaining the crucial distinction between active/passive intermediaries and update it in light of CJEU jurisprudence[1]. The rich jurisprudence of the CJEU and national courts is not reflected in the approach to the conditional exemption of liability for online intermediaries.

Online intermediaries that take active measures to maximise profit and consumer attention by designing their algorithms to index and recommend content for commercial gains, play an active role and should be held liable for the content they disseminate. The optimisation of illegal and harmful content drives massive advertising revenues for these services. This is further evidence of the fact that they are not neutral nor passive vis-a-vis the content that is made available and augmented on their platforms.

**ECD/Requalification of active/passive distinction.** While the definition of "mere conduit", "caching" and "hosting services" (Art. 3-5) are largely similar to the provisions of the eCommerce Directive, the active/passive distinction is *de facto* requalified as active/neutral (Recitals 18, 20 and 23). This requalification creates ambiguity despite attempting to provide more clarity on the basis of the active/passive distinction, especially as set out in Recital 18 ("*the provider of intermediary services who plays an active role of such a kind as to give it knowledge of, or control over, that information")*. An intermediary that takes an editorial decision over content should not benefit from the liability limitations.

**Key criteria for effective liability & scope.** The key criteria for liability is and should remain "*optimising the presentation or promoting the content*" (regardless of whether this happens in an automated way or not) in line with CJEU case law (L'Oréal/eBay). We would also caution against the concept of "*deliberate collaboration*" (see Recital 20) which is a too high threshold and appears difficult to prove in practice. The criteria of "*engaging in*" is more suitable.

While we understand the need to avoid a one-size-fits-all approach, the DSA should tackle rogue players regardless of their size. Size cannot be a criteria for existing rules. Exemptions for small players are exclusively provided for online intermediaries. Small broadcasters do not benefit from the same exceptions, and we as such encourage policy-makers to not adopt a two-tier approach to the law by allowing small rogue players to continue their illegal activities in a legal vacuum. Any new classification should uphold the EU *acquis*[2].

## 1.2 Exemption from liability conditional on the compliance with due diligence obligations (Article 5a)

**Conditionality.** Providers of hosting services including online platforms should be deemed ineligible for the liability exemptions foreseen in Article 5. Mandatory compliance with due diligence obligations should be a precondition of eligibility for liability exemptions. This is an effective solution to ensure compliance with the Regulation. This conditional approach to liability exemptions produces more tangible results and incentives; specifically in cases where penalties foreseen could be factored in as a cost of doing business, rather than genuinely adhering to the principle of delivering a higher level of safety online and increase in consumer trust.

[1] www.acte.be/publication/ACT-perspectives-on-the-digital-services-act
[2] See Annex I for some relevant ECJ decisions

### 1.3. "Good Samaritan" Principle (Article 6)

**Legal certainty.** We question the legal certainty this principle brings in comparison to clear and long established CJEU jurisprudence on "active hosts", clearly indicating that intermediaries optimising content do not have a neutral position and are therefore not entitled to the privileges of liability exemptions. The so-called "Good Samaritan" (GS) principle would only benefit certain large online platforms rather than the European interest or a safer online space.

**Established jurisprudence**. The GS principle goes against established EU doctrine and risks being abused by active platforms looking to avoid liability entirely. Without a strong safeguard this will create a weaker system. Liability of active hosting platforms needs to be bolstered, not watered down. Article 6 introduces the concept of removing alleged disincentives for platforms to proactively act against illegal content. Yet there is no evidence to support the existence of said alleged disincentives. Moreover, the assumption that platforms need protections to avoid losing their "passive host" status, fails to recognise that duties of care are already applicable to passive hosts in the eCommerce Directive (Recitals 40, 48).

**Perverse incentives.** The principle creates a perverse incentive for active hosting platforms to requalify themselves in order to ensure they are shielded from liability. The EU needs to strengthen its tools to ensure that citizens in the EU are afforded a high level of protection, alongside being well informed from a plurality of perspectives. Without safeguards, online intermediaries will always be impermeable to CJEU caselaw and will never be requalified as active and fully liable. Allowing online intermediaries to decide for themselves the type of illegal content they choose to track or not may not necessarily align with effective prioritisation of illegal and harmful content which negatively impact EU citizens.

### 1.4. Orders to act against illegal content/Catalogue-wide and dynamic injunctions (Article 8)

**Reinforce legal basis.** It is of the utmost importance that judicial or administrative authorities may bolster their courts' ability to issue forward looking, catalogue-wide and agile injunctions. This allows for effective tackling of new forms of IP infringements, such as illegal internet protocol television (IPTV) and other forms of illegal (live) streaming. As of today, the EU Commission only advocates[3] that such measures are not contrary to Article 11 of the Directive[4]. The proposed regulation on the DSA, only recalls in its recitals that the liability regime does not affect the possibility for a court or administrative authority, to issue injunction to terminate or prevent an infringement (Recital 24). This is not sufficient. In some Member States, such as France, Courts remain reluctant to issue such injunctions without a greater legal basis to buttress their opinion.

**Scope.** Orders to act usually don't focus on a specific item but rather on the domain names of the platforms via which the illegal content is made available. The order usually aims at disabling access to a website or blocking IP addresses. Also, the exact uniform resource locators (URLs) can't be deemed necessary to identify the illegal material on a platform service. Furthermore, the requirement to have the order drafted in the language of the provider risks slowing down the process. Relevant national judicial or administrative authorities should be allowed to send orders in their national languages.

[3] 2017 Communication intended to provide guidance on the enforcement of the IPRED Directive – link
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0048R(01)

### 1.5. Orders to provide information (Article 9)

**Scope of information reflecting practices.** The collection of information should be extended beyond information already obtained by the provider in order to avoid jeopardising the effectiveness of the provision and conflict with the practices currently carried out under the e-Commerce Directive. Article 15.2 ECD already allows providers to collect information that effectively enables the identification of the recipient of the service[5]. To ensure information requests are effective, the language provided in Article 15.2 of the ECD should be mirrored in Art. 9 of the DSA.

**Scope limitation to cross-border orders.** The clear intention of Articles 8 and 9 is to harmonise aspects of orders that are of a cross-border nature. This is however not explicitly reflected in the current wording of the articles; which seem to capture all orders, regardless of their territorial scope. It is essential that the scope of these articles is explicitly limited to cross-border orders in order to avoid unnecessary overregulation and interference in Member States' judicial laws. This limitation is therefore necessary to ensure remedies that currently exist under national law (often by virtue of EU norms) are not undermined.

### 1.6. Content moderation

Recommendation tools and content moderation (or lack thereof) are largely to blame for the spread of illegal and harmful content online. However, they can be part of the solution to address it.

We therefore welcome the introduction in Article 12 of an obligation for all providers of intermediary services to clearly describe in their terms and conditions and to enforce in a diligent manner any policies, procedures, measures and tools used for the purpose of content moderation and recommender systems.

This should include explicit references to how content that is illegal or has the potential to harm users, such as the spread of disinformation, discriminatory content or content that harms minors. In this respect, to publicly know which tools are used to moderate content is not sufficient to understand if algorithms designed by very large online platforms contain biases that promote illegal or harmful content.

Very large online platforms as defined by Article 25 of this Regulation shall not have lawfully uploaded content owned, and editorially selected by an audiovisual media provider as defined in Article 1 Paragraph 1 (a) in the AVMS Directive (2018/1808) unduly obscured, obfuscated or otherwise disabled by virtue of its alleged non-adherence to terms and conditions that go beyond the thresholds applied to legal and harmful requirements applicable in relevant European and national regulations and jurisdictions (see point 3.1.).

[5] "2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements".

# SECTION II: DUE DILIGENCE OBLIGATIONS FOR A TRANSPARENT AND SAFE ONLINE ENVIRONMENT (Chapter III, Section 2, 3, Articles 14-24)

## 2.1 Notice and Action Procedures (Article 14)

Broadcasters need robust and effective instruments with high liability standards for the protection of content on all online service providers. As a whole, the procedures described in the Commission's proposal are limited to hosting providers and are overly burdensome to achieve the desired outcomes.

**Extension of definition of hosting provider**. In practice, broadcasters face organisations that tend to escape their expeditious removal obligations, manipulating their business model in order to argue that they qualify as mere infrastructure providers. This is particularly the case for organisations that do not only provide a web hosting service but also a server leasing service, allowing their customers to offer hosting services to their own subscribers. In order to make sure that such organisations comply with the obligation provided for hosting service providers - namely Article 14 of the DSA Proposal (ie. Notice and Action) - we suggest to adjust the definition of the hosting services providers set forth in Articles 2 and 5 to include the leasing of servers for hosting services.

**Content of notices.** The title of the copyrighted content and the logo of the broadcaster are and should remain sufficient to trigger the validity of the notice as already validated by rulings[6]. Any other more time-consuming requirements are unwarranted and go against the established EU acquis. As such we recommend that a number of clarifying amendments be made to Article 14.

The requirements of the notices which include an explanation of reasons as to why notified content is considered illegal, a statement of good faith, exact URL or URLs, and where necessary additional information enabling the identification of the illegal content (Article 14.2.(b)) are costly and time consuming. The notice and action requirements proposed will diminish the nature and effectiveness of the existing notice and take down procedures, which are already ineffective in respect of content (e.g. live sport) where expeditious take down is a necessity. The requirement to provide for a URL is especially problematic for structurally infringing platforms, particularly as it is not coupled with a robust stay-down obligation.

The systematic re-uploading, for example under a different URL, of content reported as illegal significantly undermines the effectiveness of notice and action systems and has a negative impact on media companies which have to issue multiple takedown requests for the same or similar illegal content. It is a clear signal that the system is being abused. In addition, it is sometimes impossible to extract an URL for an infringing video. The requirement to provide for a URL does not allow for technical innovations or changes. The current wording does not provide for a future proof solution and risks to become obsolete immediately after publication.

## 2.2 Trusted flaggers (Art. 19)

**Scope.** The Commission's decision to exclude from the scope of Chapter III, micro and small enterprises, does not account for the damaging role that such small platforms can play on specific types of pirated content. We firmly believe that ensuring that what is illegal offline is illegal online is dependent on a certain equality in

[6] RTI vs Dailymotion – Ruling of the Court of Rome of 15 July 2019; RTI vs Yahoo – Ruling of the Italian Supreme Court (Corte di Cassazione) of 19 March 2019; RTI vs. Facebook: Ruling of the Court of Rome of 15 February 2019; TI vs VIMEO: Ruling of the Court of Rome of 10 January 2019

front of the law regardless of size. ACT believes that the trusted flagger system should become a standard for all hosting service providers.

**Attribution.** ACT is a strong advocate for IP rightholders and their partners to be recognised as trusted flaggers. We welcome the Commission's proposal to formalise the attribution of such a quality by involving an independent third party (the Digital Services Coordinators), but based on established practices, hosting services should also continue to be able to appoint trusted flaggers. Indeed, some have similar systems in place and collaboration can work. Shifting attribution entirely to DSCs would slow the process down.

Moreover, we are concerned with the requirement that the trusted flagger should represent collective interests in Art. 19.2(b). Such a provision would not qualify our members (and third parties operating notices on their behalf) as trusted flaggers although they have been at the forefront of the evolution of notice and action mechanisms and have invested to develop them. This is a retrograde step from the position today and should be corrected. It is imperative that broadcasters be clearly included so as to preserve their IPR commitments and uphold their rights.

**Expediency.** ACT has insists that the content flagged by trusted flaggers should always trigger a fast track procedure. Whilst the Commission's proposal has the potential to provide with a helpful instrument for the industry, we believe that an obligation for hosting providers to treat notices from trusted flaggers with priority should be combined with a fast track procedure if it is to be effective in the fight against illegal content in a fast paced online environment. As regards infringing live content, when notified by trusted flaggers, the infringing content should be removed immediately.

To this end, we recommend that a number of clarifying amendments be made to Article 15 and respectfully suggest moving Article 19 from Section 3 of Chapter III, to Section 2 of Chapter III in combination with slight alterations for the instrument to become an effective instrument for broadcasters to fight against online piracy.

### 2.3 Repeat infringer policy (Article 20)

**Scope.** ACT welcomes the European Commission's intention to provide legal certainty regarding repeat infringers. We however believe that proportionality in this case is not best served with obligations limited to online platforms and very large online platforms; while dissuasive measure would not apply to micro and small enterprises. For more efficiency in the fight against infringers, we suggest moving Article 20 from Section 3 of Chapter III, to Section 2 of Chapter III.

**Timing of suspension.** Equally, the prospect of suspending the repeat infringing accounts for a reasonable period of time does not constitute a sufficient safeguard in light of the systemic nature of online piracy because it is very easy for users to create new accounts and repeat infringing behaviour. Article 20 should clarify that, just as illegal content repeatedly uploaded should stay down, hosting services should terminate the provision of their services to recipients that frequently provide illegal content, regardless of which account they use to access the service. A small proportion of hosting services already have similar systems in place that work. This should equally be the case for recipients of service that facilitate the dissemination of illegal content.

As such we recommend that a number of clarifying amendments be made to Article 20.

### 2.4 Know Your Business Costumer (KYBC) (Art. 22)

**Scope.** The Commission has proposed the underlying idea of the KYBC in providing for rules requiring platforms to know the identities of traders using their services to promote messages or offer products or services to EU consumers (see Art. 22 and Recital 49). Unfortunately, the scope of the KYBC provision is too narrow, as it is limited to online platforms which allow "consumers to conclude distance contract with traders", i.e. marketplaces, thereby excluding infrastructure services. As a result, it fails to provide meaningful assistance in fighting illegal websites and audio-visual streaming services that contract for the use of such services. KYBC obligations should apply to providers of information society services that piracy services and other illegal operators rely on. Requiring any commercial entity to reveal its identity on the Internet would automatically reduce illegal or harmful content online. Limiting KYBC to online marketplaces is a missed opportunity to address the broad range of illegal content online.

In order to ensure that KYBC provisions can meaningfully contribute to the goal of creating a safe and predictable online environment for European citizens and legitimate European companies, the scope of application should be broadened to cover all providers of intermediary services. We therefore suggest an amendment to Article 2 to include a definition of "business customers" that would make a clear distinction between commercial operators and private customers (who would be out of scope) and put in place safeguards to ensure full compliance with existing EU acquis.

On the KYBC provision, we respectfully invite policy makers to consider moving Article 22 to Chapter III Section 1, which would broaden its scope of application to all providers of intermediary services, including providers of infrastructure services.

### 2.5 Transparency reporting obligations hosting services and providers for online platforms (Articles 13, 23-24)

**Scope.** We welcome the basic obligations of Art. 13.1 (a), (b) and (c) as they address a real need.

**Information obligations.** Transparency of online platforms requires detailed information on actions taken and on the notices received, as well as on the time for processing. Confirmations of receipt should be sent to notice providers to avoid that the latter have to check manually whether his/her request has been followed through. This can also serve as evidence in judicial or out-of-court proceedings. We welcome the provisions requiring additional *transparency measures in Articles 23 - 24* for online platforms. We note the requirement in Article 23.1(b) to provide reporting for the suspensions enacted regarding manifestly illegal content. As explained above, ACT firmly believes that there should not be any distinction between illegal content and manifestly illegal content. Prohibited content is detrimental to European values, regardless of whether it is manifestly illegal or simply illegal.

**Due diligence applied fairly**. The compliance with the due diligence obligations for a transparent and safe online environment (particularly those pursuant Articles. 13, 19, 20 and 22) should not be seen as burdensome. Enterprises willing to be active players in the digital environment, whatever their size, should make sure that their services by design limit fraud and encourage transparency. In this respect, the regime should be proportionate yet be mindful of creating dual obligation types – namely between digital and other SMEs – on due diligence requirements. All businesses should be expected to have reliable reporting, measures against misuse, KYBC and other measures in place. Otherwise, the objectives to (i) ensure that what is illegal offline should be illegal online, and; (ii) to guarantee a safer online environment for internet users and customers; would be missed.

As such we recommend that a number of clarifying amendments be made to Article 13, 16 and 23.

# SECTION III: ADDITIONAL OBLIGATIONS FOR VERY LARGE ONLINE PLATFORMS TO MANAGE SYSTEMIC RISKS FOR ILLEGAL AND HARMFUL CONTENT (CHAPTER III, SECTION 4, ART. 25-33)

### 3.1 Risk assessment (Article 26)

**Regular assessments with meaningful oversight.** We welcome the obligation for very large online platforms to conduct risk assessments specific to their services, especially with regard to illegal and harmful content. Such requirements are a step in the right direction for providing users and business users with much needed visibility with regard to content moderation systems that these platforms deploy, the systems of selecting and displaying advertising around illegal content, on one side, and harmful and intentional manipulation of their services, on the other. These assessments should be more regular.

**Thresholds to be adjusted.** We are concerned that the thresholds foreseen by the Commission to qualify risk as systemic or significantly systemic are quite high. We firmly believe that the dissemination of illegal content, infringing our members' property right which is fully protected by Article 17 of the Charter of Fundamental Rights of the EU, bringing substantial prejudice to our members' bottom line, should be considered as sufficiently prejudicial risks. For broadcasters, the routine distribution of infringing content is sufficiently prejudicial to imply a systemic risk. The terms that very large online platforms should take into account such as "rapid and wide" dissemination are of little consequence to broadcasters. If European legislators wish to provide rightsholders with a sufficiently robust toolbox, the systemic nature of the risk should be assessed in light of the prejudicial nature it has on a certain sector.

**Very large online platforms should refrain from taking any editorial decision, in the sense of removing, suspending, disabling access to or generally interfering with pre-vetted content.** Given the significant impact of such platforms on the formation of opinion in Europe and increasingly on media plurality, very large online platforms should refrain from taking any editorial decision, in the sense of removing, suspending, disabling access to or generally interfering with pre-vetted content lawfully uploaded from the account of a recognised audiovisual media provider as defined in Article 1 Paragraph 1 (a) of the AVMSD Directive (2018/1808), in order to preserve and uphold media and editorial freedom. The obligation of not interfering with curated content emanating from an audiovisual media provider should have no effect on the measures very large online platforms take to disable the dissemination of illegally uploaded content.

### 3.3. Mitigation of risks (Article 27)

ACT welcomes the mitigation of risks obligations for very large online platforms, and particularly Art. 27.1 (b) and (d). This could be a useful element in broadcasters' fight against online piracy and the necessary hook to switch from a self-regulatory to a co-regulatory model to tackle harmful content online.

**Adequate content moderation and recommender systems.** Platforms benefit directly from the spread of harmful content that they recommend and amplify (notably via their algorithms) and they should behave diligently with regards to it, as broadcasters do. Risk mitigation provision measures are an essential step in building a regulatory environment in which online platforms are responsible for the harmful content – be it legal or illegal – that they distribute and amplify through their services. Adequate content moderation and recommender systems are essential to address systemic risks foreseen in Art. 26. It would be useful to build upon this by introducing a non-exhaustive list through recitals of the different practices covered: from content

removal, amplification/de-amplification of content, artificial delays to limit virality, to the ban/suspension of accounts.

The introduction of risk mitigation measures outlined in Art. 27 is positive insofar as it will contribute to an environment where platforms have to behave responsibly. This is equally true of the possibility for the Commission and Digital Services Coordinators to issue guidelines.

**Role of regulators**. We are concerned about the proposal's over-reliance on voluntary "Codes of Conducts" and "Crisis protocols" to demonstrate platforms' mitigation measures. Regulators should have a more direct role in drawing up these mitigation measures and have the means to order platforms to make specific commitments (see also amendment to article 41 below).

While broadcasters are supportive of the measures in place to create more accountability for very large online platforms, another element should be taken into account. Broadcasters' content – both offline and online – is strictly regulated by national and European legislation.

At present very large online platforms can unilaterally demote Broadcasters' content if they deem it non-compliant with their policies. This comes at a great cost to media and editorial freedom especially given the platforms' influence on shaping opinions and perceptions. Co-legislators should ensure provisions address situations where platforms with so called absence of editorial responsibility take editorial decisions over content that is selected by editorially responsible entities.

This aspect also raises severe economic concerns in the online advertising market, as platforms may unilaterally remove content to damage broadcasters. To preserve the integrity of our services, the visibility of our content, and bolster competition in online advertising; very large online platforms' terms and conditions should not apply to lawfully uploaded pre-vetted content of editorially responsible players such as broadcasters. This should always be the case when the content emanates from its rightful owner, or from a legal source. However, such a ban on secondary control of content should not have any effect on the obligation of online intermediaries to act against illegal uploads of broadcasters content.

### 3.4. Transparency measures for very large online platforms (Articles 28 – 29)

We call for the implementation of time efficient and dynamic supervision of VLOPs' algorithms mechanisms. The lee-way afforded to platforms in Article 28.4, where operational recommendations of the independent audit are not mandatory as long as the platform can justify why it has not done so. Such a provision provides a loophole for platforms to escape responsibility and taking the prerequisite actions.

We welcome more transparency on recommender systems and their parameters (Art. 29) as a first step, but the whole VLOPs' algorithms supervision should be defined as previously explained to be really effective to fight against the dissemination of illegal and harmful content on a large scale. Supervision of VLOP's recommendation and moderation algorithms upon request of the Digital Services Coordinator to address pro illegal or harmful content biases, prevalence of compliance over trade secret to prevent the dissemination of illegal content online.

### 3.5. Additional online advertising transparency (Article 30)

We welcome the obligation for very large online platforms to compile and make publicly available advertising repositories (Article 30). This will aid regulators to assess the revenues made by very large online platforms

through the dissemination of illegal and harmful content and would provide advertisers with more visibility on the systems in place, helping the latter to ensure greater brand safety online.

The very large online platforms monetise their business through online advertising and have real market dominance due to their reach and massive data collection capabilities. More accountability and visibility is a prerequisite for a healthy online environment. We do however fear that the reporting on these figures will be done unilaterally by very large online platforms, once again without any regulatory or independent oversight.

Sponsored content and advertising are instrumental in monetising and amplifying the spread of harmful content on online platforms. Mandatory advertising transparency obligations as foreseen in Articles 24 and 30 are a positive development but they represent the bare minimum acceptable. Online platforms directly draw their revenues from online advertising and should be held responsible for it, as is the case for broadcasters. Where platforms suspend accounts or take-down content because of illegal activities, breach of terms and conditions or in compliance with codes of conducts, they should refund the advertisers and disclose this in their registries. The same applies to ads suspended by platforms.

It should also be noted that personalised advertising is a crucial and growing source of revenue for media companies. These targeted solutions can improve the effectiveness of advertising, increase its value, and enhance the viewer experience. The DSA creates the conditions for fair competition as it does not impose unnecessary restrictions and obligations on online advertising, which already has to comply with a comprehensive set of legal and self-regulatory rules, including regarding data and privacy.

### 3.6. Data access and scrutiny (Article 31)

ACT supports strong measures that would increase the accountability and transparency for very large online platforms (VLOPs), especially in light of their dual role as distributors and publishers of information. We firmly believe that shedding light on activities that have been conducted in the dark through algorithms' black boxes, will help the Digital Services Coordinators, the newly established Board and the Commission to understand the influence very large online platforms have on consumer behaviour, the way content is distributed and monetised online to maximise the profits of these players and the consequences such power holds.

Considering the major role played by VLOPs' algorithms in the acceptance, ranking and dissemination of illegal and harmful content; failing to provide a solid control and supervision mechanism on a permanent basis (given that the algorithms are constantly evolving) of algorithms related to moderation, ranking, acceleration and recommendation will make the DSA regulation miss its primary goal[7]. Transparency measures mentioned in the DSA seek to tackle the effects of the dissemination of illegal and harmful content, our proposal is focused on addressing the root causes. Algorithms are built by humans in order to capture the attention of the users on the VLOP for commercial and data collection purposes. In this way, VLOPs are encouraged to promote the most engaging content which is very often of an illegal and/or harmful nature. In practice, this means that algorithms may contain illegal or harmful content biases, voluntarily or unintentionally, which should be detected and corrected quickly by the Digital Services Coordinator.

Reciprocally, trade secrets should not be opposed by VLOPs to the Digital Services Coordinator. Obligations like explainability[8], transparency by design and active collaboration with the Digital Services Coordinator on algorithms' purposes should be included in the DSA. This kind of mechanism will be the best guarantee for EU

[7] For further reference on this, see the following study https://cdn.uclouvain.be/groups/cms-editors-crides/droit-intellectuel/CRIDES_WP_2_2021_Alain%20Strowel%20and%20Laura%20Somaini.pdf

[8] Extent to which the internal mechanics of a machine or deep learning system can be explained in human terms

citizens to be protected from illegal and harmful content. This will also ensure the respect for freedom of speech whilst ensuring this (and other fundamental rights) is not implemented at the VLOPs' sole discretion and according to its own interests. As such, if a clear editorial bias is detected, or any bias leading to the dissemination of illegal/harmful content, VLOPs should lose their liability exemption to reflect the loss of claimed neutrality. This neutrality itself can only be reasonably assessed with proper supervision of content-related algorithms.

In order to reach a proper balance between fighting against illegal and harmful content online and respecting VLOP's trade secrets, article 31 should be split in two parts. The first one addressing data access for DSCs or the Commission and the second one dealing with access to data for vetted researchers. They cannot be treated in the same way as the guarantees offered to deal with trade secrets are not alike.

DSCs should be entitled to have access to all data and algorithms requested for their investigation to ensure that VLOPs are DSA compliant. Vetted researchers should be able to conduct studies on the DSA and thus request data from the VLOPs. Yet only the DSCs (being NRAs) provide the required guarantees to handle highly sensitive data. As such, while trade secrets may be opposed to vetted researchers where warranted, the same cannot be justified for NRAs which have extensive expertise in handling trade secrets to ensure proper compliance. This is already the case for a large swathe of sectors such as telecoms, health, finance… A blanket exception granted to VLOPs on the basis of trade secrets would not be justified and would introduce a major loophole in the DSA implementation.

The transparency measures should extend to the key criteria for aggregation, selection and presentation of content, as well as functionalities of the algorithms in real time. When criteria or algorithms are modified, such changes need to be communicated immediately. Additionally, empowering the Commission to adopt standards on reporting templates is also commendable to avoid situations whereby the lack of verifiable and common key performance indicators severely undermine the monitoring and verifiability of the claims made.

### 3.7. Codes of conducts (Art.35)

We welcome the declaration of the Commission in its European Democracy Action Plan that the Digital Services Act would contain a co-regulatory backstop with regard to the Code of Practice on online disinformation. Creating a link between the Digital Services Act and the Code of Practice (CoP) on online disinformation through Art. 26, 27 and 35 is very important. Yet, the current text is too flexible to be considered a true regulatory backstop. In our view, for such a co-regulatory backstop to be effective, it is essential that (a) regulators have the power to compel a platform to participate in good faith in a co-regulatory framework; (b) that it be held against platforms when they do not participate in good faith, and; (c) that the code be binding and enforceable by regulators directly through fines. ,

Finally, the descriptions of the codes of practices in recitals 67 and 68 are not helpful as it does not reflect the co-regulatory nature that such codes are meant to have, particularly in the field of disinformation. Language describing disinformation should also be reinforced. We would support an enhanced role for the Board in the development of codes of conducts. As ERGA stressed in its assessment report on the Code of Practice on online disinformation[9]: "*existing backstop mechanisms are already functioning in other areas on a member state level and these tend to be grounded in EU and Member States legislation that provides for a state-founded, albeit often independent, authority*". The Board could fulfil such a role. As such we recommend that a number of clarifying amendments be made to Article 35.

[9] https://erga-online.eu/wp-content/uploads/2020/05/Executive-Summary-ERGA-2019-report-published-2020.pdf

## SECTION V: IMPLEMENTATION, COOPERATION, SANCTIONS AND ENFORCEMENT (CHAPTER IV, SECTIONS 1-3)

The spread of illegal and harmful content can have swift dramatic impact (as was seen recently in France for hate speech or in the U.S. for disinformation). The lengthy procedures foreseen in the proposal before the Commission can take the lead and investigate are too lengthy and should be streamlined.

As outlined above, relevant authorities should have the power to request and suggest commitments by VLOPs in relation to their compliance with articles 26 and 27 of the DSA. As such we recommend that a number of clarifying amendments be made to Article 38, 41, 43 & 45.

# ANNEX I - REFERENCES TO ECJ JURISPRUDENCE

Relevant CJEU case-law:

- "*Where, by contrast, the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 222/31*". (Case C-324/09 L'Oréal and others)
- "*if the fact remains that those operators, by making available and managing an online sharing platform such as that at issue in the main proceedings, intervene, with full knowledge of the consequences of their conduct, to provide access to protected works, by indexing on that platform torrent files which allow users of the platform to locate those works and to share them within the context of a peer-to-peer network. In this respect […] without the aforementioned operators making such a platform available and managing it, the works could not be shared by the user or, at the very least, sharing them on the internet would prove to be more complex*". (C-610/15 Stichting Brein v. Ziggo – The Pirate bay case)
- "*[...] user makes an act of communication to the public when he intervenes, in full knowledge of the consequences of his action, to give access to a protected work to his customers and does so, in particular, where, in the absence of that intervention, his customers would not, in principle be able to enjoy the broadcast work*" (Case C-527/15 Stichting Brein v. Filmspeler)
- "*it is to be determined whether those links are provided without the pursuit of financial gain by a person who did not know or could not reasonably have known the illegal nature of the publication of those works on that other website or whether, on the contrary, those links are provided for such a purpose, a situation in which that knowledge must be presumed*." (Case C-160/15 GS Media)

# ANNEX II – SUGGESTED AMENDMENTS

## Contents

# SECTION I: CONDITIONAL LIABILITY EXEMPTIONS (Chapter II, Articles 3-9)

## 1.1. Active/Passive distinction (Art. 3-5)

| Article: Recital # | Proposed Regulation, suggested deletion (~~strike through~~) and *new insertions* |
|---|---|
| **Article 2** | Article 2 (f)<br>[… ] a 'hosting' service that consists of the storage ***or the allowance of storage*** of information provided by, and at the request of, a recipient of the service; |
| **Article 5** | 1. Where an information society service is provided that consists of the storage ***or the allowance of storage*** of information provided by a recipient of the service the service provider shall not be liable for the information stored at the request of a recipient of the service on condition that the provider:<br>(a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or<br>(b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.<br>(c) abides by the due diligence obligations as stated in Chapter III<br><br>2. Paragraph 1 shall not apply where the recipient of the service is acting under the authority or the control of the provider.<br><br>3. Paragraph 1 shall not apply ~~***with respect to liability under consumer protection law of online platforms allowing consumers to conclude distance contracts with traders,***~~ where ***such an hosting services including*** online platform places ~~***the***~~ a specific item of information or otherwise enables ~~***the***~~ a specific transaction at issue in a way that would lead an average and reasonably well-informed ~~***consumer***~~ recipient of the service to believe that the information, or the product or service that is the object of the transaction, is provided either by ~~***the online platform***~~ ***the hosting service provider*** itself or by a recipient of the service who is acting under its authority or control. ***This is notably the case where online platforms present the information in a way that is not neutral as it specifically relates to the profile of one's recipient of the service in order to maximise profit and attention of the recipient of the service. Such practices are understood as online platforms organising or promoting the information, products or services in such a way that the platform decides, based on human intervention or algorithms, which and how information, products or services is accessed or found.***<br><br>***3.1 Paragraph 1 shall not apply for hosting services editorially controlled advertisement content as defined by Article 2 (n) of this Regulation.***<br><br>***3.2. Providers of intermediary services shall be deemed ineligible for the exemptions from liability referred to in Articles 3, 4 and 5 when their main purpose is to engage in or facilitate illegal activities.*** |
| **Recital 18** | The exemptions from liability established in this Regulation should not apply where, instead of confining itself to providing the services neutrally, by a merely technical**,** automatic ***and passive*** processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control |

| | |
|---|---|
| | over, that information. Those exemptions should accordingly not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of intermediary service itself, including where the information has been developed under the editorial responsibility of that provider ***or where the provider optimises or promotes the content, beyond offering basic search and indexing functionalities that are absolutely necessary to navigate the content.*** |
| **Recital 20** | A provider of intermediary services that ~~***deliberately collaborates***~~ ***engages*** with a recipient of the services in order to undertake illegal activities does not provide its service neutrally and should therefore not be able to benefit from the exemptions from liability provided for in this Regulation. |
| **Recital 23** | 23) ~~In order to ensure the effective protection of consumers when engaging in intermediated commercial transactions online, certain providers of hosting services, namely,~~***Hosting*** services~~, online platforms that allow consumers to conclude distance contracts with traders~~ should not be able to benefit from the exemption from liability ***for*** hosting service providers established in this Regulation, in so far ~~as as those online platforms~~ ***they*** present the relevant information relating to the transactions ***or exchanges*** at issue in such a way that it leads consumers to believe that the information was provided by those ~~those online platforms~~ ***services providers*** themselves or by recipients of the service acting under their authority or control, and that those ~~those online platforms~~ ***service providers*** thus have knowledge of or control over the information, even if that may in reality not be the case. In that regard, it should be determined objectively, on the basis of all relevant circumstances, whether the presentation could lead to such a belief on the side of an average and reasonably well-informed consumer |

## 1.2 Make the exemption of liability conditional on the compliance with due diligence obligations (Article 5a)

| **Article # NEW** | **Proposed Regulation, suggested deletion (~~*strike through*~~) and *new insertions*** |
|---|---|
| **Article 5a. Conditionality to the compliance with due diligence obligations NEW** | ***Providers of hosting services including online platforms shall be deemed ineligible for the liability exemptions foreseen in Article 5 of the Regulation if they do not comply with the due diligence obligations foreseen in Chapter III of this Regulation.*** |
| **Recital 18a NEW** | ***(18a) Those exemptions from liability should also not be available to providers of hosting services, including online platforms and very large online platforms that do not comply with the due diligence obligations in this Regulation. This is in line with to Recital 42 of the eCommerce Directive which implies that all active services are excluded from the limited liability regime.*** |

## 1.3 Orders to act against illegal content/ Catalogue wide injunctions (Article 8)

| Article # | Proposed Regulation, suggested deletion (~~strike through~~) and *new insertions* |
|---|---|
| **Article 8 Cross boarder** *orders to act against illegal content* | 1. Providers of intermediary services shall, upon the receipt of an order to act against ~~a specific item of~~ illegal content, issued by the relevant national judicial or administrative authorities, on the basis of the applicable Union or national law, in conformity with Union law, inform the authority issuing the order of the effect given to the orders, without undue delay, specifying the action taken and the moment when the action was taken. ***Under the condition that necessary safeguards are provided, such orders could, in particular, consist of catalogue-wide and dynamic injunctions by courts or administrative authorities requiring the termination or prevention of any infringement.***<br>2. (…)<br>2. Member States shall ensure that the orders referred to in paragraph 1 meet the following conditions:<br>(a) the orders contains the following elements:<br>– a statement of reasons explaining why the information is illegal content, by reference to the specific provision of Union or national law infringed;<br>– ~~one or more exact uniform resource locators and,~~ ***where*** necessary, additional information enabling the identification of the illegal content concerned;<br>– information about redress available to the provider of the service and to the recipient of the service who provided the content;<br>(b) the territorial scope of the order, on the basis of the applicable rules of Union and national law, including the Charter, and, where relevant, general principles of international law, does not exceed what is strictly necessary to achieve its objective;<br>(c) the order is ~~drafted in the language declared by the provider and is~~ sent to the point of contact, appointed by the provider, in accordance with Article 10. |
| **Recital 29** | (29) Depending on the legal system of each Member State and the field of law at issue, national judicial or administrative authorities may order providers of intermediary services to act against certain specific items of illegal content or to provide certain specific items of information ***on a cross-border basis***. The national laws on the basis of which such orders are issued differ considerably and the orders are increasingly addressed ***in cross-border situations***. In order to ensure that those cross-border orders can be complied with in an effective and efficient manner, so that the public authorities concerned can carry out their tasks and the providers are not subject to any disproportionate burdens, without unduly affecting the rights and legitimate interests of any third parties, it is necessary to set certain conditions that those orders should meet and certain complementary requirements relating to the processing of those orders. |
| **Recital 30** | (30) Orders to act against illegal content or to provide information should be issued in compliance with Union law, in particular Regulation (EU) 2016/679 and the prohibition ~~of general obligations to monitor information or to actively seek facts or circumstances indicating illegal activity laid down in this Regulation~~ ***on Member States to impose a monitoring obligation of a general nature.*** The conditions and requirements laid down in this Regulation which apply ***to cross-border*** orders to act against illegal content are without prejudice to other Union acts providing for similar systems for acting against specific types of illegal content, such as Regulation (EU) …/…. [proposed Regulation addressing the dissemination of terrorist content online], or |

| | |
|---|---|
| | Regulation (EU) 2017/2394 that confers specific powers to order the provision of information on Member State consumer law enforcement authorities, whilst the conditions and requirements that apply to orders to provide information are without prejudice to other Union acts providing for similar relevant rules for specific sectors. Those conditions and requirements should be without prejudice to retention and preservation rules under applicable national law, in conformity with Union law and confidentiality requests by law enforcement authorities related to the non-disclosure of information. |

## 1.4 Orders to provide information (Article 9)

| Article/ Recital# | Proposed Regulation, suggested deletion (~~strike through~~) and *new insertions* |
|---|---|
| **Article 9** | 1. Providers of intermediary services shall, upon receipt of an order to ***provide*** ~~***a specific item of***~~ information about one or more specific individual recipients of the service, issued by the relevant national judicial or administrative authorities on the basis of the applicable Union or national law, in conformity with Union law, inform without undue delay the authority of issuing the order of its receipt and the effect given to the order.<br><br>2. Member States shall ensure that orders referred to in paragraph 1 meet the following conditions:<br>(a) the order contains the following elements:<br>– a statement of reasons explaining the objective for which the information is required and why the requirement to provide the information is necessary and proportionate to determine compliance by the recipients of the intermediary services with applicable Union or national rules, unless such a statement cannot be provided for reasons related to the prevention, investigation, detection and prosecution of criminal offences;<br>– information about redress available to the provider and to the recipients of the service concerned;<br>(b) the order only requires the provider to provide information ***enabling the identification of recipients of the service*** ~~***already collected for the purposes of providing the service***~~ and which lies within its control;<br>(c) the order ~~***is drafted in the language declared by the provider and***~~ is sent to the point of contact appointed by that provider, in accordance with Article 10;<br>[…] |
| **Recital 31** | (31) The territorial scope of such ***cross-border*** orders to act against illegal content should be clearly set out on the basis of the applicable Union or national law enabling the issuance of the order and should not exceed what is strictly necessary to achieve its objectives. In that regard, the national judicial or administrative authority issuing the order should balance the objective that the order seeks to achieve, in accordance with the legal basis enabling its issuance, with the rights and legitimate interests of all third parties that may be affected by the order, in particular their fundamental rights under the Charter. In addition, ***because*** the order referring to the specific information may have effects beyond the territory of the Member State of the authority concerned, the authority should assess whether the information at issue is likely to constitute illegal content in other Member States concerned and, where relevant, take account of the relevant rules of Union law or international law and the interests of international comity. |

| | |
|---|---|
| **Recital 32** | (32) The orders to provide information ***on a cross-border basis*** regulated by this Regulation concern the production of specific information about individual recipients of the intermediary service concerned who are identified in those orders for the purposes of determining compliance by the recipients of the services with applicable Union or national rules. ***This information should include the relevant email addresses, telephone numbers, IP addresses and other contact details necessary to ensure such compliance.*** Therefore, orders about information on a group of recipients of the service who are not specifically identified, including orders to provide aggregate information required for statistical purposes or evidence-based policy-making, should remain unaffected by the rules of this Regulation on the provision of information. |
| **Recital 33** | 33) Orders to act against illegal content and to provide information ***on a cross-border basis*** are subject to the rules safeguarding the competence of the Member State where the service provider addressed is established and laying down possible derogations from that competence in certain cases, set out in Article 3 of Directive 2000/31/EC, only if the conditions of that Article are met. Given that the orders in question relate to specific items of illegal content and information, respectively, where they are addressed to providers of intermediary services established in another Member State, they do not in principle restrict those providers' freedom to provide their services across borders. Therefore, the rules set out in Article 3 of Directive 2000/31/EC, including those regarding the need to justify measures derogating from the competence of the Member State where the service provider is established on certain specified grounds and regarding the notification of such measures, do not apply in respect of those orders. |

## 1.5 Content moderation (Article 12)

| **Article/ Recital #** | **Proposed Regulation, suggested deletion (~~*strike through*~~) and *new insertions*** |
|---|---|
| **Article 12**<br><br>**Terms and conditions** | 1. Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review. It shall be set out in clear and unambiguous language and shall be publicly available in an easily accessible format.<br><br>***1a. Very large online platforms as defined by Article 25 of the Regulation shall ensure that their terms and conditions as well as other policies, procedures, measures and tools used for the purpose of content moderation are applied and enforced by taking into account the provisions of Article 26 Paragraph 2 and Recital 38***.<br><br>2. Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the applicable fundamental rights of the recipients of the service as enshrined in the Charter. |
| **Recital 38** | (38) Whilst the freedom of contract of providers of intermediary services should in principle be respected, it is appropriate to set certain rules on the content, application |

| | |
|---|---|
| | and enforcement of the terms and conditions of those providers in the interests of transparency, the protection of recipients of the service and the avoidance of unfair or arbitrary outcomes. ***To this end, terms and conditions of Very Large Online Platforms shall not have lawfully uploaded content owned, and editorially selected by an audiovisual media provider as defined in Article 1 Paragraph 1 (a) in the AVMS Directive (2018/1808) unduly obscured, obfuscated or otherwise disabled by virtue of its alleged non-adherence to terms and conditions that go beyond the thresholds applied to legal and harmful requirements applicable in relevant European and national regulations and jurisdictions.*** |

# SECTION II: DUE DILLIGENCE OBLIGATIONS FOR A TRANSPARENT & SAFE ONLINE ENVIRONMENT (Chapter III)

## 2.1 Notice and Action Procedures

| Article/ Recital # | Proposed Regulation, suggested deletion (~~*strike through*~~) and *new insertions* |
|---|---|
| **Article 14** | 2. The mechanisms referred to in paragraph 1 shall be such as to facilitate the submission of sufficiently precise and adequately substantiated notices, on the basis of which a diligent economic operator can identify the illegality of the content in question. To that end, the providers shall take the necessary measures to enable and facilitate the submission of notices containing ~~all~~ of the following elements:<br><br>(b***) ~~a clear indication of the electronic location of that information, in particular the exact URL or URLs,*~~** where necessary, additional information enabling the identification of the illegal content;<br>[…]<br>3. Notices that include the elements referred to in paragraph 2 shall be considered to give rise to actual knowledge or awareness for the purposes of Article 5 in respect of the specific item of information concerned ***and shall create an obligation on behalf of the notified provider of hosting services to remove or disable access to the notified information expeditiously***<br>6. Providers of hosting services shall process any notices that they receive under the mechanisms referred to in paragraph 1, and take their decisions in respect of the information to which the notices relate, in a timely, diligent and objective manner. ***When a decision has been taken to remove or disable information, the providers of hosting services shall take all necessary measures to prevent the same or equivalent illegal material from reappearing on their service***. Where they use automated means for that processing or decision-making, they shall include information on such use in the notification referred to in paragraph 4. |
| **Recital 40** | 40) Providers of hosting services play a particularly important role in tackling illegal content online, as they store information provided by and at the request of the recipients of the service and typically give other recipients access thereto, sometimes on a large scale. It is important that all providers of hosting services, regardless of their size, put in place user-friendly notice and action mechanisms that facilitate the notification of specific items of information that the notifying party considers to be illegal content to the provider of hosting services concerned ('notice'), pursuant to which that provider can decide whether or not it agrees with that |

| | |
|---|---|
| | assessment and wishes to remove or disable access to that content ('action'). Provided the requirements on notices are met, it should be possible for individuals or entities to notify multiple specific items of allegedly illegal content through a single notice ***in order to ensure effective of operation of notice and action mechanisms***. The obligation to put in place notice and action mechanisms should apply, for instance, to file storage and sharing services, web hosting services, advertising servers and paste bins, in as far as they qualify as providers of hosting services covered by this Regulation. |
| **Recital 42** | Where a hosting service provider decides to remove or disable information provided by a recipient of the service, for instance following receipt of a notice or acting on its own initiative, including through the use of automated means, that provider ***should prevent the reappearance of the notified or equivalent illegal information***. The provider should also inform the recipient of its decision, the reasons for its decision and the available redress possibilities to contest the decision, in view of the negative consequences that such decisions may have for the recipient, including as regards the exercise of its fundamental right to freedom of expression. That obligation should apply irrespective of the reasons for the decision, in particular whether the action has been taken because the information notified is considered to be illegal content or incompatible with the applicable terms and conditions. Available recourses to challenge the decision of the hosting service provider should always include judicial redress. |

## 2.2 Trusted flaggers (Article 19)

| **Article/ Recital#** | **Proposed Regulation, suggested deletion (~~*strike through*~~) and *new insertions*** |
|---|---|
| **Article 15 bis** | (~~***b) it represents collective interests,***~~ or it has a significant legitimate interest, ***either collectively or as individual entity,*** is independent from any online platform, ***and has a proven expertise of flagging illegal content with a high rate of accuracy***; […] |
| | 5. Where ~~***an online platform***~~ ***hosting service*** has information indicating that a trusted flagger submitted a significant number of ~~***insufficiently precise or inadequately substantiated***~~ ***wrongful*** notices through the mechanisms referred to in Article 14, including information gathered in connection to the processing of complaints through the internal complaint-handling systems referred to in Article 17(3), it shall communicate that information to the Digital Services Coordinator that awarded the status of trusted flagger to the entity concerned, providing the necessary explanations and supporting documents. |
| **Recital 46** | (46) Action against illegal content can be taken more quickly and reliably where online platforms take the necessary measures to ensure that notices submitted by trusted flaggers through the notice and action mechanisms required by this Regulation are treated with priority, without prejudice to the requirement to process and decide upon all notices submitted under those mechanisms in a timely, diligent, objective and effective manner. Such trusted flagger status should be awarded to entities, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content, ***have significant legitimate interests, have a proven record in flagging content with a high rate of accuracy and particular expertise and have demonstrated competence for the purposes of detecting, identifying and notifying illegal content.*** Such entities can also be public in nature, such as, for terrorist content, |

| | |
|---|---|
| | internet referral units of national law enforcement authorities or of the European Union Agency for Law Enforcement Cooperation ('Europol') or they can be non-governmental organisations and semi-public bodies, such as the organisations part of the INHOPE network of hotlines for reporting child sexual abuse material and organisations committed to notifying illegal racist and xenophobic expressions online. For intellectual property rights, organisations of industry and of right-holders could be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions. The rules of this Regulation on trusted flaggers should not be understood to prevent online platforms from giving similar treatment to notices submitted by entities or individuals that have not been awarded trusted flagger status under this Regulation, from otherwise cooperating with other entities, in accordance with the applicable law, including this Regulation and Regulation (EU) 2016/794 of the European Parliament and of the Council. |

## 2.3 Repeat infringer policy (Article 20)

| **Article/ Recital #** | **Proposed Regulation, suggested deletion (~~strike through~~) and *new insertions*** |
|---|---|
| **Article 20** *Measures and protection against misuse* | 1. Providers of hosting services shall suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide ***or facilitate the dissemination of*** ~~***manifestly***~~ illegal content. ***In cases of repeat suspension, providers of hosting services shall terminate the provision of their services and introduce mechanisms that prevent the re-registration of recipients of service that frequently provide or facilitate the dissemination of illegal content.***<br><br>2. Providers of hosting services shall ***terminate,*** ~~***suspend, for a reasonable period of time and***~~ after having issued a prior warning, the processing of notices and complaints submitted through the notice and action mechanisms and internal complaints-handling systems referred to in Articles 14 and 17, respectively, by individuals or entities or by complainants that frequently submit notices or complaints that are manifestly unfounded.<br><br>(a) the absolute numbers of items of ~~***manifestly***~~ illegal content or ~~***manifestly***~~ unfounded notices or complaints, submitted in the past year; |
| **Recital 47** | The misuse of services of online platforms by frequently providing or ***facilitating the dissemination of illegal content*** or by frequently submitting manifestly unfounded notices or complaints under the mechanisms and systems, respectively, established under this Regulation undermines trust and harms the rights and legitimate interests of the parties concerned.<br>[…] |

## 2.4 Know Your Business Customer (Article 22)

| **Article #** | **Proposed Regulation, suggested deletion (~~strike through~~) and *new insertions*** |
|---|---|
| **Article 2 ea (NEW)** | ***ea) 'business customer' means:***<br>***legal entities, except any entity which qualifies as a large undertaking as defined in Article 3(4) of Directive 2013/34 of the European Parliament and the Council;*** |

| | |
|---|---|
| | ***any natural person that:***<br><br>***purchases a type or amount of service indicative of, or otherwise indicates, the intent to operate a business online; or***<br>***contracts for the purchase of more than €10.000 of services provided by the intermediary service provider in a one-year period; or*** |
| **Article 12a Traceability of business customers NEW** | ***Article 12a***<br>***Traceability of business customers***<br><br>***1. A provider of intermediary services shall ensure that business customers can only use its services to promote messages on or to offer products or services to consumers located in the Union if, prior to the use of its services, the provider of intermediary services has obtained the following information:***<br><br>***(a) the name, address, telephone number and electronic mail address of the business customer;***<br><br>***(b) a copy of the identification document of the business customer or any other electronic identification as defined by Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council;***<br><br>***(c) the bank account details of the business customer~~,~~ where the business customer is a natural person;***<br><br>***(d) the name, address, telephone number and electronic mail address of the economic operator, within the meaning of Article 3(13) and Article 4 of Regulation (EU) 2019/1020 of the European Parliament and the Council or any relevant act of Union law;***<br><br>***(e) where the business customer is registered in a corporate or trade register or similar public register, the register in which the business customer is registered and its registration number or equivalent means of identification in that register;***<br><br>***(f) a self-certification by the business customer committing to only offer products or services that comply with the applicable rules of Union law.***<br><br>***2. The provider of intermediary services shall, upon receiving that information, make reasonable efforts to assess whether the information referred to in points (a), (d) and (e) of paragraph 1 is reliable through the use of any publicly accessible official online database or online interface made available by a Member States or the Union or through requests to the business customer to provide supporting documents from reliable and independent sources.***<br><br>***2a. The provider of intermediary services shall also verify that any person purporting to act on behalf of the business customer is so authorised and identify and verify the identity of that person.***<br><br>***3. Where the provider of intermediary services obtains indications, including through a notification by law enforcement agencies or other individuals with a legitimate interest, that any item of information referred to in paragraph 1 obtained from the business customer concerned is inaccurate, misleading, ~~or~~ incomplete, or otherwise invalid, that provider of an intermediary service shall request the business customer to correct the*** |

| | |
|---|---|
| | ***information in so far as necessary to ensure that all information is accurate and complete, without delay or within the time period set by Union and national law.***<br><br>***Where the business customer fails to correct or complete that information, the provider of intermediary services shall suspend the provision of its service to the business customer until the request is complied with.***<br><br>***4. The provider of intermediary services shall store the information obtained pursuant to paragraph 1 and 2 in a secure manner for a period of five years following the termination of their contractual relationship with the business customer concerned. They shall subsequently delete the information.***<br><br>***4a. Providers of intermediary services shall apply the identification and verification measures not only to new business customers but they shall also update the information they hold on existing business customers on a risk-sensitive basis, and at least once a year, or when the relevant circumstances of a business customer change.***<br><br>***5. Without prejudice to paragraph 2, the provider of intermediary services shall disclose the information to third parties where so required in accordance with the applicable law, including the orders referred to in Article 9 and any orders issued by Member States' competent authorities or the Commission for the performance of their tasks under this Regulation, as well as pursuant to proceedings initiated under other relevant provisions of Union or national law.***<br><br>***6. The provider of intermediary provider of intermediary services shall make the information referred to in points (a), (d), (e) and (f) of paragraph 1 available to the recipients of the service, in a clear, easily accessible and comprehensible manner.***<br><br>***7. The provider of intermediary services shall design and organise its online interface in a way that enables business customers to comply with their obligations regarding pre-contractual information and product safety information under applicable Union law.***<br><br>***7a. The Digital Services Coordinator of establishment shall determine dissuasive financial penalties for non-compliance with any provision of this Article.*** |
| **Recital 48 (a) NEW** | **(48a)** ***Online transparency requirements for commercial entities are vital for ensuring accountability, trust and access to effective redress. To this end, Article 5 of Directive 2000/31/EC establishes general information requirements for service providers to render to service recipients and competent authorities. In addition, Article 6 of Regulation (EU) 2016/67 allows for the processing and disclosure of all information on domain name holders from the WHOIS database for the performance of tasks carried out in the public interest, and a number of Member States require their national country code top-level domain registries to make such information publicly accessible. However, the lack of effective enforcement of Article 5 and the often outdated and inaccurate information contained within the WHOIS database emphasize the need to put in place a clear obligation for providers of intermediary services to verify the identity of their business customers. The Know Your Business Customer provision should also prohibit providers of intermediary services from providing their services to unverified customers and oblige them to cease the provision of their services when the identification provided proves to be incomplete, inaccurate or fraudulent;*** |
| **Recital 49** | 49) In order to contribute to a safe, trustworthy and transparent online environment for consumers ***and other users***, as well as for other interested parties such as competing traders |

| | |
|---|---|
| | and holders of intellectual property rights, and to deter ***the selling and dissemination of products and services in violation of the applicable rules all providers of intermediary services, including hosting providers, domain name registrars, providers of content delivery networks, proxy and reverse proxy providers, online marketplaces, online payment service providers and online advertising service providers*** should ensure that ***their business customers*** are traceable. The ***business customer*** should therefore be required to provide certain essential information to the online platform, including for purposes of promoting messages on or offering products. That requirement should also be applicable to ***business customers*** that promote messages on products or services on behalf of brands, based on underlying agreements. ***Providers of intermediary services*** should store all information in a secure manner for a reasonable period of time that does not exceed what is necessary, so that it can be accessed ***and verified***, in accordance with the applicable law, including on the protection of personal data, by ***the providers of intermediary*** services***,*** public authorities and private parties with a legitimate interest, including through the orders to provide information referred to in this Regulation. |
| **Recital 50** | (50) To ensure an efficient and adequate application of that obligation, without imposing any disproportionate burdens, the ***providers of intermediary services*** should make reasonable efforts to verify the reliability of the information provided by ***their business customers***, in particular by using freely available official online databases and online interfaces, such as national trade registers and the VAT Information Exchange System, or by requesting ***their business customers*** to provide trustworthy supporting documents, such as copies of identity documents, certified bank statements, company certificates and trade register certificates. They may also use other sources, available for use at a distance, which offer a similar degree of reliability for the purpose of complying with this obligation. However, the ***providers of intermediary*** should not be required to engage in excessive or costly online fact-finding exercises or to carry out verifications on the spot.<br><br>Nor should such ***providers of intermediary*** services, which have made the reasonable efforts required by this Regulation, be understood as guaranteeing the reliability ***and accuracy*** of the information towards consumer or other interested parties. Such **providers of intermediary services** should ***update the information they hold on a risk-sensitive basis, and at least once a year and*** also design and organise their online interface in a way that enables ***their business customers*** to comply with their obligations under Union law, in particular the requirements set out in Articles 6 and 8 of Directive 2011/83/EU of the European Parliament and of the Council, Article 7 of Directive 2005/29/EC of the European Parliament and of the Council and Article 3 of Directive 98/6/EC of the European Parliament and of the Council. |

## 2.5 Transparency reporting obligations for providers for online platforms & online advertising (Articles 13, 23-24)

| **Article #** | **Proposed Regulation, suggested deletion (~~*strike through*~~) and *new insertions*** |
|---|---|
| **Article 16** *Exclusion for micro and small enterprises* | ~~***This Section shall not apply to online platforms that qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC.***~~ |

| | |
|---|---|
| **Article 23** *Transparency reporting obligations for providers of online platforms* | 1.In addition to the information referred to in Article 13, online platforms shall include in the reports referred to in that Article information on the following:<br>[…]<br>(b) the number of suspensions imposed pursuant to Article 20, distinguishing between suspensions enacted for the provision of ~~***manifestly***~~ illegal content, the submission of manifestly unfounded notices and the submission of manifestly unfounded complaints; |

# SECTION III: ADDITIONAL OBLIGATIONS FOR VERY LARGE ONLINE PLATFORMS TO MANAGE SYSTEMIC RISKS FOR ILLEGAL AND HARMFUL CONTENT

## 3.1. Risk assessment (Article 26)

| **Article #** | Proposed Regulation, suggested deletion (~~***strike through***~~) and ***new insertions*** |
|---|---|
| **Article 26** *Risk assessment* | (a) the dissemination ***and amplification*** of illegal content through their services;<br><br>(b) any negative effects for the exercise of the fundamental rights to respect for ***human dignity,*** private and family life, freedom of expression and information, ***right to property,*** the prohibition of discrimination and the rights of the child, as enshrined in Articles ***1***, 7, 11, ***17***, 21 and 24 of the Charter respectively;<br><br>~~***(c) intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable***~~ ***any negative effects*** ~~***on on aspects such as***~~ ***to*** the protection of public health, minors, civic discourse, or ~~***actual or foreseeable***~~ effects related to electoral processes and public security.<br><br>2. When conducting risk assessments, very large online platforms shall take into account, in particular, how their content moderation systems, recommender systems and systems for selecting and displaying advertisement influence any of the ~~***systemic***~~ risks referred to in paragraph 1, including the potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions.<br><br>***Very large online platforms shall ensure that their terms and conditions as well as other policies, procedures, measures and tools used for the purpose of content moderation are applied and enforced in such a way as to prohibit any removal, suspension, disabling access to or otherwise interference with content and services from the account of a recognised audiovisual media service provider as defined in Article 1 Paragraph 1 (a) of the AVMSD Directive (2018/1808)***. |

## 3.2. Mitigation of risks (Article 27)

| Article/ Recital # | Proposed Regulation, suggested deletion (~~strike through~~) and *new insertions* |
|---|---|
| **Article 27** *Mitigation of risks* | 1.Very large online platforms shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific ~~systemic~~ risks identified pursuant to Article 26. Such measures may include, where applicable:<br>(…..)<br>(d) initiating or adjusting cooperation with trusted flaggers in accordance with Article *15 bis*~~19~~;<br>2. The Board, in cooperation with the Commission, *shall oversee compliance with the measures foreseen in Paragraph 1 and* shall publish comprehensive reports, once a year, which shall include the following:<br>(a) identification and assessment of the most prominent and recurrent ~~systemic~~ risks reported by very large online platforms or identified through other information sources, in particular those provided in compliance with Article 31 and 33;<br>(b) best practices for very large online platforms to mitigate the ~~systemic~~ risks identified.<br>3. The Commission, in cooperation with the Digital Services Coordinators, ~~may~~ *shall* issue ~~general~~ guidelines on the application of paragraph 1 in relation to specific risks, in particular to present best practices and ~~recommend possible~~ *request specific* measures, having due regard to the possible consequences of the measures on fundamental rights enshrined in the Charter of all parties involved. When preparing those guidelines the Commission shall organise public consultations. |
| **Recital 56** | […] Under this Regulation, very large online platforms should therefore assess the ~~systemic~~ risks stemming from the functioning and use of their service, as well as by potential misuses by the recipients of the service, and take appropriate mitigating measures. |
| **Recital 57** | Three categories of ~~systemic~~ risks should be assessed in-depth. A first category concerns the risks associated with the misuse of their service through the dissemination of illegal content, such as the dissemination of child sexual abuse material ~~or~~ illegal hate speech, and the conduct of illegal activities, such as the sale of products, *copyright protected content and* services prohibited by Union or national law, including counterfeit products. For example, and without prejudice to the personal responsibility of the recipient of the service of very large online platforms for possible illegality of his or her activity under the applicable law, such dissemination or activities may constitute a significant ~~systematic~~ risk where access to such content may be amplified through accounts with a particularly wide reach. A second category concerns the impact of the service on the exercise of fundamental rights, as protected by the Charter of Fundamental Rights, including the freedom of expression and information, the right to private life, *the right to property*, the right to non-discrimination and the rights of the child. Such risks may arise, for example, in relation to the design of the algorithmic systems used by the very large online platform or the misuse of their service ~~through the submission of abusive notices or other methods for silencing speech or hampering competition~~. A third category of risks *concerns artificial and endemic amplification*~~, the intentional and, often~~ *some*times *due to* coordinated manipulation of the platform's service, *and virality on online platforms which* ~~with~~ can have a*n* ~~foreseeable~~ impact on health, civic discourse, electoral processes, public security and protection of minors, having regard to the need to safeguard public order, protect privacy and fight fraudulent and deceptive commercial practices. Such risks may arise, for example, through the creation of fake accounts, the use of bots, and other automated or partially automated behaviours *and the use of proxy services on a large scale* which may lead |

| | |
|---|---|
| | to the rapid and widespread dissemination of information that is illegal ~~***content***~~***, harmful*** ~~***content***~~ or ***otherwise*** incompatible with an online platform's terms and conditions. ***Additionally, given their significant impact on the formation of opinion in Europe and increasingly on media plurality, very large online platforms should refrain from taking any editorial decision, in the sense of removing, suspending, disabling access to or generally interfering with pre-vetted content lawfully uploaded from the account of a recognised audiovisual media provider as defined in Article 1 Paragraph 1 (a) of the AVMSD Directive (2018/1808), in order to preserve and uphold media and editorial freedom. The obligation of not interfering with curated content emanating from an audiovisual media provider should have no effect on the measures very large online platforms take to disable the dissemination of illegally uploaded content.*** |
| **Recital 58** | Very large online platforms should deploy the necessary means to diligently mitigate the ~~***systemic***~~ risks identified in the risk assessment. Very large online platforms ***shall*** ~~***should***~~ under such mitigating measures ~~***consider, for example***~~, ***enhance***~~***ing***~~ or otherwise adapt~~ing~~ the design and functioning of their content moderation, algorithmic recommender systems and online interfaces, so that they ~~***discourage and***~~ limit the dissemination of illegal content***, for instance by building in systems to amplify or demote content identified as harmful, introducing artificial delays to limit virality***, adapting their decision-making processes, or adapting their terms and conditions.They may also include corrective measures, ***such as discontinuing advertising revenue for specific content and retroactively refunding advertisers where their advertisements appear next to***, or other actions, such as improving the visibility of authoritative information sources***, such as content under a media provider's editorial control and subject to specific standards, media regulation and independent oversight.*** Very large online platforms may reinforce their internal processes or supervision of any of their activities, in particular as regards the detection of systemic risks. They ~~***may***~~ ***shall*** initiate or increase cooperation with trusted flaggers, organise training sessions and exchanges with trusted flagger organisations, and cooperate with other service providers, including by initiating or joining existing codes of conduct or other self-regulatory measures. Any measures adopted should respect the due diligence requirements of this Regulation and be effective and appropriate for mitigating the specific risks identified, in the interest of safeguarding public order, protecting privacy and fighting fraudulent and deceptive commercial practices, and should be proportionate in light of the very large online platform's economic capacity and the need to avoid unnecessary restrictions on the use of their service, taking due account of potential negative effects on the fundamental rights of the recipients of the services. |

## 3.3. Transparency measures for VLOPs (Articles 28-29)

| Article # | Proposed Regulation, suggested deletion (~~***strike through***~~) and ***new insertions*** |
|---|---|
| **Article 28** *Independent audit* | 1. Very large online platforms shall be subject, at their own expense and at least ~~***once***~~ ***twice*** a year, to audits to assess compliance with the following:<br>[…]<br>4. Very large online platforms receiving an audit report that is not positive shall take due account of any operational recommendations addressed to them with a view to take the necessary measures to implement them. They shall, ~~***within one month from receiving those recommendations***~~, ***without delay*** adopt an audit implementation report setting out those measures. |

## 3.4. Additional online advertising transparency (Article 30)

| Article | Proposed Regulation, suggested deletion (~~***strike through***~~) and ***new insertions*** |
|---|---|
| **Article 30** – Additional advertising tran-sparency | 1. Very large online platforms that display advertising on their online interfaces shall compile and make publicly available through application programming interfaces a repository containing the information referred to in paragraph 2, until one year after the advertisement was displayed for the last time on their online interfaces. They shall ensure that the repository does not contain any personal data of the recipients of the service to whom the advertisement was or could have been displayed.<br><br>2. The repository shall include at least all of the following information:<br>(a) the content of the advertisement;<br>(b) the natural or legal person on whose behalf the advertisement is displayed;<br>(c) the period during which the advertisement was displayed;<br>(d) whether the advertisement was intended to be displayed specifically to one or more particular groups of recipients of the service and if so, the main parameters used for that purpose;<br>(e) the total number of recipients of the service reached and, where applicable, aggregate numbers for the group or groups of recipients to whom the advertisement was targeted specifically.<br>***(f) when the advertising appeared next to content that was removed because it was illegal, infringed the platforms terms and conditions, or in order to comply with a code of conduct foreseen in Article 35 of this Regulation, or for advertising that appeared on accounts terminated or suspended for uploading illegal content according to Article 20 of the Regulation or content infringing platforms' terms and conditions and in complying with codes of conduct. This shall be the case for the number of recipients of the service such advertising reached, the funds transferred to those that uploaded the content and the amounts refunded to the advertisers.***<br><br>***3) All information about advertising that was removed because it contained illegal content, content that infringed the platforms' terms and conditions or in order to comply with a code of conduct foreseen by article 35, shall also be included in the repository foreseen in paragraph 1.*** |

## 3.5. Data access and scrutiny (Article 31)

| Article/ Recital # | Proposed Regulation, suggested deletion (~~***strike through***~~) and ***new insertions*** |
|---|---|
| **Article 31** ***Data access and scrutiny for the Digital Services Coordinator or the Commission*** | 1. Very large online platforms shall provide the Digital Services Coordinator of establishment or the Commission, upon their reasoned request and ~~***within a reasonable period***~~ ***without undue delay***, ~~***specified in the request,***~~ ***full*** access to data that are necessary to monitor and assess compliance with this Regulation. That Digital Services Coordinator and the Commission shall only use that data for those purposes.<br><br>***With regard to moderation and recommender systems, very large online platforms shall provide the Digital Services Coordinator or the Commission a real-time access to algorithms and associated data that allow the detection of possible biases which could lead to the dissemination of illegal content or threats to fundamental rights including freedom of expression. When disclosing these data, very large online platforms shall have a duty of explainability and ensure close cooperation with the Digital Services Coordinator or the Commission to make moderation and recommender systems fully understandable. When a bias is detected, very large online platforms should correct it expeditiously following requirements from the Digital Services Coordinator or the Commission.***<br><br>***As a duty to care obligation, very large online platforms should be able to demonstrate their compliance at every step of the process pursuant to this Article.***<br><br>~~***2. Upon a reasoned request from the Digital Services Coordinator of establishment or the Commission, very large online platforms shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers who meet the requirements in paragraphs 4 of this Article, for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks as set out in Article 26(1).***~~<br><br>3. Very large online platforms shall provide access to data pursuant to paragraph~~s~~ 1 ~~and 2~~ through online databases or application programming interfaces, as appropriate.<br><br>~~***4. In order to be vetted, researchers shall be affiliated with academic institutions, be independent from commercial interests, have proven records of expertise in the fields related to the risks investigated or related research methodologies, and shall commit and be in a capacity to preserve the specific data security and confidentiality requirements corresponding to each request.***~~<br><br>5. The Commission shall, after consulting the Board, adopt delegated acts laying down the technical conditions under which very large online platforms are to share data pursuant to paragraph~~s~~ 1 ~~***and 2***~~ and the purposes for which the data may be used. Those delegated acts shall lay down the specific conditions under which such sharing of data with ~~***vetted researchers***~~ ***the Digital Services Coordinator or the Commission*** can take place in compliance with Regulation (EU) 2016/679, taking into account the rights and interests of the very large online platforms and the recipients of the service concerned, including the protection of confidential information, in particular trade secrets, and maintaining the security of their service.<br><br>~~***6. Within 15 days following receipt of a request as referred to in paragraph 1 and 2, a very large online platform may request the Digital Services Coordinator of establishment or***~~ |

| | |
|---|---|
| | ~~*the Commission, as applicable, to amend the request, where it considers that it is unable to give access to the data requested because one of following two reasons:*~~<br><br>~~*(a) it does not have access to the data;*~~<br><br>~~*(b) giving access to the data will lead to significant vulnerabilities for the security of its service or the protection of confidential information, in particular trade secrets.*~~<br><br>~~*7. Requests for amendment pursuant to point (b) of paragraph 6 shall contain proposals for one or more alternative means through which access may be provided to the requested data or other data which are appropriate and sufficient for the purpose of the request.*~~<br><br>~~*The Digital Services Coordinator of establishment or the Commission shall decide upon the request for amendment within 15 days and communicate to the very large online platform its decision and, where relevant, the amended request and the new time period to comply with the request.*~~ |
| ***Article 31a (new)*** *Data access and scrutiny* ***for vetted researchers*** | ***1. Upon request from the Digital Services Coordinator of establishment or the Commission, very large online platforms shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers who meet the requirements in paragraphs 4 of this Article, for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks as set out in Article 26(1).***<br><br>***2. Very large online platforms shall provide access to data pursuant to paragraph~~s~~ 1 ~~and 2~~ through online databases or application programming interfaces, as appropriate.***<br><br>***3. In order to be vetted, researchers shall be affiliated with academic institutions, be independent from commercial interests, have proven records of expertise in the fields related to the risks investigated or related research methodologies, and shall commit and be in a capacity to preserve the specific data security and confidentiality requirements corresponding to each request.***<br><br>***4. The Commission shall, after consulting the Board, adopt delegated acts laying down the technical conditions under which very large online platforms are to share data pursuant to paragraph~~s~~ 1 ~~and 2~~ and the purposes for which the data may be used. Those delegated acts shall lay down the specific conditions under which such sharing of data with vetted researchers can take place in compliance with Regulation (EU) 2016/679, taking into account the rights and interests of the very large online platforms and the recipients of the service concerned, including the protection of confidential information, in particular trade secrets, and maintaining the security of their service.***<br><br>***5. Within 15 days following receipt of a request as referred to in paragraph 1 ~~and 2~~, a very large online platform may request the Digital Services Coordinator of establishment or the Commission, as applicable, to amend the request, where it considers that it is unable to give access to the data requested by vetted researchers because one of following two reasons:***<br><br>***(a) it does not have access to the data;***<br><br>***(b) giving access to the data will lead to significant vulnerabilities for the security of its service or the protection of confidential information, in particular trade secrets.***<br><br>***6. Requests for amendment pursuant to point (b) of paragraph 5 shall contain proposals for one or more alternative means through which access may be provided to the*** |

| | |
|---|---|
| | ***requested data or other data which are appropriate and sufficient for the purpose of the request.***<br><br>***The Digital Services Coordinator of establishment or the Commission shall decide upon the request for amendment within 15 days and communicate to the very large online platform its decision and, where relevant, the amended request and the new time period to comply with the request.*** |
| **Recital 64** | In order to appropriately supervise the compliance of very large online platforms with the obligations laid down by this Regulation, the Digital Services Coordinator of establishment or the Commission may require access to or reporting of specific data. Such a requirement may include, for example, the data necessary to assess the risks and possible harms brought about by the platform's systems, data on the accuracy, functioning and testing of algorithmic systems for content moderation, recommender systems or advertising systems, ***corresponding underlying source codes,*** or data on processes and outputs of content moderation or of internal complaint-handling systems within the meaning of this Regulation. ~~***Investigations by researchers on the evolution and severity of online systemic risks are particularly important for bridging information asymmetries and establishing a resilient system of risk mitigation, informing online platforms, Digital Services Coordinators, other competent authorities, the Commission and the public.***~~ This Regulation therefore provides ***on one hand*** a framework for compelling access to data from very large online platforms ***to the Digital Services Coordinator or the Commission, and on the other hand, a framework for compelling access to data from very large online platforms*** to vetted researchers. All requirements for access to data under ~~***that***~~ ***those*** framework***s*** should be proportionate and appropriately protect the rights and legitimate interests, including trade secrets and other confidential information, of the platform and any other parties concerned, including the recipients of the service. |
| **Recital 64a (new)** | ***Moderation and recommendation algorithms used by very large online platforms pose high risks and require closer and further regulatory supervision, because of the presence of algorithmic biases which often lead to a massive dissemination of illegal content or threats to fundamental rights including freedom of expression. Taking into account the permanent evolution of these algorithms and the immediate risks they could generate when deployed, very large online platforms should ensure full and real-time disclosure of moderation and recommendation algorithms to the Digital Services Coordinator or the Commission.***<br><br>***This disclosure should include all the data regarding the creation and the settings of these algorithms, such as corresponding datasets. To facilitate the supervision of the Digital Services Coordinator or the Commission, this Regulation provides a framework of obligations for very large online platforms, including explainability of algorithms, accountability and close cooperation with the Digital Services Coordinator or the Commission. Should an algorithmic bias be detected, very large online platforms should correct it expeditiously, following requirements from the Digital Services Coordinator or the Commission.*** |

## 3.6. Codes of conducts (Article 35)

| Article/ Recital # | Proposed Regulation, suggested deletion (~~strike through~~) and new insertions |
|---|---|
| **Article 35** *Codes of conduct* | 1. The Commission and the Board shall ~~encourage and facilitate~~ request and coordinate the drawing up of codes of conduct at Union level to contribute to the proper application of this Regulation, taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks, in accordance with Union law, in particular on competition and the protection of personal data.<br><br>2. Where ~~significant systemic~~ risks within the meaning of Article 26(1) emerge and concern several very large online platforms, the Commission ~~may~~ shall invite the very large online platforms concerned, other very large online platforms, other online platforms and other providers of intermediary services, as appropriate, as well as civil society organisations and other interested parties, to participate in the drawing up of codes of conduct, including by setting out commitments to take specific risk mitigation measures, as well as a regular reporting framework on any measures taken and their outcomes. |
| | 3. When giving effect to paragraphs 1 and 2, the Commission and the Board shall aim to ensure that the codes of conduct clearly set out their objectives, contain verifiable key performance indicators to measure the achievement of those objectives, have an independent monitoring and audit systems in place and take due account of the needs and interests of all interested parties, including citizens, at Union level. The Commission and the Board shall also aim to ensure that participants report regularly and in good faith to the Commission and their respective Digital Service Coordinators of establishment on any measures taken and their outcomes, as measured against the key performance indicators that they contain. |
| | 4. The Commission and the Board shall assess whether the codes of conduct meet the aims specified in paragraphs 1 and 3, and shall regularly monitor and evaluate the achievement of their objectives. They shall publish their conclusions and request that the organisations involved amend the codes of conducts accordingly.<br><br>5. The Board shall regularly monitor and evaluate the achievement of the objectives of the codes of conduct, having regard to the key performance indicators that they ~~may~~ contain. |
| **Recital 67** | (67)The Commission and the Board should be empowered to request and coordinate ~~encourage~~ the drawing-up of codes of conduct to contribute to the application of this Regulation. ~~While~~ The implementation of codes of conduct should be measurable and subject to public oversight~~, this should not impair the voluntary nature of such codes and the freedom of interested parties to decide whether to participate~~. In certain circumstances, it is important that very large online platforms cooperate in the drawing-up and adhere to specific codes of conduct. Nothing in this Regulation prevents other service providers from adhering to the same standards of due diligence, adopting best practices and benefitting from the guidance provided by the Commission and the Board, by participating in the same codes of conduct. |

| | |
|---|---|
| **Recital 68** | It is appropriate that this Regulation identify certain areas of consideration for such codes of conduct. In particular, risk mitigation measures concerning specific types of illegal content should be explored via self- and co-regulatory agreements. Another area for consideration is the possible negative impacts of systemic risks on society and democracy, such as ***misinformation,*** disinformation or manipulative and abusive activities. This includes the ***spread and amplification of misinformation and disinformation, sometimes through coordinated operations aimed at amplifying*** information, ~~***including disinformation, such as for instance through***~~ the use of bots, ~~***or***~~ fake accounts ***and proxy services*** for the creation **and spread** of fake or misleading information, sometimes with a purpose of obtaining economic gain, which are particularly harmful for vulnerable recipients of the service, such as children. In relation to such areas, adherence to and compliance with a given code of conduct by a very large online platform may be considered as a~~***n***~~ necessary ~~***appropriate***~~ risk mitigating measure. The refusal ~~***without proper explanations***~~ by an online platform of the Commission's invitation to participate in the application of such a code of conduct ~~***could***~~ **must** be taken into account~~***, where relevant,***~~ when determining whether the online platform has infringed the obligations laid down by this Regulation. ***When codes of conducts are used as a risk mitigating measure, they shall be made binding by the Digital Services Coordinator of the platform.*** |

## SECTION IV: IMPLEMENTATION, COOPERATION, SANCTIONS AND ENFORCEMENT (CHAPTER IV)

| **Article/ Recital #** | **Proposed Regulation, suggested deletion (~~*strike through*~~) and *new insertions*** |
|---|---|
| **Article 43** *Right to lodge a complaint* | Recipients of the service ***and parties with a legitimate interest*** shall have the right to lodge a complaint against providers of intermediary services alleging an infringement of this Regulation with the Digital Services Coordinator of the Member State where the recipient resides or is established. The Digital Services Coordinator shall assess the complaint and, where appropriate, trans mit it to the Digital Services Coordinator of establishment. Where the complaint falls under the responsibility of another competent authority in its Member State, the Digital Service Coordinator receiving the complaint shall transmit it to that authority |
| **Recital 81** | (81) In order to ensure effective enforcement of this Regulation, individuals or representative organisations and ***parties with a legitimate interest*** should be able to lodge any complaint related to compliance with this Regulation with the Digital Services Coordinator in the territory where they received the service, without prejudice to this Regulation's rules on jurisdiction. Complaints should provide a faithful overview of concerns related to a particular intermediary service provider's compliance and could also inform the Digital Services Coordinator of any more cross-cutting issues. The Digital Services Coordinator should involve other national competent authorities as well as the Digital Services Coordinator of another Member State, and in particular the one of the Member State where the provider of intermediary services concerned is established, if the issue requires cross-border cooperation. |

| | |
|---|---|
| **Article 50** *Enhanced supervision for very large online platforms* | 1. The Commission acting on its own initiative, or the Board acting on its own initiative or upon request of at least ~~***three***~~ ***two*** Digital Services Coordinators of destination, may, where it has reasons to suspect that a very large online platform infringed any of those provisions, recommend the Digital Services Coordinator of establishment to investigate the suspected infringement with a view to that Digital Services Coordinator adopting such a decision ***without delay*** ~~***within a reasonable time period***~~.<br><br>2. When communicating the decision referred to in the first subparagraph of paragraph 1 to the very large online platform concerned, the Digital Services Coordinator of establishment shall request it to draw up and communicate to the Digital Services Coordinator of establishment, the Commission and the Board, within one month from that decision, an action plan, specifying how that platform intends to terminate or remedy the infringement. The measures set out in the action plan ~~***may***~~ ***shall*** include, where appropriate, participation in a code of conduct as provided for in Article 35.<br><br>***3.*** Within one month following receipt of the action plan, the Board shall communicate its opinion on the action plan to the Digital Services Coordinator of establishment. Within ***10 days*** ~~***one month***~~ following receipt of that opinion, that Digital Services Coordinator shall decide whether the action plan is appropriate to terminate or remedy the infringement.<br><br>Where the Digital Services Coordinator of establishment has concerns on the ability of the measures to terminate or remedy the infringement, it ***shall*** ~~***may***~~ request the very large online platform concerned to subject itself to an additional, independent audit to assess the effectiveness of those measures in terminating or remedying the infringement. In that case, that platform shall send the audit report to that Digital Services Coordinator, the Commission and the Board within ~~***four***~~ ***one*** month~~s~~ from the decision referred to in the first subparagraph. When requesting such an additional audit, the Digital Services Coordinator may specify a particular audit organisation that is to carry out the audit, at the expense of the platform concerned, selected on the basis of criteria set out in Article 28(2). |