DIGITALEUROPE

31 March 2021

Digital Services Act position paper

Executive Summary

The Digital Services Act (DSA) proposal marks an important update to internet regulation in Europe. DIGITALEUROPE's membership supports the European Commission's ambition to strengthen the Single Market for digital services in the EU. Clarity is needed on the role and responsibilities of online intermediaries to address the problem of illegal content online and help boost trust in the internet.

Internet regulation is a balancing act between protecting fundamental rights like freedom of speech on the one hand, and preventing illegal and harmful activities online on the other. In this paper, DIGITALEUROPE builds upon its previous publications[1][2] and proposes some constructive suggestions to the EU institutions to help improve the proposed DSA.

- We welcome that the proposal preserves the eCommerce Directive's core tenets, which have allowed Europe to develop and enjoy a vibrant internet economy. Maintaining principles such as limited liability, no general monitoring, and the country-of-origin is key to the continued innovation and growth of these digital services in Europe and will be crucial to a rapid economic recovery.
- We agree that the DSA needs to clearly distinguish between the liability and responsibility of online players of all sizes and risk profiles. The law should uphold the foundations of the tried and tested eCommerce regime where liability should be based on actual knowledge and failure to act. Liability should not result from illegal content of which the platform is not aware.
- We welcome that the DSA recognises that harmful (but legal) content requires a different set of provisions than illegal content. Harmful content

[1] DIGITALEUROPE (May 2020) Towards a more responsible and innovative internet

[2] DIGITALEUROPE (Sept 2020) DSA consultation response

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

is contextual, difficult to define, may be culturally subjective and is often legally ambiguous.

- DIGITALEUROPE strongly believes that important definitions, such as what constitutes a very large online platform, should not be left to delegated acts. All relevant stakeholders should be given the opportunity to contribute to developing definitions and methodologies which can significantly impact the implementation of the law.
- We believe the DSA due diligence requirements such as trusted flaggers, trader traceability, and transparency mechanisms, if developed in a proportionate and workable way, will provide opportunities to enhance collaboration among all stakeholders leading to a safer online environment.
- We welcome the formalisation of rules on notice and action mechanisms across online intermediaries. This formalisation will facilitate the review process and expeditious action on illegal content and goods.
- We support providing stakeholders with meaningful transparency about content moderation and enforcement practices. However, it will be important that transparency measures in the DSA ensure that users' privacy is protected, bad actors cannot game the system and that commercially sensitive information is not disclosed.
- DIGITALEUROPE has concerns about the feasibility of the implementation timeline. We would recommend a 12 to 18 month period to leave sufficient time to build and implement new processes

We look forward to working with all stakeholders to create a framework that improves trust in digital services, unlocks innovation and reduces the prevalence of illegal and harmful content online.

Table of Contents

Liability regime

DIGITALEUROPE welcomes the strong endorsement in the DSA of the core principles from the eCommerce Directive. This includes specifically the country-of-origin principle and the limited liability regime for online intermediaries, based on the notice-and-takedown system. We agree that the DSA needs to clearly distinguish between the liability and responsibility of online players of all sizes and risk profiles. The law should uphold the foundations of the tried and tested eCommerce regime where liability should be based on actual knowledge and failure to act. Liability should not result from illegal content of which the platform is not aware.

Voluntary measures clause

Article 6

Although online intermediaries cannot be compelled by a Member State to conduct general monitoring of content or activities, this does not imply that service providers cannot initiate such activities on their own. Some DIGITALEUROPE members perform certain voluntary monitoring activities at the moment in order to enforce their terms of service or to better protect their users. Those online intermediaries who carry out such voluntary monitoring are concerned that it carries a risk of depriving them of their intermediary liability protection. For example, the eCommerce Directive does not contain a provision which ensures that, where an online intermediary has voluntarily reviewed content or activities for a certain type of specific illegality unlawfulness (or for a specific violation of its terms of service), the service provider is not deemed to have knowledge of any other ways in which the reviewed content or activities might be unlawful. We welcome that the European Commission has recognised this challenge, however, we believe that a more clearly defined provision as to scope and inherent constraints would be welcome.

No general monitoring

Article 7

DIGITALEUROPE welcomes that the prohibition of general monitoring obligations is maintained in the DSA. Member States may not impose a general obligation to systematically monitor information that intermediary service providers transmit or store. Any obligation to introduce general monitoring could pose significant risks for freedom of expression and fundamental rights. A general monitoring obligation would also have a negative effect on competition and the market entrance of new actors.

Harmful content

We welcome that the DSA recognises that harmful (but legal) content requires a different set of provisions than illegal content. Any regulation should recognise the need to balance the removal of harmful content with the protection of freedom of expression and other fundamental rights. Harmful content is contextual, difficult to define, may be culturally subjective and is often legally ambiguous. Harmful content should, therefore, not form part of the liability regime. At the same time, it is desirable for society that online intermediaries have the capacity to moderate and enforce against lawful but potentially harmful content according to their clear policies. Not all content is suitable for all platforms and the communities they serve.

We welcome the important role that the European Commission assigns to co-regulation, risk assessments and mitigation measures. However, these provisions in relation to harmful content are very broad and can encompass many content areas and affect freedom of expression. We are concerned that these provisions, if not appropriately scoped, may serve as backdoors to ad hoc regulation of lawful content instead of lawful content being regulated through democratic processes. Given the large fines for non-compliance, there needs to be more clarity about what exactly triggers sanctions. Regulation should recognise that intermediaries face challenges when seeking to remove harmful but not illegal content pursuant to their policies.

Scope

Asymmetric approach

The DSA addresses a broad range of service providers from different sectors and different types of content. We broadly welcome the idea of a horizontal regulatory approach covering all online intermediaries and preserving the fundamental principles of the eCommerce Directive for all these services.

While we understand that reach or size can play an important role, in general, we recommend a consistent, reasonable and workable set of rules for all market players. While we acknowledge that not all services have the same level of

resources, but to be truly effective, the legislation should strive at preventing illegal content from migrating from mainstream sites to less moderated platforms and social networks in the shadows. This is not a theoretical risk, and indeed migration of content is a worrisome trend that analysts have observed with terrorist content, violent extremism, and child sexual abuse imagery.

Definitions

Article 2

DIGITALEUROPE strongly believes that important definitions should not be left to delegated acts. It is fundamental that these aspects are addressed within the DSA. All relevant stakeholders should be given the opportunity to contribute to developing definitions and methodologies which can significantly impact the implementation and protection of the rule of law. This is particularly the case for how monthly active users of an online platform are to be calculated.

Clarity on which services belong in which category is also essential. We do not think clearer definitions will be an obstacle to a horizontal and future proof DSA. Rather, they will allow for smoother and more effective implementation. In the context of the DSA discussion, we think it remains important to consider the different degrees of authority and control that providers either can or should exert over content they host on behalf of customers and users.

Illegal content

DIGITALEUROPE supports the principle that what is illegal offline should remain illegal online.

We note that, whereas the Commission has explicitly stated that the DSA does not purport to define what illegal content is (which remains a matter for applicable national and EU law), it does include an illegal content definition. There is a need to clarify that definition by removing the "reference to an [illegal] activity" as illegal content already includes illegal activity.

Online platforms

DIGITALEUROPE welcomes the approach in the proposal which recognises that certain provisions in the DSA (for example, the due diligence obligations) should only apply to specific types of intermediary services. This approach is consistent with the notion that a "one-size-fits-all" structure will not work when applied to digital services, since the nature of the different types of services involved and the role of the relevant service provider varies greatly. However, the definition of an "online platform" as currently proposed is overly broad. It would have the unintended consequence of subjecting, for instance, providers of IT infrastructure

services (i.e. cloud infrastructure services) to obligations that are not appropriate for these types of services. Providers of IT infrastructure services do not have direct visibility or control over how customers use their services, including whether a customer chooses to make its content available to the public and what content is displayed. The obligations in the DSA which are tailored for online platforms (for example, traceability of traders' requirements, advertising transparency requirements) are therefore not appropriate for providers of services deeper in the internet stack, such as IT infrastructure services (on-premise, cloud-based and or hybrid). Likewise, cloud-based hosting solutions that store user-generated content and offer their users basic sharing features (such as links to their files) should not be considered online platforms because their main feature is not the dissemination of content to the public, and because the information they store cannot be made available to the public directly within their ecosystem. The legislation should clarify that the aforementioned services are not considered online platforms under the DSA.

When it comes to the responsibilities of intermediaries deeper in the internet stack, DIGITALEUROPE underlines that any obligation to remove or disable access to illegal content should be first on the customer or end-user who has made available online the content. Services deeper in the internet stack acting as online intermediaries should be required to take proportionate actions where the customer fails to remove the illegal content, unless technically impracticable (e.g. they own the hosting service; or it would not result in indiscriminate or disproportionate removal of legitimate customer content). This should also be reflected in the due diligence requirements for hosting services.

Due diligence obligations

Legal representatives

Article 11

The proposal requires intermediary services established outside of the EU to appoint a legal representative within the Union liable for non-compliance with the obligations of the DSA.

Designating a legal representative could, for some smaller platforms, be a significant burden for non-EU based services. DIGITALEUROPE is concerned about how Europe's trading partners will react and potentially retaliate to such a requirement. DIGITALEUROPE wants to avoid a situation where EU-based services are required to appoint a legal representative to provide services in non-EU territories. The most tangible example to reflect on is to consider all of the services accessed from Europe currently located in the UK and vice versa.

Notice and action mechanisms

Article 14

DIGITALEUROPE welcomes the EU-level formalisation of rules on notice and action mechanisms across online intermediaries and the proposed elements that notices must contain to be actionable. This formalisation will facilitate the review process and expeditious action on illegal content and goods. The tools for such notices should be, wherever possible, made available exclusively electronically.

Regarding the content of notices, all responsible platforms should have efficient and accessible processes. At the same time, there should be some flexibility to implement these requirements in a way that best reflects the nature of their services, the type of content they make available, and their risk exposure.

DIGITALEUROPE notes that in the requirement to provide "a statement confirming the good faith belief of the individual or entities submitting the notice that the information and allegations contained therein are accurate and complete" in Art.14 (2)(d), the reference to "good faith belief" risks being unclear and open to interpretation. This provision's application and effect would be clearer if it explicitly linked the accuracy and completeness of the statement "to the best knowledge" of the individual or entities submitting the notice.

The current wording of Art.14(3) suggests that a platform will be deemed to have actual knowledge of an illegality once the elements mentioned in Art.14(2) are fulfilled. Depending on the nature of the intermediary and of the illegal content, it can be difficult for the intermediary to determine whether content is illegal. This needs to be taken into account and a balance struck between ensuring clearly illegal content is dealt with responsibly and swiftly whilst platforms continue to receive the benefits of the hosting defence (Art. 5) in respect to content which is not so easy to assess for illegality.

In addition, we suggest the European Commission and the Board, as provided for by Article 35, facilitate developing a code of conduct for online platforms on informing customers who purchased confirmed counterfeit products from third party traders. Some e-commerce platforms already send these notifications, which increase awareness and thereby contribute to the fight against counterfeits.

Internal complaint-handling system

Article 17

Complaint handling systems for decisions taken by online platforms can provide an adept tool to ensure a fair process of weighing the various interests involved in an online environment. Many such systems already exist in various shapes

and forms today. This reflects the fact that the nature of the decisions taken, their impact and the types of content differ significantly from platform to platform. A general requirement for such systems will be very burdensome for a large proportion of online platforms and conflicts with the proportionality principle. The DSA, in its current form, applies this requirement also to ancillary functions and content of online platforms such as, e.g. comments sections, customer reviews or even just a "like" of a piece of content. This appears excessive and also goes beyond the reasonable expectations of recipients of decisions in such cases. It will impose significant costs on platforms for even low-risk scenarios. The de-facto prohibition of automated decisions exacerbates this problem and raises serious concerns as to the provision's practical implementation given the scale of content moderation it covers. Human decisions will require more time but more importantly, they can be just as error-prone as automated decisions and may be even more subjective and biased. Platforms should be given a reasonable degree of discretion on how to best handle complaints reflecting the specific context and challenges of their services.

Out-of-court dispute settlement

Article 18

Alternative dispute resolution mechanisms can offer a fast and more cost-effective resolution for parties that agree contractually to be bound by the outcome, but the option proposed by the DSA amounts to a binding resolution and not a settlement and the nomenclature should be amended.

Such systems can have the advantage of allowing amicable resolutions of conflicts given participants can engage voluntarily. It is, however, unclear why the DSA proposal opts for this system while giving up its key advantage over court procedures: the non-binding, open nature of proceedings. This would mean that rather than a dialogue between complainant and platform, the dispute settlement will turn into a legal process with the level of formality and resource intensity of normal court procedures, which begs the question of what the added value of such as system would be. The DSA also fails to clarify who is liable for the implementation of settlement decisions if they are subsequently overturned by a regular court.

The DSA should, as in the Platform-to-Business Regulation, require the platform operator to designate one or more independent dispute settlement bodies (DSBs), rather than leaving the complainant free choice. Realistically, a DSB will not be able to provide its service for all types of platforms but will specialise, e.g. in e-commerce marketplace matters, social media business questions or rental/booking platform. At the very least, a platform should be able to challenge the choice of a particular DSB. The experience from the recently adopted

Platform-to-Business Regulation has shown, it is questionable whether an economically viable setup of dispute settlement bodies (DSB) is even possible.

The DSA should address potential abuse of the dispute resolution system. It should be clarified that complainants first need to exhaust internal complaints mechanisms (as these are legally mandated by the DSA) before costly DSB processes are triggered. Furthermore, platform operators should be able to decline dispute resolution where, for example, there are clearly no merits to a claim, where there are abusive repeat requests or where it is evident that the complaint is unfounded. Finally, it is unclear why the platform operator should not be reimbursed for costs of dispute resolutions where the decision was in their favour. This could be an effective means to prevent abusive claims.

Trusted flaggers

Article 19

DIGITALEUROPE welcomes the proposal for a trusted flaggers regime. Such a system would bring advantages for both online platforms and third parties (including rights holders). However, the regime should continue to allow a service to manage and exceptionally prioritise other notices, based on existing internal systems, depending on the urgency/severity of the content and not purely on whether the notice comes from an accredited trusted flagger.

DIGITALEUROPE calls for the development of a trusted flagger system that is practical and efficient for all actors involved and can maximise the benefits inherent in this mechanism to streamline processes. In order to improve the proposed system, we make the following suggestions:

- We would welcome clarifications on what constitutes "organisations of industry". For example, would this include trade associations and or IPR service providers/agencies (e.g. REACT).
- We are concerned that trusted flaggers, as defined in the proposal, acting on behalf of multiple rightsholders who could have a different tolerance on what constitutes an IPR infringement. This may expose individual rightsholders represented by the broader organisation to the risk of losing its trusted flagger status because of the actions of others represented by the same organisation.
- Clarifications would be helpful on how a Digital Services Coordinator should assess trusted flaggers, the authority granted to a trusted flagger, whether there are any limitations (e.g. field of expertise, or to any geographic or other limitation) and finally, whether there are limits to the number of trusted flaggers.

DIGITALEUROPE believes that the Digital Services Coordinator should be able to grant platforms the power to appoint additional trusted flaggers, including individual companies or rights holders, as well as maintaining an ultimate right to receive requests from and appoint entities to trusted flagger status. 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.

It is important that the Digital Services Coordinator of the respective Member State engages in dialogue with platforms and rightsholders to gather input on making appointments and for maintaining the accuracy and efficacy of a trusted flagger system. The trusted flaggers status should be revoked if a trusted flagger has submitted a significant number of insufficiently precise or inadequately substantiated notices with an ultimate right of appeal to the Digital Service Coordinator in the relevant territory.

Measures and protection against misuse

Article 20

DIGITALEUROPE welcomes the inclusion of specific measures to address users frequently providing illegal content and those involved in submitting unfounded notice and takedown complaints. Such measures help to improve content moderation and ultimately help to boost trust in the digital environment. However, we would like to see more flexibility inserted in Article 20.

We see the need to strengthen the provisions against repeat offenders. It should be possible to permanently exclude repeat offenders from a platform rather than merely suspending them temporarily. We are concerned that if Article 20 is given a strict interpretation, the hosting provider may be limited from suspending services without prior notice, and after a single severe incident because the text suggests suspension can only occur if something occurs "frequently". The DSA should be clear that the rules defined are a baseline and intermediaries can go beyond what is set out in this clause, as in many cases, "suspension" should be permanent or at least conditional on a set of commitments to actions to remove illegal content or in case of manifestly unfounded notices, to improve the quality of notices. In our view, the provisions on measures and protection against

misuse of the notice and action mechanisms by individuals or entities outlined in Art. 20(2-3) would be best placed under Art.14 on notice and action mechanisms.

DIGITALEUROPE would also welcome clarifications on the meaning in Art. 20(3)(a) of the wording "manifestly illegal content" and how it differs from "illegal content".

DIGITALEUROPE also recommends that Art. 20(3)(d) should be deleted, as it would require online platforms to evaluate the "intention" of the alleged abuser, which would entail a subjective assessment online platforms are not appropriately placed to investigate or judge. The requirement in Art. 20(4) should be in general terms so as to avoid providing a roadmap to abuse. This issue was successfully addressed in the P2B Regulation and that should be reproduced here.

Traceability of traders

Article 22

Traceability of traders is an important tool for platforms to prevent misuse of their services, dis-incentivise bad actors online and provide a safe and trusted environment for their customers. Several DIGITALEUROPE members already conduct background checks on business users. While DIGITALEUROPE welcomes the introduction of legally mandated KYBC schemes, we want to underline the need to consider further the diversity of digital services and the variety of actors subject to these obligations.

The information that a trader must provide to an online platform must be workable and proportionate. We want to avoid a situation where legitimate traders are put off opening an account unnecessarily. In this regard, with the exception of the self-certification regime under Art. 22 (1)(f), product-specific information, which is not related to a trader's traceability, and may not be known at the time of account creation, should not be required.[3]

Overall, we recommend clarifying that the trader should provide all the information required under Article 22 to the online platform and that the online platform should not be held liable for information provided by the trader that ends up being false. The registration system in the DSA should be coherent with the system in other areas in which such (legal) obligations already exist, such as

[3] In this respect, the requirement to collect information on the economic operator in Art. 22(1)(d) has nothing to do with the “traceability” of the trader. It is product-specific information. This introduces a monitoring obligation for one specific legal requirement and product type (as there is no general obligation for a product to have an EO). Marketplaces don’t have a relationship with EOs, and there’s no public register, so verification is impossible. A trader will have many products with different EOs, and the EO is the same for a product no matter who sells it, so it does not make sense to collect and verify that information from every individual trader.

money laundering, in order to prevent duplication. Where a trader has already been subject to financial KYC in respect to a particular platform, it may be appropriate to discharge the KYBC obligation of the online platform to the extent that such financial KYC overlaps with KYBC obligations in the DSA.

DIGITALEUROPE recommends that where the online platform has been notified by an authority of legal action against a trader, they should maintain the information collected via Article 22 until resolution of the action and should not delete the information of expiry of their contractual relationship with the trader.

Transparency obligations

DIGITALEUROPE's members are committed to increasing transparency vis-a-vis governments, regulators, researchers and users. Our platform members already provide various transparency tools that allow stakeholders to better understand their content management policies and enforcement, and always look for further ways to expand meaningful transparency. That includes also publishing of regular transparency reports.

The legislators should ensure that the final DSA text takes into account already existing transparency measures while ensuring that users' privacy is protected, bad actors are prevented from misusing the systems and that commercially sensitive information is not revealed. The provisions also need to be technologically neutral and flexible to respect the specific nature of various online intermediaries and their services. Finally, any transparency obligations should be tailored to the needs of the specific stakeholders for which they are introduced. For example, meaningful transparency will likely mean something else for the average user vis-a-vis a regulator. Finally, we would be concerned if the DSA allowed third parties to require direct access to platforms' algorithms.

Transparency reports

Articles 13, 23, 33 / Recitals 39, 51, 65

DIGITALEUROPE recognises the importance of improving accountability and user trust. Our members are participating in numerous voluntary codes of conduct, for example, the Code of Practice on hate speech or the Product Safety Pledge. It is critical to ensure that reporting obligations are proportionate, reasonable and scalable.

Transparency requirements should allow for enough flexibility to take into account the differences between services. Metrics based on "average turnaround time" are problematic for several reasons - 1) platforms might be forced to prioritise speed, 2) it may not be the most effective metric to assess the effectiveness of the measures deployed by a platform, and 3) measuring average

turnaround times risks disregarding other relevant measurements. Where appropriate, services should be able to opt to use more meaningful metrics, such as median turnaround times or a number of interactions with a piece of content.

Overall, we urge policymakers to also consider what the audience of such transparency reporting requirements is. The average user may not benefit from the same level of detail as researchers or regulators. On the contrary, too much detail or technical explanations may overwhelm users and fail to achieve meaningful user transparency. For example, it is not clear why statements of reasons under Art.15(4) or the reports under Art.33(2) need to be made publicly available.

Additional obligations for VLOPs to manage systemic risk

Chapter 4 on very large online platforms (VLOPs) differentiates from the rest of the proposal solely based on the number of users. Linking regulation to threshold values such as user volume, as suggested by the proposal, broadly reflects a notion of proportionality – the idea that small enterprises should not be burdened with the same obligations as their larger counterparts which have more resources – and the understanding that services with a high user volume and reach have a greater societal and economic relevance and thereby responsibility. Even if this notion of proportionality is correct and reach remains the decisive factor, it may be inappropriate or ineffective to link regulation only to specific threshold values.

When it comes to determining which platforms should take additional measures to prevent the dissemination of illegal content, additional qualitative factors should also be considered. The provider with the most monthly users might not necessarily be the most likely to disseminate illegal content. Therefore, we propose a mechanism that allows platforms that exceed the VLOP 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.

Advertising transparency

Articles 24 & 30 / Recitals 52 & 63

It will be critical to ensure that ads libraries do not disclose business-sensitive information. It is also important to clarify that the ads libraries should not be required to cover ads that were disapproved or removed for policy violations. Online platforms should be allowed enough flexibility while building these libraries, taking into account differences in their services and the scale in which they are operating.

It is also important to note the shared responsibility when it comes to transparency - advertisers themselves play an important role in terms of providing necessary information.

We understand concerns around the role that personalised advertising might be having on political decisions of citizens. That is why many DIGITALEUROPE members launched ads libraries for elections ads. However, we would suggest limiting the need to provide detailed information about ads targeting only to political or otherwise sensitive ads. The creation and maintenance of such repositories more generally is a hugely disproportionate burden, for example, where it is clear that the advertisements appear in digital services devoted to the very goods and services promoted. Maintaining an advertising archive would mean a significant administrative burden and result in distorting competition. There is no such publicly accessible archive for other advertising channels, and there is no compelling reason for why this should be any different for online advertising.

Data access to researchers

Article 31, Recital 64

The DSA should define clear limits when it comes to the scope of data that vetted researchers might request. Legislators should clarify what "reasoned requests" encompass, set very clear parameters regarding what types of data vetted researchers can request and what can be shared with them. The DSA should help ensure all necessary privacy compliance safeguards, including by respecting the principle of purpose limitation and requiring researchers to access and review any data through tools and systems mandated by the online platforms.

We agree that VLOPs should be equipped with a right for due process and a right to challenge requests received. However, we believe that grounds to refuse requests should be extended to not only include unavailability of data requested or protection of trade secrets but to also include concerns about the requesting institution or academic in particular and the purposes for which it may be used. We are strongly of the view that the details on exact circumstances under which VLOPs have to share data with these groups should not be left to be decided in Delegated Acts as this is an extraordinary power and should instead be specified in the Regulation itself. Lastly, we urge flexibility in the format that data would be transferred in so as not to impose additional burden.

We would also welcome clarity as to the interplay of this DSA provision with similar provisions proposed by Germany in the context of the NetzDG revision and the implementation of the Copyright Directive. Both German provisions have been notified to the European Commission. We suggest that the European

Commission examines them carefully, in particular in so far as their compatibility with the country-of-origin principle is concerned.

Risk assessments & mitigation

Articles 26 & 27 / Recitals 56-59

We appreciate the importance of assessing and acting to mitigate risk. The DSA should further clarify what platforms need to do to satisfy these requirements. We are concerned that unclear requirements could lead to platforms being overly cautious, simply in order to prevent the oversight bodies to apply penalties. This might lead to removals of legitimate lawful content, thus having a negative impact on fundamental rights, such as freedom of expression, access to information and the freedom to conduct business

Risk assessments might include highly sensitive information about platforms. Making such information publicly available (beyond the Commission and platforms concerned) creates risks related to trade secrets. It is also vital that risk assessments do not become a tool for bad actors to game the system. To the extent that any trade secrets are specifically identified in the risk assessments or vulnerabilities that would allow bad actors to game the system, platforms should be able to claim confidentiality and accordingly redact their reports with respect to such disclosures which are to become public. The legislative proposal should also include penalties for potential violations of confidentiality by the Digital Coordinators or the Commission.

Independent audits

Article 28 / Recitals 60 & 61

Given the scope of the DSA, clarifying the scope of these audits will be critical in order to create a clear and functioning system of constructive collaboration between platforms and the regulators. For example, the provisions on Codes of Conduct (Article 35) and on Crisis Protocols (Article 37) already envisage that there will be reporting on the measures taken under those frameworks--such reporting will allow assessments that are tailored and more appropriate to the measures at issue than the broader auditing framework; these frameworks should therefore be out of scope of routine independent audits.

To support the usefulness of auditors' findings, especially given the large scope proposed in Art. 28(1), the DSA should provide mechanisms to facilitate areas of more specific focus in a given auditing period. For example, this could include DSCs providing an annual plan that identifies to VLOPs and their auditors' key areas of interest for the upcoming reporting period.

It will be also important to clarify the nature of the auditors, ensuring a high level of accuracy, consistency, privacy and independence. Similarly to other transparency obligations, it will be critical to assure that trade secrets and privacy of users are protected.

The current timelines regarding providing timelines would not give platforms enough time to provide necessary feedback. To allow sufficient time for activities, the frequency of routine audits under Art. 28(1) should be at least every two years. Similarly, remediation auditing timelines should be flexible and adopt a risk-based approach, where the response time would be based on the scope, severity and complexity of the recommendations.

Recommender systems

Article 29 / Recital 62

We support efforts to give users more control and transparency around recommendations, so long as any requirements are flexible and principled-based, so that they can be tailored to the particular service.

It will be important to ensure that the obligations with respect to recommender systems respect the specifics of intermediaries and different models. Given their scale, some recommendations are critical - also to limit the potential reach of harmful or borderline content.

Governance & enforcement

Country of origin

DIGITALEUROPE welcomes that the country-of-origin principle has been maintained as a guiding principle as it is fundamental in providing legal certainty to businesses operating cross-border in the EU and ensuring that platforms are not subject to 27 different legal regimes. The principle eliminates burdens for SME businesses and supports innovation and growth in digital services. Further, the right of a party to seek redress in a dispute in accordance with Brussels I, other specific instruments such as the Trade Marks Regulation, and recent case law developments should be maintained[4].

However, today, there still exists doubt about the interpretation of the country-of-origin principle and, consequently, businesses, in practice, still feel obliged to

[4] Both the EU Regulation No.1215/2012, often referred to as “Brussels I” and Council Regulation (EC) No.207/2009 (“the Trade Mark Regulation”) contain exceptions that allow a party to choose either to sue a defendant in the country of origin or in the country of destination based on rules elaborated in case law such as the recent ECJ decision C-172/18 AMS Neve Ltd.

adapt to legislation in the countries where the users are located. Aside from the fact that each Member State can exempt national rules, some Member States, like Denmark, interpret the principle in a way that it only pertains to public law, whereas other Member States interpret the principle as also pertaining to civil law in several areas. Therefore, DIGITALEUROPE calls for more guidance on the interpretation of the principle.

Ultimately, the best way to ensure the effectiveness of single market legislation is to strengthen the cooperation between Member States. DIGITALEUROPE welcomes enhanced coordination and cooperation across the EU. Hence, it is important that the European Board for Digital Services ensures consistent application of the DSA and its core principles. The interpretation of the country-of-origin principle should therefore be added to the activity reporting of Article 44.

Cross-border orders from authorities

DIGITALEUROPE welcomes the provisions (Articles 8 & 9) to clarify how authorities can flag illegal content and request information from platforms. However, further clarifications are needed. Firstly, the draft proposal lacks procedural rules to clarify how online intermediaries can challenge orders that are unlawful. Online intermediaries need clear and effective means to do so. Secondly, it is unclear whether the scope also includes cross-border orders to act against illegal content or provide information are possible and if so, according to which procedure. Due to cultural differences and different legal approaches to illegal content among Member States cross-border orders can in some areas be problematic.

If the DSA foresees cross-border orders, Article 9 should be aligned with the e-Evidence Regulation. It is important that the regime does not undermine the country-of-origin principle, which remains key to the functioning of the internal market.

Digital Services Coordinator

DIGITALEUROPE welcomes the introduction of a "Digital Services Coordinator" to oversee enforcement of the Regulation as it makes cooperation with legal enforcement authorities simpler. We also support the establishment of the European Board for Digital Services as it is important to contribute to the guidance and consistent application of the Regulation and assist the digital service coordinators. It is essential that the new rules are interpreted consistently across the EU to support clarity for business.

The DSA should provide more clarification on the processes and procedural safeguards for cross-border cooperation among Digital Services Coordinators. As regards requests to the Digital Services Coordinator of establishment to

investigate a suspected infringement (Article 45), the DSA should clarify the thresholds for triggering this mechanism - we would recommend linking this threshold to a definition of systemic failure tied to specific provisions in the DSA. The current reference to "an infringement" of the DSA is too generic and does not serve legal certainty.

Given the importance of the country of origin principle we identify above, we would also welcome clarification on the processes and procedural safeguards for joint investigations provided for in Article 46, including the interaction with oversight responsibility of the country of establishment, and on the expected nature of actions resulting from any joint investigations.

Sanctions

Any sanctions should be based on systemic violations, where there has been a sustained failure to comply with specific DSA obligations, rather than one-off events or individual pieces of content. The DSA should make clear what constitutes systemic violations.

Sanctions and fines should be proportionate to the service itself, rather than the overall corporate ownership.

Regarding the enforcement of interim measures and fines, the Member States and the Digital Services Coordinator play an important role. We have experienced with the GDPR, that some Member States are not able to issue financial fines through the competent national authority and the case is therefore referred to the police as the next step. In these circumstances, it is important, that we learn from our previous experiences and put in place a smooth process from the beginning as it otherwise creates an insecure situation for the business involved.

Implementation timeline

DIGITALEUROPE has concerns about the feasibility of the implementation timeline. We would recommend a 12 to 18 month period to leave sufficient time to build and implement new processes.

FOR MORE INFORMATION, PLEASE CONTACT:

Hugh Kirk

Policy Manager

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

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, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
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: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK