EuroISPA's views on the Digital Services Act

Introduction

EuroISPA is the voice of the European Internet industry, representing over 2,000 Internet Service Providers across Europe, all along the Internet value chain. As we have been engaging in discussions on intermediary liability and content moderation for over 20 years, we highly appreciate the opportunity to share our feedback with the European Commission on the Digital Services Act (DSA).

Overall, EuroISPA supports the DSA and its objectives to protect consumers and their fundamental rights online, to foster transparency and accountability of online platforms, and to favour innovation, growth, and competitiveness within the Single Market.

In particular, we welcome that the European Commission decided to adopt an evolutionary approach maintaining the key principles of the E-Commerce Directive, such as the limited exemption from secondary liability while creating a due diligence framework for intermediary services. At the same time, EuroISPA believes that several changes would be needed in order to achieve a regulation truly fostering innovation and growth in the Digital Single Market. Therefore, we call on policymakers to take into consideration the recommendations below:

Recommendations on Chapter I – General Provisions

We welcome the horizontal scope of the DSA

EuroISPA welcomes that the proposed DSA will apply horizontally to any type of illegal content. Differing procedures for different types of content should be justified by objective distinctions (for example, whether or not the nature and legal status of the content are objectively classifiable; whether or not the alleged infringement is of criminal law or instead of private rights).

Coherency between the DSA and existing horizontal and vertical legislation is necessary

Policymakers will need to ensure legal coherence between the DSA and existing vertical and horizontal laws. Coherence with other legislation must conform with the requirements of the Treaties, including on its compatibility with European and national competences respectively. In order to achieve that, the extensive use of wording mentioning that the DSA is "without prejudice" to other laws should be

carefully assessed and limited to the particular provisions for which a derogation from existing legislation is necessary.

We support the DSA clearly distinguishing between illegal content and harmful but legal content

EuroISPA supports the DSA clearly distinguishing between illegal content and harmful but legal content.

Illegal content is precisely defined by law and is not influenced by individual positions and moral views, as it is defined through the democratic process. Harmful content lacks such qualities, and, as soon as it is defined in law, it becomes "illegal". In terms of protection from liability, the implications of these two kinds of content also diverge. While certain platforms are able to filter out illegal content, it is impossible for them to moderate harmful content on a fair and legal basis without running into the risk of losing their limited liability.

Furthermore, from certain subjective points of view, dealing with "harmful content" online would amount to censorship, harming citizens' fundamental rights such as freedom of speech. The definition of "harmful" is highly contentious, and frequently includes material that is considered contrary to social welfare or good policy according to one political or philosophical viewpoint or another: in other words, advocates of one political or philosophical position claim that their opponents' material is harmful.

It would undermine both freedom of expression and the integrity of the European democratic process if online platforms that are central to public debate were to take sides in such disputes. Even accidentally, by suppressing lawful material from one political cause, or at the demand of another, on the basis of a disagreement of view.

When companies do take voluntary actions to moderate specific kinds of lawful content on their services, in accordance with their terms of service, they should comply with certain requirements. They should ensure fair treatment of users procedurally, by providing them with clarity and transparency concerning decisions on content, and by putting in place appropriate processes to maintain a high quality of decision making, enabling users to challenge decisions made against them and to hold online platforms to a consistent and unbiased standard.

The definition of "online platforms" is too broad

While the differentiation between pure hosting service providers and online platforms is to be welcomed, the definition of "online platforms" (Article 2(h)) is potentially too broad.

The concept of "dissemination to the public" (Article 2(i)) is problematic: it refers to making information available to a "potentially unlimited number of third parties". Such a definition risks including infrastructure services such as webhosting or cloud services, as they store and share content at the request of the recipient of the service and make that content available to users from the general public (e.g. anyone visiting a web site).

We identify two significant flaws in the definition given of online platform:

- Firstly, it fails to clearly distinguish between infrastructure services and platforms which have a greater role and function in relation to the content, and so risks misclassifying most hosting services as online platforms; and
- Secondly, we believe it needs to be made clear that when considering whether information is disseminated to the public, what is to be considered is whether there is already an existing private relationship between the content provider and the end-user accessing that content, and not the relationship between the intermediary and either one of them.

Distinguishing online platforms from mere hosting

The key distinction between traditional web hosting services that merely connect a third party website to the Internet, and online platforms such as Facebook, Youtube, Instagram and Twitter, is that traditional web hosting services play no role in determining what content is available or displayed to particular users: the web site owner determines what content exists and how it is presented, and the intermediary merely facilitates its availability on the Internet. By contrast, in an online platform, it is the platform itself that determines (algorithmically) what content is presented to the visitor, by selecting from amongst content provided by one or more of the content providers. Thus, an online platform plays a role and function in the selection of content that a mere hosting provider does not. It is this additional function that provides both the reason for imposing additional obligations on the platform, and in many cases the means of discharging those responsibilities.

Improving the definition

Accordingly, we recommend that where content providers store information on an intermediary hosting services and that information is later accessed by members of the public,

- If the intermediary selects which information/content members of the public see from amongst a selection of content provided by the content providers, then the intermediary is an online platform; whereas
- If the information accessed by the public at a given address or on a given service is wholly controlled by the content providers themselves, and the intermediary plays no role in determining what content is accessed by which users (other than by removing illegal content from the hosting service altogether), then the intermediary is merely a hosting service and not an online platform.
- In applying this definition, “public” and “private” shall be construed according to the relationship (or lack thereof) between the users providing the content and the users accessing it, and not according to the relationship between the intermediary and either one of them.
- Consistent with the definition of information society services, it should be clarified that only online platforms storing and disseminating to the public information on a commercial basis should fall into the definition.

Enterprise hosting services should not be included in the scope of the additional obligations

Enterprise hosting services do not have the technical capabilities to identify or remove specific pieces of content that their customers store on their services. They also generally do not have a direct contractual relationship with the individuals who stored the content. Therefore, enterprise hosting services should be excluded from the scope of the DSA's obligations - while still benefitting from the limitations on liability and related provisions.

Maintaining the Country of Origin Principle

The Country of Origin principle is one of the key features of the E-Commerce Directive and has played an essential role in the development of the Internet as we know it today. However, the DSA, especially its Articles 8 and 9, risk undermining the long-established Country of Origin principles. An additional focus should be put on the question of conflicts of laws and the general principles of international law (see Article 8 (2) (b) DSA). Furthermore, solutions for immanently emerging issues need to be found on how to prevent national laws from intervening with the Digital Single Market and with companies acting on an international level - within but also outside of the EU.

Gaining clarity on "ancillary features"

Clarification on the application of the DSA on ancillary features of services would be welcome. While some recitals do provide guidance, they are not exhaustive. For instance, it is unclear whether the DSA would apply to services which are out of its scope but offer a hosting ancillary feature.

Recommendations on Chapter II – Liability of providers of intermediary services

We welcome the preservation of the limited exemption from secondary liability

EuroISPA supports the preservation of the E-Commerce Directive's limited exemptions from secondary liability for intermediary services as it is exactly this system that allowed the Internet to become this melting pot of services to the benefit of the people. On the basis of its notice-and-takedown principle hosting provider have successfully implemented and executed a procedure to remove illegal content from the Internet upon notification.

Further clarity on the liability regime and voluntary own-initiative investigations is needed

EuroISPA welcomes that Article 6 of the proposed DSA clarifies that providers of intermediary services "shall not be deemed ineligible for the exemptions from liability (…) solely because they carry out voluntary own-initiative investigations".

However, such a protection should be extended to cases in which intermediary services have actual knowledge of allegedly illicit content on which they decide in good faith that it does not qualify for removal. Especially where they implement procedures containing measures to preserve fundamental rights.

While the current proposal for Article 6 would already enhance suppression of genuinely illicit content (by removing the disincentive to search actively), this additional protection would enhance the protection of fundamental rights.

It is necessary to maintain the no general monitoring obligation

EuroISPA supports the European Commission's proposal to maintain the prohibition of a general monitoring obligation. While there has been an inaccurate interpretation of what constitutes general monitoring[1], it is clear that the definition of general monitoring, and its antonym specific monitoring, must be clearly understood. Requiring a company to scan all the information on its service to detect and take down specific content would amount to a general monitoring obligation. By contrast, specific monitoring obligations are targeted at a known user or location.

It can never be considered "specific" to target a whole category of data or a class of persons or a general description of a type of communications. Specific monitoring should be considered as the equivalent of wiretapping telecom services in the digital sphere. In order to ensure that a specific monitoring obligation is proportionate and does not infringe fundamental rights, these should be limited in time and focus on an identified target (e.g. a user or a website), rather than a category of data.

Orders to act against illegal content and Orders to provide information

The wording of Articles 8(4) and 9(4) is confusing and raises questions about when those articles would apply and creates a lack of clarity on how the DSA relates to laws which are not in conformity with Union law. They should be amended not to create the mistaken impression that their requirements prejudice other forms of applicable law.

Recommendations on Chapter III - Due diligence obligations for a transparent and safe online environment

Overall, EuroISPA supports the concept of requiring intermediary services to comply with a set of due diligence obligations, conducive to a transparent and safe online environment. Furthermore, we support the European Commission's tiered approach imposing progressively increased obligations respectively on providers of intermediary services, hosting services, online platforms, and very large

[1] Senftleben, Martin and Angelopoulos, Christina, The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market, Amsterdam/Cambridge, October 2020, https://ssrn.com/abstract=3717022.

online platforms. However, we are concerned that the overall proposed set of obligations would be too burdensome on certain parts of the industry and could potentially stifle innovation. We detail below our main concerns and recommendations:

The requirement to have a legal representative in the EU should not be an obstacle to cross-border business

It is essential that intermediary services which do not have an establishment in the EU appoint a "legal representative", so they can be reached by the European Commission or national authorities, in order to ensure accountability. However, this should not impose disproportionate barriers on cross-border business with non-EU intermediary services.

Therefore, while EuroISPA reads the text with the understanding that the function of the legal representative envisaged in Article 11 of the DSA could be fulfilled by a third-party (e.g. a lawyer or a law firm) duly authorized to act and responsible to ensure the liaison between the company and the Member States' authorities, the Commission and the Board, we would suggest adding a corresponding explicit clarification.

We note that certain stakeholders called for an obligation to appoint a legal representative for each one of the 27 Member States. We welcome that the Commission does not take up these proposals. Such a requirement would simply be unfeasible for companies without substantial financial means, it would completely run against the country of origin principle and would fragment the Single Market as a result.

Due diligence obligations applying to online platforms should not apply to medium-sized enterprises

Certain strict requirements under Chapter III, Section 3 of the DSA, such as putting in place a comprehensive internal complaint-handling system, are likely to overburden medium-sized enterprises with their limited financial and human resources.

In order to ensure that market-entry and market-viability are available to SMEs and startups, and to preserve vigorous competition and innovation, EuroISPA recommends excluding SMEs, and not only micro and small companies, from the scope of the Section.

An additional liability shield in the context of the notice and action procedures

We suggest an additional liability shield that would apply against any complaint that a provider had acted wrongfully under private or public law when it applies Article 14(6) or when it decides that it cannot do so when the takedown is not justified.

Trusted flaggers partnerships must remain voluntary

In 2019 EuroISPA gathered best practices through a written survey from companies resorting to partnerships with trusted flaggers and summarized the results in this paper. Considering the results of this study, which highlighted that such partnerships are only effective when a high degree of flexibility between the parties involved is granted, we are particularly concerned about Article 19 making collaboration with trusted flaggers mandatory.

In addition, the Article raises several other concerns. Firstly, it allows any entity to apply for being awarded a trusted flagger status by the Digital Services Coordinator of the Member State in which the applicant is established. This is particularly alarming as some entities might have vested interests, with the risk of co-opting critical platforms for political, cultural, or private economic interests. Secondly, the fact that any Member State can certify a potentially unlimited number of trusted flaggers is also dangerous, as the system might become untenable due to an overload of priority notices from a plethora of stakeholders with which the platform has no relation or any regular correspondence. However, the latter are key to the success of the trusted flagger system currently in use. Thirdly, EuroISPA believes that such entities must be a private organization, rather than a public authority.

Considering the above, we reiterate that operators should have the exclusive right to appoint trusted flaggers, including measures concerning liability, and contractual obligations for the trusted flaggers to correct mistakes. It should also be clarified that the final decision concerning the treatment of reports should stay within the online platform concerned.

Preservation of the complaint mechanism by measures against misuse

While Article 20, establishing "measures and protection against misuse", is to be welcomed, it needs to be further strengthened. Those who file fraudulent notices, in order to induce the intermediary to interfere with content published by a third party, or to induce the intermediary to restrict the third-party publisher (e.g. account cancellation), should be held accountable and liable for economic loss and other harm to both the end-user and to the Internet intermediary. A mere suspension of the account of an individual or entity fraudulently abusing the system would not provide adequate remedy, not least because such fraudulent misuse could be continued even without an account, causing serious harms to both the online platform and targeted victims.

Limiting the know-your-business-customer principle to online marketplaces

EuroISPA supports the European Commission's approach to enforce measures ensuring the traceability of traders in order to further strengthen consumer protection.

"Know your business customer" requires a careful balance between the privacy interests of the person being required to identify themselves and countervailing interests supporting disclosure. We believe that for online marketplaces, the risks of harms from fraudulent traders justifies introducing "know

your business customer". We do not think the privacy interests are so easily overcome in the case of mere online speech, where the risk of harms is not so severe and the chilling effect of requiring disclosure of personally identifying information is more pronounced. Accordingly, we recommend that Know Your Business Customer requirements be applied exclusively to online marketplaces.

However, several limitations to the principle should be introduced. Firstly, it is excessive to expect the operator of the marketplace to identify the full supply chain for items listed on the marketplace from the point of manufacture. Secondly, we believe that justification for this traceability concerns the safety and legality of the items listed, and accordingly it is sufficient to identify the trader that places the item for sale on the online market. The privacy of the customer that purchases the item can be maintained. Accordingly, EuroISPA recommends that the obligations to identify traders should be limited in scope to identifying traders that place items for sale on online marketplaces. Thirdly, the provider should not be liable for information given by the trader which is false or misleading.

Data access, scrutiny, and trade secrets

It should be clarified that, when being audited, respecting their transparency obligations, or granting data access to researchers, very large online platforms should not be asked to disclose commercially and operationally sensitive information, including for example source-code of algorithms and other industry secrets. Further, access to especially sensitive data should not fall under an obligation to be made accessible online. EuroISPA recommends clarifying with regards to Article 31(5) the purpose for which the data may be used to be defined in the legal text and not be left to the decisions of the European Commission on the basis of delegated acts.

The provision on very large online platforms' risk assessments must be clarified

Article 26 of the proposal requires very large online platforms to perform a risk assessment, which also entails the analysis of "intentional manipulation of their service" (Article 26(1)(c)). The fact that the list of such "manipulations" is open-ended creates legal uncertainty, transmitting a high level of quasi-legislative responsibilities to the very large online platform in question. This lack of foreseeability for businesses, coupled with the threat of massive sanctions, is problematic from a rule of law standpoint. Therefore, EuroISPA suggests amending the Article and limiting it to an exhaustive list.

The provisions on VLOP risk mitigation

The provisions on risk mitigation by online platforms fail to meet essential standards for foreseeability in law. They are targeted at an unknown and unknowable set of risks, yet to be identified, and extend to an unknowably broad set of future mitigations. It is impossible for the Legislator to assess whether the measures to be taken under this section are of a kind that would be necessary or proportionate, a core legislative responsibility.

However, not all risks in society need to be acted upon by removal, but some risks are necessarily incurred as the price for a free and democratic society. Consequently, it is necessary in a democratic society for the Legislator to assess whether a particular class of risk (as yet unidentified) requires mitigation at all, as well as at least the broad outlines of the measures to be taken. Setting these basic boundaries cannot be delegated to a regulatory agency on the basis that it, rather than the legislative body, will determine public policy as to where the public interest lies, or when public policy overcomes fundamental rights.

Accordingly, the provisions on risk mitigation must be much more clearly specified, both in terms of the risks to which they would apply and the measures to be taken, so that they may meet minimum standards of legal foreseeability.

Recommendations on Chapter IV - Implementation, cooperation, sanctions, and enforcement

Penalties should be proportionate and take into account specificities of SMEs

EuroISPA questions why the European Commission envisages sanctions of up to 6 % of the annual income or turnover of the provider of intermediary services concerned and periodic penalty payments of up to 5 % of the average daily turnover of the provider of intermediary services concerned (Articles 42, 59, and 60). Such high penalties seem disproportionate, exceeding even those of the GDPR.

Sanctions against operators for non-compliance should be proportionate to the offence and level of culpability. When determining the sanction, aggravating and mitigating factors, such as the size and capabilities of the intermediary, must be considered. Individual instances of non-compliance with a statutory duty should only give rise to a maximum penalty proportionate to that instance of non-compliance. If the operator systematically refuses to comply, a greater sanction that is sufficiently dissuasive may be justified, but this further aggravation should be proved, not assumed. Sanctions should only be assigned after verifying that the online platform has failed to deliver the best efforts to comply with the obligations, rather than because of the failure to achieve the assumed result.

Access blocking must be limited and clearly defined

EuroISPA sees a clear need to limit the enforcement powers of Digital Services Coordinators (DSCs), as the current text would provide them with the possibility to impose web-blocking injunctions on intermediary services. For instance, Article 41(2)(b) allows them to “impose remedies proportionate to the infringement and necessary to bring the infringement effectively to an end”, which grants wide room for interpretation.

Similarly, Article 41(3)(b) envisages blocking obligations, as it describes the possibility of imposing a “temporary restriction of access of recipients of the service concerned by the infringement or, only where that is not technically feasible, to the online interface of the provider of intermediary services on which the infringement takes place.”

Therefore, EuroISPA recommends adopting a principle of "subsidiarity." In the first instance, competent authorities should always take action against the content provider of the illegal content itself (the user) or the online platform. Removal at source should always be the preferred and prioritised solution. Only in the case that there is no action by the content provider or platform, as ultima ratio, the DSC should request an access provider to intervene. It is up to the access provider to determine the technical means by which blocking is achieved. As blocking at the level of the access provider is in principle neither effective nor proportionate, such injunctions should only be mandated by a court or a public authority, in full respect of fundamental rights' safeguards, accompanied by cost reimbursement for the affected Internet intermediaries.

Ensuring that commitments are without prejudice to rights of third parties

Articles 41 and 56 allow Digital Services Coordinators (DSCs) and the European Commission respectively to accept commitments by providers and make those binding. Given the broad and ill-defined nature of the commitments that could be made, these agreements have the potential to have adverse impacts on the rights and interests of third parties, either inadvertently or as a matter of policy preference, but without the third party being heard or their interests being duly taken into account.

To protect against such eventuality, such agreements should be published in draft form and the DSC should have a duty to consult publicly and to consider the legitimate interests of third parties before they are finalised. After an agreement is concluded, where a third party alleges their rights have been harmed by the operation of the agreement, they should have the right to challenge the application of the agreement to them before an appropriate tribunal, with the possibility of the DSC and the VLOP being required to revise the agreement to take into account third party interests if their claim is upheld. To ensure that this mechanism does not unduly intrude onto the DSC's regulatory responsibility, such challenge should only cover positive harms caused by the commitments made; it should not be possible to challenge an such agreement on the basis that the DSC failed to obtain commitments to further protect the third party's interests.

Recommendations on Chapter V – Final provisions

An overly short application deadline would not be conducive to widespread adoption of the rules

Article 74 envisages that the DSA will apply from three months after its entry into force. From the point of view of the intermediary services in the scope, it would simply be impossible to adapt within such a short timeframe: the obligations imposed in Chapter III will require serious internal organizational efforts from the industry, to be able to liaise effectively with Digital Services Coordinators and the European Commission, and to be able to put in place the various mechanisms required by the law. Therefore, EuroISPA recommends extending the deadline to at least 12 months.