DIGITALEUROPE

26 JANUARY 2022

Ironing out new rules for online platforms: What to watch out for during the Digital Services Act trilogues

Executive summary

The proposed Digital Services Act (DSA)[1] maintains the core elements of the eCommerce Directive,[2] which have been critical to growing the internet, whilst introducing new due diligence requirements that can address the real problem of illegal content and products online. As trilogues begin, preserving this delicate balance will be key to protecting fundamental rights and innovation.[3]

As a horizontal framework covering all online intermediaries and types of content, the DSA will not be able to solve all challenges related to the internet. Some concerns, such as child sexual abuse, will be better addressed via additional targeted (voluntary or regulatory) measures.[4] Similarly, overlapping requirements should be avoided wherever there are relevant rules either already in place or in the process of being written.

In particular, the final text should:

- Uphold the principle of limited liability which has been crucial to the growth of the digital economy.

[1] COM(2020) 842 final.

[2] Directive 2000/31/EC.

[3] This paper complements our position on the original Commission proposal, available at https://www.digitaleurope.org/wp/wp-content/uploads/2021/03/FINAL-DSA-Paper-March-2021-1.pdf and our suggested amendments, available at: https://www.digitaleurope.org/wp/wp-content/uploads/2022/01/DIGITALEUROPE-DSA-Amendments-June-2021-FINAL.pdf

[4] See our *Position paper on the EU strategy for combating child sexual abuse and exploitation*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2021/03/DIGITALEUROPE-Position-paper-CSAM-proposal-04-March-2021-003.pdf

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- Create more effective trusted flagger mechanisms which allow ‘trusted corporates’ to be designated as trusted flaggers by platforms.
- Introduce effective know-your-business-customer obligations that hamper bad actors but do not present barriers to legitimate traders by requiring them to submit burdensome information to open an account.
- Add additional safeguards for user redress systems to create effective procedures to appeal content decisions, requiring users first to exhaust internal appeals mechanisms.
- Refrain from including a media ‘must-carry’ obligation, which would create a dangerous backdoor for disinformation. Publishers, or those who pose as publishers, may misuse their channels under the guise of free speech.
- Consider a proportionate approach for dealing with low-risk services captured by the very large online platform obligations, such as a procedure that allows low-risk platforms that exceed the user threshold to appeal the status.

Table of contents

User redress

Out-of-court dispute settlement

It is important for users to be able to appeal content decisions, and many platforms already offer mechanisms to this end. However, any out-of-court settlement (OoC) mechanism under the DSA – especially as its scope has been further expanded by the co-legislators – should avoid abuse from bad actors, in line with other pieces of legislation.

Notably, bad actors could use alternative dispute resolution to arbitrate every content removal at a company's expense. They could slow down the process for legitimate seekers of redress. In addition, under the current text, content uploaders may arguably also challenge services' removals made under national authorities' removal orders (under Art. 8), including where those orders may be confidential and appear as the online platforms' own decision.

The current OoC provisions overlap with existing laws, notably the Audiovisual Media Services Directive,[5] the Platform-to-Business Regulation[6] and the Copyright Directive. This overlap creates legal uncertainty for platforms and confusion for users, likely resulting in contradictory decisions by different bodies in different Member States over the same issues or policies.

To improve the proposal, we suggest clarifying the scope, so that the OoC mechanism would only apply to termination of consumer accounts or service provision to consumers, and thus exclude decisions made on spam grounds. We also suggest introducing the following safeguards:

- Requiring users to first exhaust internal appeals mechanisms;
- Ensuring that users submit an OoC request only once for the same issue, and setting a clear time limit within which users may request that disputes be submitted to the OoC mechanism;
- Ensuring that service providers and users bear a reasonable proportion of the total cost of using the OoC mechanism; and
- Adding penalties for bad-faith actors.

Decisions reached through use of OoC mechanisms should not be legally binding. Judicial recourse against them should always remain possible, for both service providers and users.

[5] Directive (EU) 2018/1808.

[6] Regulation (EU) 2019/1150.

Restrictions of visibility

Some stakeholders have suggested expanding transparency and user redress requirements beyond content removals to also cover 'any restrictions' to the visibility of content, including choices made as to what content to recommend to users under the Council text.

While well intentioned, these provisions could lead to unnecessarily high numbers of user notifications, and would jeopardise intermediaries' ability to operate systems in a way that benefits users.

We urge that 'restrictions of visibility' should be removed from the list of actions for which notification and user redress are widely available. At the very least, the final text should more precisely define what restrictions may trigger user redress, in line with the principles of proportionality and legal certainty.

Marketplace-specific provisions

We welcome that the co-legislators have confirmed the conditional liability regime for online platforms, including for online marketplaces. Any deviations from this keystone principle for marketplaces would have undermined the provision of these services in Europe.

Basic verification of traders on marketplaces is an important tool for platforms to prevent misuse of their services, disincentivise bad actors online and provide a safe and trusted environment for customers.

However, the Parliament has significantly expanded the KYBC obligations for marketplaces. The list of data points that operators need to verify is overly extensive and raises the question of what 'best efforts' means in practice.

We encourage a workable KYBC mechanism. In particular, verifying traders' self-declarations regarding product types and compliance with EU law is not possible for marketplaces, as they often do not have physical control of the products.

Specific proposals for product safety online are better addressed under the proposed General Product Safety Regulation (GPSR), which is best placed to designate roles along the supply chain.[7]

[7] See *DIGITALEUROPE comments on the proposed General Product Safety Regulation*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2022/01/DIGITALEUROPE-comments-on-the-proposed-General-Product-Safety-Regulation.pdf.

Trusted flaggers

Introducing a trusted flaggers regime will bring advantages for both online platforms and third parties, including rightsholders.

We welcome the Parliament's proposed clarification that trusted flaggers should only act within their designated area of expertise. For example, a trusted flagger working on disinformation will have no expertise in trademark violations and should not be able to flag in this area.

However, further improvements would be needed to make the trusted flaggers mechanism more effective for all stakeholders involved. Online platforms should be allowed to designate individual rightsholders as trusted flaggers, which is unfortunately not envisaged in the Parliament's position.

While the Digital Services Coordinator (DSC) is in charge of appointing general trusted flaggers, platform operators should be able to appoint additional trusted flaggers, including individual rightsholders with regard to the service they provide. In case of disputes in the platform's trusted flagger appointment or withdrawal process, the DSC could act as an appeals body for the trusted flagger. In general, platforms should be free to choose their own trusted flaggers and determine the specific privileges based on objective, transparent criteria. For example, trusted corporate entities (brand owners) should be able to qualify as trusted flaggers directly. A trusted corporate may be determined by, for example, the number of notice-and-takedown requests that it files with a platform during a defined period versus the number of unfounded or incorrect notice-and-takedown requests. The DSA should encourage cooperation between brand owners and online platforms as this often allows for faster removal of infringing listings and less administrative burden for all involved.[8]

While the Council acknowledges the role of private entities and removes the mention of 'collective interests' from Art. 19(2)(b), Recital 46 emphasises the role of industry associations over individual rightsholders. Limiting the trusted flaggers status to organisations raises practical and implementation issues. For example, a trade association is not ordinarily authorised to confirm whether a trademark infringement has taken place on behalf of one of its members. Additionally, multiple rightsholders within a trusted flagger organisation could have a different tolerance as to what constitutes an IPR infringement. This may expose individual rightsholders represented by the broader organisation to the risk of losing trusted flagger status because of the actions of others represented by the same organisation. Further, the recital recognises existing collaboration schemes between platforms and rightsholders, but it does not clarify the formal processes

[8] See our suggested amendment, available at: https://www.digitaleurope.org/wp/wp-content/uploads/2022/01/DIGITALEUROPE-DSA-Amendments-June-2021-FINAL.pdf

in case of disputes in the platform's appointment or withdrawal of the trusted flagger status.

Notice and action

The European Parliament has clarified the notice-and-action framework to facilitate the review process and expeditious action on illegal content and goods. In particular, we welcome the clarification that content should remain accessible pending assessment, given the far-reaching consequences a removal can have from an economic and fundamental rights perspective.

During the legislative process, some stakeholders have raised the reappearances of illegal content, goods or services. In general, reappearances are the result of continued attempts at abuse. Eliminating all abuses all the time is as tricky online as offline, and there are many factors outside a platform's control.[9] In particular when it comes to goods, working with customs authorities and stepping up enforcement is key to minimising the entry of illegal goods into the EU.

Cloud computing services

The proposal recognises that certain provisions only apply to specific types of intermediary services, given the wide variety of services and the different roles of the relevant service provider captured. Clear definitions to ensure the right services are covered are crucial.

In this context, we welcome the Parliament's proposal in Recital 13 to clarify that cloud computing services should not be considered as an online platform when dissemination to the public constitutes a minor or ancillary feature. Many cloud services are business-to-business services where the cloud service provider is in direct relation with its own business customer, which is, in turn, in relation with the end-user/customer who may, in certain cases, provide illegal content online. Since the cloud service provider has no direct link or relationship with the end-user/customer, it is not able, technically or even contractually, to act to remove, edit or curate user-generated illegal content.

We also welcome the Parliament's proposal to allow a service provider to forward the notice where the provider has no technical, operational or contractual ability to act against specific items of illegal content.

[9] For example, millions of genuine identities have been stolen through cybercrime and are available to register new accounts. Similar content can also occur for many reasons that are not always apparent to humans, or may not be recognisably identical to a machine.

Notification of suspicions of criminal offences

Art. 15(a) widens an obligation to proactively notify law enforcement from online platforms to all hosting service providers, in conflict with the ban on general monitoring.

This expansion is highly problematic when applied to hosting service providers, e.g. IT infrastructure, which do not always have visibility of and access to user content to make the judgments set out in this article.

Art. 15(a) relies on several vague concepts, such as 'information giving rise to a suspicion.' The vagueness of these concepts constitutes a low threshold above which disclosure must be provided, effectively resulting in a content monitoring obligation. We urge policymakers to align the scope and language of this provision with that of similar requirements included in the Terrorist Content Online Regulation.[10]

Voluntary measures

The co-legislators have made limited changes to the Commission's proposal on voluntary own-initiative investigations.

Among these, we support the Council's clarification in Recital 25 that 'voluntary actions should not be used to circumvent the obligations of all providers of intermediary services under this Regulation.'

Accessibility requirements

DIGITALEUROPE encourages careful consideration of the Parliament's proposal to create new accessibility obligations for online platforms. The European Accessibility Act (EAA) already includes a sweeping list of products and services, determined after careful consideration with stakeholders to determine the appropriate scope.[11]

Rather than extending accessibility obligations to all online platforms via the DSA, the European Parliament should leverage existing EAA mechanisms to

[10] Regulation (EU) 2021/784.

[11] Directive (EU) 2019/882.

determine whether to amend the EAA and expand its scope to expressly include online platforms.[12]

At the very least, should accessibility provisions remain in the DSA, the implementation deadline should be aligned to the EAA. The EAA is technically complex and will be implemented via yet to be adopted standards for all services and products covered. Member States have until June 2022 to bring their national measures in line with the EAA and enforce the new requirements as of 2025.

New compensation for non-compliance

A newly introduced liability for direct damages resulting from non-compliance with the DSA is far-reaching, and its practical impact has not been properly assessed.

The relationship of Art. 43a with the limited liability regime is unclear. Beyond this, intermediaries would face double jeopardy as they would not only be subject to maximum fines of 6 per cent of turnover for non-compliance with the DSA but also, as a consequence of this article, face individual court actions.

The legal uncertainty of this provision, e.g. what would still be considered direct damage, in combination with vague regulatory requirements such as the 'reasonable effort' obligations in the KYBC article, results in significant legal risks for operators – even beyond online platforms as the article addresses all intermediaries.

VLOPs criteria/exceptions for low-risk services

Chapter IV on very large online platforms (VLOPs) differentiates from the rest of the proposal solely based on the number of users. The Parliament's position adds further obligations for VLOPs, seeking to address specific high-risk situations and services.

This raises the question as to whether a purely quantitative threshold is appropriate and proportionate. The systemic risk of a service is not reflected by its size only, but by the type of service and the nature of the content hosted. A very large travel booking website will not bring about additional systemic risks just because it surpasses a given user number threshold. In fact, larger services may exhibit fewer risks than smaller ones.

The final text should provide for additional risk factors to be fulfilled for any VLOP designation. Alternatively, a transparent and accountable procedure should be

[12] Art. 33 EAA.

envisaged allowing platforms that exceed the VLOP user threshold to appeal to the status by laying out why, despite their reach, the assumed risks concerning the dissemination of illegal content are not present.[13]

Media must-carry obligations

Several stakeholders have proposed media exemptions (so-called must-carry obligations). Under these proposals, online platforms would not be allowed to take actions against content violating their terms and conditions, including harmful or even illegal content, in case such content was posted by a 'publisher' or 'editorial content providers.'

While media freedom and independence are paramount, a broad exemption will lead to cases where publishers in some jurisdictions may use their channels to push misinformation. Another challenge, which became apparent during implementation of the Copyright Directive,[14] is that most Member States have no official definition of what qualifies as a media organisation.

To protect free speech, exceptions should instead apply to *content*, not to a list of creators. Many online platforms are taking voluntary actions as a part of their commitments under the EU Code of Practice on Disinformation – something they couldn't do if media exemptions were part of the DSA.[15]

Targeted advertising, recommender systems and dark patterns

Several stakeholders have proposed banning or severely restricting the use of targeted advertising.

Nearly all online services provided free of charge rely on revenue generated through advertisement, and a ban on targeted advertising would force most providers to either direct more (potentially irrelevant) ads at users or charge them for the use of their services. This risks reducing the variety of online services and hampering business development across the value chain – online platforms, media outlets, content creators, and smaller providers of products and services, who would have a more challenging task reaching potential customers.

[13] See our suggested amendment, available at: https://www.digitaleurope.org/wp/wp-content/uploads/2022/01/DIGITALEUROPE-DSA-Amendments-June-2021-FINAL.pdf

[14] Directive (EU) 2019/790.

[15] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

It is important to consider that both the ePrivacy Directive[16] and the General Data Protection Regulation (GDPR)[17] set clear rules regarding transparency and consent, which are key to consumer protection in the advertising market. We therefore urge against the introduction of new provisions in the DSA.

Similarly, requirements regarding recommendations received by users should focus on clarity, transparency, explainability and user control principles, as in the Commission's initial approach. Profiling is already covered under the GDPR, and requiring user opt-in in all circumstances will unnecessarily implicate the balance of legal bases provided under data protection law.

Finally, the Parliament's introduction of a 'dark patterns' provision appears to ignore the protection already afforded under the Unfair Commercial Practices Directive[18] and the GDPR. This has been made clear by the recent Commission guidance to the Omnibus Directive.[19]

The new provision overlaps with several existing legal requirements, and it is unclear what additional concerns the Parliament seeks to address. It must also be considered that, should genuinely new concerns be identified, as with the proposed new restrictions on targeted advertising, the 'dark patterns' provision would only apply to the entities covered by the DSA, thus leaving consumers unprotected elsewhere depending on the service they use.

FOR MORE INFORMATION, PLEASE CONTACT:

Hugh Kirk

Senior Manager for Digital Commerce Policy

hugh.kirk@digitaleurope.org / +32 490 11 69 46

Alberto Di Felice

Director for Infrastructure, Privacy and Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

[16] Directive 2002/58/EC as amended by Directive 2009/136/EC.

[17] Regulation (EU) 2016/679.

[18] Directive 2005/29/EC as amended by Directive (EU) 2019/2161.

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021XC1229%2805%29&qid=1640961745514.

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK