DIGITALEUROPE

21 June 2021

Digital Services Act amendment suggestions

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 position paper and proposes some constructive amendments 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 is contextual, difficult to define, may be culturally subjective and is often legally ambiguous.
- 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 continue to work 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.

Subject	EC proposed DSA text	DIGITALEUROPE suggested amendments	Justifications
1. Definition of online platform	**Article 2(h)** 'Online platform' means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation. **Recital 14** The concept of 'dissemination to the public', as used in this Regulation, should entail the making available of information to a potentially unlimited number of persons, that is, making the information easily accessible to users in general without further action by the recipient of the service providing the information being required, irrespective of whether those persons actually access the information in question. The mere possibility to create groups of users of a given service should not, in itself, be understood to mean that the information disseminated in that manner is not disseminated to the public. However, the concept should exclude dissemination of information within closed groups consisting of a finite number of pre-determined persons. Interpersonal communication services, as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council, such as emails or private messaging services, fall outside the scope of this Regulation. Information should be considered disseminated to the public within the meaning of this Regulation only where that occurs upon the direct request by the recipient of the service that provided the information.	**Article 2(h)** 'Online platform' means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation. ***Cloud infrastructure service providers shall not be covered by the definition of online platforms.*** **Recital 14** The concept of 'dissemination to the public', as used in this Regulation, should entail the making available of information to a potentially unlimited number of persons, that is, making the information easily accessible to users in general without further action by the recipient of the service providing the information being required, irrespective of whether those persons actually access the information in question. The mere possibility to create groups of users of a given service should not, in itself, be understood to mean that the information disseminated in that manner is not disseminated to the public. However, the concept should exclude dissemination of information within closed groups consisting of a finite number of pre-determined persons. Interpersonal communication services, as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council, such as emails or private messaging services, fall outside the scope of this Regulation. Information should be considered disseminated to the public within the meaning of this Regulation only where that occurs upon the direct request by the recipient of the service that provided the information. ***Consequently, providers of cloud infrastructure services should not be covered by the definition of online platforms.***	• 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).
2. Consumer protection	**Article 5(c)** Paragraph 1 ~~***shall not apply with respect to liability under consumer protection law of***~~ online platforms allowing consumers to conclude distance contracts with traders~~***, where such an online platform presents the specific item of information or otherwise***~~	**Article 5(c)** ***Notwithstanding Article 5*** paragraph 1***,*** online platforms allowing consumers to conclude distance contracts with traders ***on the platforms shall ensure that the trader complies with its obligations under Article 13 of Directive 2011/83/EU, Article 16 (1) of Directive***	• The limited liability safe harbour for consumer protection should not be dependent on the subjective impression of the consumer – this would lead to significant legal uncertainty for the design of services. Instead, we propose to make this dependent on the platform fulfilling it's trader traceability obligations under article 22. If the traders' data are verified and published, there should

Subject	EC proposed DSA text	DIGITALEUROPE suggested amendments	Justifications
	~~***enables the specific transaction at issue in a way that would lead an average and reasonably well-informed consumer to believe that the information, or the product or service that is the object of the transaction, is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control.***~~	***2019/770/EU and Article 13 (3)(b) of Directive 2019/771/EU if and to the extent that the online platform fulfils its obligations under Article 22.***	be no more doubt for the consumer that the sale is made by this trader and not the platform. Furthermore, the amendment seeks to specify which consumer protection rights the platform should cover in such cases.
3. Voluntary own-initiative investigations and legal compliance	**Article 6** Providers of intermediary services ~~***shall not be deemed ineligible for the exemptions from liability referred to in Articles 3, 4 and 5 solely because they carry out voluntary own-initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content, or take the necessary measures to comply with the requirements of Union law, including those set out in this Regulation.***~~	**Article 6** ***In order to encourage proactive activities to detect and take action on illegal content by*** providers of intermediary services***, such providers shall not be deemed to have actual knowledge of an illegal activity or illegal content for the purpose of Article 3, 4 and 5 solely because they carry out a voluntary activity, by automated or non-automated means, to detect and identify illegal content or content that violates their terms and conditions.***	• 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.
4. Orders to act against illegal content	**Article 8** (1) Providers of intermediary services shall, upon the receipt of an order to act against a specific item of illegal content, issued by the relevant national judicial or administrative authorities, on the basis of the applicable Union or national law, in conformity with Union law, inform the authority issuing the order of the effect given to the orders, without undue delay, specifying the action taken and the moment when the action was taken. (2) Member States shall ensure that the orders referred to in paragraph 1 meet the following conditions: (a) the orders contains the following elements: – a statement of reasons explaining why the information is illegal content, by reference to the specific provision of Union or national law infringed; – one or more exact uniform resource locators and, where necessary, additional information enabling the identification of the illegal content concerned; – information about redress available to the provider of the service and to the recipient of the service who provided the content; (b) the territorial scope of the order, on the basis of the applicable rules of Union and national law, including the Charter, and, where relevant, general principles of international law, do~~***es***~~ not exceed what is strictly necessary to achieve its objective; (c) the order is drafted in the language declared by the provider and is sent to the point of contact, appointed by the provider, in accordance with Article 10.	**Article 8** (1) Providers of intermediary services shall, upon the receipt of an order to act against a specific item of illegal content, issued by the relevant national judicial or administrative authorities, on the basis of the applicable Union or national law, in conformity with Union law, inform the authority issuing the order of the effect given to the orders, without undue delay, specifying the action taken and the moment when the action was taken. ***NEW (1a) Only providers that have the legal right and technical ability to locate and remove specific items of content identified on the service at issue fall within the scope of this Article.*** (2) Member States shall ensure that the orders referred to in paragraph 1 meet the following conditions: (a) the orders contains the following elements: – a statement of reasons explaining why the information is illegal content, by reference to the specific provision of Union or national law infringed; – one or more exact uniform resource locators and, where necessary, additional information enabling the identification of the illegal content concerned; – information about redress available to the provider of the service and to the recipient of the service who provided the content; (b) the territorial scope of the order, on the basis of the applicable rules of Union and national law, including the Charter, and, where relevant, general principles of international law, ***and the requirements imposed by the order,*** do not exceed what is strictly necessary to achieve its objective; (c) the order is drafted in the language declared by the provider and is sent to the point of contact, appointed by the provider, in accordance with Article 10. ***NEW (2a) Member States shall ensure that, where a provider of an intermediary service has a good faith belief that complying with an order referred to in paragraph 1 would infringe on the fundamental rights enshrined in the Charter or otherwise infringe Union or Member State law, the service provider has the right to challenge the order in the Member State of its establishment.***	• These amendments ensure the obligations under Article 8 are workable. More specifically, they ensure (1) that providers can object to orders that they believe contravene EU or Member State law; (2) that where a provider does comply with an order, it will not face liability under Union or Member State law for doing so; and (3) that only providers with the legal right and technical ability to locate and remove specific items of content identified on the service at issue are obliged to comply with orders to act against illegal content. For clarity, the Commission should publish a list of all national courts and authorities that may lawfully issue orders under Article 8, so that providers do not face any uncertainty about whether a particular order was issued by an appropriate authority.

Subject	EC proposed DSA text	DIGITALEUROPE suggested amendments	Justifications
		NEW (2b) Where a provider of an intermediary service complies in good faith with an order referred to in paragraph 1, the provider shall not be liable under Union or Member State law for any measures reasonably taken to enable such compliance.	
	(3) The Digital Services Coordinator from the Member State of the judicial or administrative authority issuing the order shall, without undue delay, transmit a copy of the orders referred to in paragraph 1 to all other Digital Services Coordinators through the system established in accordance with Article 67.	(3) The Digital Services Coordinator from the Member State of the judicial or administrative authority issuing the order shall, without undue delay, transmit a copy of the orders referred to in paragraph 1 to all other Digital Services Coordinators through the system established in accordance with Article 67. ***NEW (3a) The Commission shall publish a list of the relevant national judicial or administrative authorities empowered to issue orders referred to in paragraph 1 on the basis of the applicable Union or national law on a dedicated website, and keep it updated.***	
5. Notice and action mechanisms	**Article 14** (5) The provider shall also, without undue delay, notify that individual or entity of its decision in respect of the information to which the notice relates, providing information on the redress possibilities in respect of that decision. (6) Providers of hosting services shall process any notices that they receive under the mechanisms referred to in paragraph 1, and take their decisions in respect of the information to which the notices relate, in a timely, diligent and objective manner. Where they use automated means for that processing or decision-making, they shall include information on such use in the notification referred to in paragraph 4.	**Article 14** (5) The provider shall also, without undue delay, notify that individual or entity of its decision in respect of the information to which the notice relates, providing information on the redress possibilities in respect of that decision***, unless the provider has a reasoned justification for not providing such notification.*** (6) Providers of hosting services shall process any notices that they receive under the mechanisms referred to in paragraph 1, and take their decisions in respect of the information to which the notices relate, in a timely, diligent and objective manner. ***Providers of cloud infrastructure services may discharge their obligation to process a notice by re-directing it to the actor that has direct control of, or has the technical and operational capability to remove or disable specific items of illegal content.*** Where they use automated means for that processing or decision-making, they shall include information on such use in the notification referred to in paragraph 4.	• Service providers should have appropriate flexibility when informing individuals who report content about their decisions, or providing information to such individuals about the use of automated means for processes and decision-making related to notice and action. In certain cases, such information could for instance, sjeopardise an ongoing criminal investigation or give rise to a material risk to the physical or mental health or safety of another person. These amendments provide that flexibility. • This article should clarify that providers of hosting services may be able to re-directed the notice to the actor that has direct control of and has the technical and operational capability to take action against specific illegal content. IT infrastructure services (such as cloud infrastructure services,), do not have direct control over content and often the only action available to the IT infrastructure provider is to take down an entire website and/or all of a customers' workloads, which is a disproportionate approach and would result in the over removal of legal content.
		NEW. Recital 40a ***Providers of hosting services should not be subject to the requirement to notify individuals or entities of their decisions in respect of the information to which a notice under Article 14 of this Regulation relates, or the requirement to provide a statement of reasons in accordance with Article 15 of this Regulation, where the provider has a reasoned justification for not providing such notification. Such a reasoned justification could be considered to exist, inter alia, where the provider has a good faith belief that notification could sjeopardise an ongoing criminal investigation or could give rise to a material risk to the physical or mental health or safety of another person. If the provider believes a reasoned justification exists, it shall inform the relevant competent and independent authority as prescribed by domestic law, who will determine if a reasoned justification exists. The provider shall act accordingly.***	
6. Trusted flaggers	**Recital 46** Action against illegal content can be taken more quickly and reliably where online platforms take the necessary measures to ensure that notices submitted by trusted flaggers through the notice and action mechanisms required by this Regulation are treated with priority, without prejudice to the requirement to process and decide upon all notices submitted under those mechanisms in a timely, diligent and objective manner. Such trusted flagger status should only be awarded to entities, and not individuals, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content, that they represent collective	**Recital 46** Action against illegal content can be taken more quickly and reliably where online platforms take the necessary measures to ensure that notices submitted by trusted flaggers through the notice and action mechanisms required by this Regulation are treated with priority, without prejudice to the requirement to process and decide upon all notices submitted under those mechanisms in a timely, diligent and objective manner. Such trusted flagger status should only be awarded to entities, and not individuals, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content, that they represent collective interests and that they work in a diligent and objective manner.	• 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). • DIGITALEUROPE believes that, while the Digital Services Coordinator is in charge of appointing general trusted flaggers, platform operators should be able to appoint additional trusted flaggers, including individual companies or rights holders with regards to the service they provide. In case of disputes in the platform's TF 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

Subject	EC proposed DSA text	DIGITALEUROPE suggested amendments	Justifications
	interests and that they work in a diligent and objective manner. Such entities can be public in nature, such as, for terrorist content, internet referral units of national law enforcement authorities or of the European Union Agency for Law Enforcement Cooperation ('Europol') or they can be non-governmental organisations and semi-public bodies, such as the organisations part of the INHOPE network of hotlines for reporting child sexual abuse material and organisations committed to notifying illegal racist and xenophobic expressions online. For intellectual property rights, organisations of industry and of right-holders could be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions. The rules of this Regulation on trusted flaggers should not be understood to prevent online platforms from giving similar treatment to notices submitted by entities or individuals that have not been awarded trusted flagger status under this Regulation, from otherwise cooperating with other entities, in accordance with the applicable law, including this Regulation and Regulation (EU) 2016/794 of the European Parliament and of the Council.	Such entities can be public in nature, such as, for terrorist content, internet referral units of national law enforcement authorities or of the European Union Agency for Law Enforcement Cooperation ('Europol') or they can be non-governmental organisations and semi-public bodies, such as the organisations part of the INHOPE network of hotlines for reporting child sexual abuse material and organisations committed to notifying illegal racist and xenophobic expressions online. For intellectual property rights, ***individual legal entities,*** organisations of industry and of right-holders could be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions. ***The status of trusted flagger may in addition be awarded by online platforms.*** The rules of this Regulation on trusted flaggers should not be understood to prevent online platforms from giving similar treatment to notices submitted by entities or individuals that have not been awarded trusted flagger status under this Regulation, from otherwise cooperating with other entities, in accordance with the applicable law, including this Regulation and Regulation (EU) 2016/794 of the European Parliament and of the Council.	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. • Trusted Flaggers should be appointed only for their area of expertise, thus e.g. an organisation with expertise in disinformation is unlikely to have the expertise for trademark violations.
	Article 19 (1) Online platforms shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers through the mechanisms referred to in Article 14, are processed and decided upon with priority and without delay.	**Article 19** (1) Online platforms shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers***, having regard to their expertise,*** through the mechanisms referred to in Article 14, are processed and decided upon with priority and without delay.	
	(2) The status of trusted flaggers under this Regulation shall be awarded, upon application by any entities, by the Digital Services Coordinator of the Member State in which the applicant is established, where the applicant has demonstrated to meet all of the following conditions: a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content; b) it represents collective interests ~~***and is independent from any online platform;***~~ c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner.	(2) The status of trusted flaggers under this Regulation shall be awarded, upon application by any entities, by the Digital Services Coordinator of the Member State in which the applicant***, whether a legal entity, organisation or entity representing collective interests,*** is established, where the applicant has demonstrated to meet all of the following conditions: a) it has particular expertise and competence for the purposes of detecting, identifying and notifying ***specific*** illegal content ***relevant to its area of expertise***; b) it represents ***(i)*** collective interests ***or (ii) has been appointed a "trusted corporate" by the online platform in question in respect to their service or (iii) has been appointed a "trusted corporate" by the Digital Services Coordinator under Article 19(3);*** c) it carries out its activities for the purposes of submitting notices in a timely, diligent, ***accurate*** and objective manner.	
		NEW (3) Any dispute resulting from the appointment or withdrawal of trusted flagger status may be referred on appeal to the Digital Services Coordinator.	
	(~~***3***~~) Digital Services Coordinators shall communicate to the Commission and the Board the names, addresses and electronic mail addresses of the entities to which they have awarded the status of the trusted flagger in accordance with paragraph 2.	***(4)*** Digital Services Coordinators shall communicate to the Commission and the Board the names, addresses and electronic mail addresses of the entities to which they have awarded the status of the trusted flagger in accordance with paragraph 2.	
	(***4***) The Commission shall publish the information referred to in paragraph 3 in a publicly available database and keep the database updated.	***(5)*** The Commission shall publish the information referred to in paragraph 3 in a publicly available database and keep the database updated.	
	(~~***5***~~) Where an online platform has information indicating that a trusted flagger submitted a significant number of insufficiently precise or inadequately substantiated notices through the mechanisms referred to in Article 14, including information gathered in connection to the processing of complaints through the internal complaint-handling systems referred to in Article 17(3), it shall communicate that information to the Digital Services Coordinator that awarded the status of trusted flagger to the entity concerned, providing the necessary explanations and supporting documents.	***(6)*** Where an online platform has information indicating that a trusted flagger submitted a significant number of insufficiently precise or inadequately substantiated notices through the mechanisms referred to in Article 14, including information gathered in connection to the processing of complaints through the internal complaint-handling systems referred to in Article 17(3), it shall communicate that information to the Digital Services Coordinator that awarded the status of trusted flagger to the entity concerned, providing the necessary explanations and supporting documents.	

Subject	EC proposed DSA text	DIGITALEUROPE suggested amendments	Justifications
	(~~6~~) The Digital Services Coordinator that awarded the status of trusted flagger to an entity shall revoke that status if it determines, following an investigation either on its own initiative or on the basis information received by third parties, including the information provided by an online platform pursuant to paragraph 5, that the entity no longer meets the conditions set out in paragraph 2. Before revoking that status, the Digital Services Coordinator shall afford the entity an opportunity to react to the findings of its investigation and its intention to revoke the entity's status as trusted flagger	***(7)*** The Digital Services Coordinator ***or the online platform*** that awarded the status of trusted flagger to an entity shall revoke that status if it determines, following an investigation either on its own initiative or on the basis information received by third parties, including the information provided by an online platform pursuant to paragraph 5, that the entity no longer meets the conditions set out in paragraph 2. Before revoking that status, the Digital Services Coordinator ***or the online platform as they case may be*** shall afford the entity an opportunity to react to the findings of its investigation and its intention to revoke the entity's status as trusted flagger	
	(~~7~~) The Commission, after consulting the Board, may issue guidance to assist online platforms and Digital Services Coordinators in the application of paragraphs 5 and 6.	***(8)*** The Commission, after consulting the Board, may issue guidance to assist online platforms and Digital Services Coordinators in the application of paragraphs 5 and 6.	
7. Measures and protection against misuse	**Article 20** (1) Online platforms shall suspend, for a reasonable period of time ~~***and after having issued a prior warning***~~, the provision of their services to recipients of the service that frequently provide ~~***manifestly***~~ illegal content.	**Article 20** (1) ***After having issued a prior warning,*** online platforms shall suspend, for a reasonable period of time ***or terminate*** the provision of their services to recipients of the service that frequently provide illegal content. ***In cases of manifestly illegal content, the platform may suspend or terminate the provision of the service without prior warning.***	• 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 restricted from suspending services without prior notice, and after a single severe incident.
8. Trader traceability	**Article 22** (1) Where an online platform allows consumers to conclude distance contracts with traders, it shall ensure that traders can only use its services to promote messages on or to offer products or services to consumers located in the Union if, prior to the use of its services, the online platform has obtained the following information: (a) the name, address, telephone number and electronic mail address of the trader; (b) a copy of the identification document of the trader or any other electronic identification as defined by Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council[1]; (c) the bank account details of the trader, where the trader is a natural person; ~~***(d) the name, address, telephone number and electronic mail address of the economic operator, within the meaning of Article 3(13) and Article 4 of Regulation (EU) 2019/1020 of the European Parliament and the Council***~~[2] ~~***or any relevant act of Union law;***~~ (e) where the trader is registered in a trade register or similar public register, the trade register in which the trader is registered and its registration number or equivalent means of identification in that register; (f) a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law.	**Article 22** (1) Where an online platform allows consumers to conclude distance contracts with traders, it shall ensure that traders can only use its services to promote messages on or to offer products or services to consumers located in the Union if, prior to the use of its services, the online platform has obtained the following information: (a) the name, address, telephone number and electronic mail address of the trader; (b) a copy of the identification document of the trader or any other electronic identification as defined by Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council; (c) the bank account details of the trader, where the trader is a natural person; (e) where the trader is registered in a trade register or similar public register, the trade register in which the trader is registered and its registration number or equivalent means of identification in that register; (f) a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law.	• DIGITALEUROPE believes that the traceability of traders is an important tool for platforms to prevent misuse of their services, disincentivise bad actors online and provide a safe and trusted environment for their customers. Several DIGITALEUROPE members already conduct background checks on business users. • 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 such as economic operator (d), which is not related to a trader's traceability, and may not be known at the time of account creation, should not be required. In the verification of the trader's identity, platforms should be able to rely on stricter identification requirements fulfilled by payment services e.g. as required by anti-money laundering laws. Para 7 should be simplified and clarified to the end that this refers to the requirements of this article.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[2] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).

Subject	EC proposed DSA text	DIGITALEUROPE suggested amendments	Justifications
	(2) The online platform shall, upon receiving that information, make reasonable efforts to assess whether the information referred to in points (a)~~, (d)~~ and (e) of paragraph 1 is reliable through the use of any freely accessible official online database or online interface made available by a Member States or the Union or through requests to the trader to provide supporting documents ~~***from reliable sources.***~~	(2) The online platform shall, upon receiving that information, make reasonable efforts to assess whether the information referred to in points (a) and (e) of paragraph 1 is reliable through the use of any freely accessible**,** official online database or online interface made available by a Member States or the Union or through requests to the trader to provide supporting documents from reliable sources. ***The online platform may rely, for the collection or verification of information under this Article, on third parties in the meaning of Chapter II Section 4 of Directive 2015/849/EU. The third party may provide the online platform with the information required under this Article, or access thereto, notwithstanding any professional secrecy obligations the third party may be subject to.*** ***NEW (2a) To the extent the online platform has previously assessed the reliability of the trader, including in the context of its compliance with another Union or national law, it shall be deemed to comply with this paragraph and paragraph (1) of this Article.***	
	(6) The online platform shall make the information referred to in points (a), ~~***(d),***~~ (e) and (f) of paragraph 1 available to the recipients of the service, in a clear, easily accessible and comprehensible manner.	(6) The online platform shall make the information referred to in points (a), (e) and (f) of paragraph 1 available to the recipients of the service, in a clear, easily accessible and comprehensible manner.	
	(7) The online platform shall design and organise its online interface in a way that ~~***enables***~~ traders to comply with their obligations ~~***regarding pre-contractual information and product safety information***~~ under applicable ~~***Union law***~~.	(7) The online platform shall design and organise its online interface in a way that ***facilitates*** traders to comply with their obligations under ***this Article***.	
9. Definition of very large online platforms	**Article 25** (1) This Section shall apply to online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, calculated in accordance with the methodology set out in the delegated acts referred to in paragraph 3.	**Article 25** (1) This Section shall apply to online platforms which; **a)** provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, calculated in accordance with the methodology set out in the delegated acts referred to in paragraph 3 **AND** ***b) On the basis of Article 26 cannot demonstrate that there are no systemic risk stemming from the functioning and use made of their services in the Union.***	• 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.
	(4) The Digital Services Coordinator of establishment shall verify, at least every six months, whether the number of average monthly active recipients of the service in the Union of online platforms under their jurisdiction is equal to or higher than the number referred to in paragraph 1. On the basis of that verification, it shall adopt a decision designating the online platform as a very large online platform for the purposes of this Regulation, or terminating that designation, and communicate that decision, without undue delay, to the online platform concerned and to the Commission. ~~***The Commission shall ensure that the list of designated very large online platforms is published in the Official Journal of the European Union and keep that list updated. The obligations of this Section shall apply, or cease to apply, to the very large online platforms concerned from four months after that publication.***~~	(4) The Digital Services Coordinator of establishment shall verify, at least every six months, whether the number of average monthly active recipients of the service in the Union of online platforms under their jurisdiction is equal to or higher than the number referred to in paragraph 1. On the basis of that verification, it shall adopt a decision designating the online platform as a very large online platform for the purposes of this Regulation, or terminating that designation, and communicate that decision, without undue delay, to the online platform concerned and to the Commission. **NEW** ***(5) The very large online platform shall demonstrate, at least once a year, that there is no systemic risk stemming from the functioning and use made of their services in the Union referred to in paragraph 1 (b).***	

Subject	EC proposed DSA text	DIGITALEUROPE suggested amendments	Justifications
		On the basis of that, the Digital Services Coordinator shall adopt a decision designating the online platform as a very large online platform for the purposes of this Regulation, or terminating that designation, and communicate that decision, without undue delay, to the online platform concerned and to the Commission. ***NEW (6) The Commission shall ensure that the list of designated very large online platforms is published in the Official Journal of the European Union and keep that list updated. The obligations of this Section shall apply, or cease to apply, to the very large online platforms concerned from twelve months after that publication.***	
10. Risk assessments	**Article 26** (1)Very large online platforms shall identify, analyse and assess, from the date of application referred to in the second subparagraph of Article 25(4), at least once a year thereafter, any significant systemic risks stemming from the functioning and use made of their services in the Union. This risk assessment shall be specific to their services and shall include the following systemic risks: a) the dissemination of illegal content through their services; b) any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child, as enshrined in Articles 7, 11, 21 and 24 of the Charter respectively; **c)** intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security.	**Article 26** (1) Very large online platforms shall identify, analyse and assess, from the date of application referred to in the second subparagraph of Article 25(4), at least once a year thereafter, any significant systemic risks stemming from the functioning and use made of their services in the Union. This risk assessment shall be specific to their services and shall include the following systemic risks: a) ***features that facilitate*** the ***exponential*** dissemination of illegal content through their services; b) any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child, as enshrined in Articles 7, 11, 21 and 24 of the Charter respectively; c) intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security.	• It is not necessarily the size of an online platform as such or on its own that leads to systemic risk but rather the provision of specific features and how these are usedor abused by recipients of the service that can lower or increase such risks.
11. Codes of conduct	**Recital 67** The Commission and the Board should encourage the drawing-up of codes of conduct to contribute to the application of this Regulation. While the implementation of codes of conduct should be measurable and subject to public oversight, this should not impair the voluntary nature of such codes and the freedom of interested parties to decide whether to participate. In certain circumstances, it is important that very large online platforms cooperate in the drawing-up and adhere to specific codes of conduct. Nothing in this Regulation prevents other service providers from adhering to the same standards of due diligence, adopting best practices and benefitting from the guidance provided by the Commission and the Board, by participating in the same codes of conduct.	**Recital 67** The Commission and the Board should encourage the drawing-up of codes of conduct to contribute to the application of this Regulation. While the implementation of codes of conduct should be measurable and subject to public oversight, this should not impair the voluntary nature of such codes and the freedom of interested parties to decide whether to participate. In certain circumstances, it is important that very large online platforms cooperate in the drawing-up and adhere to specific codes of conduct. ***One area for potential codes of conducts could be processes to inform 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.*** Nothing in this Regulation prevents other service providers from adhering to the same standards of due diligence, adopting best practices and benefitting from the guidance provided by the Commission and the Board, by participating in the same codes of conduct.	• 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.
12. Implementation timeline	**Article 74** (1) This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. (2) It shall apply from [date - ***~~three~~*** months after its entry into force].	**Article 74** (1) This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. (2) It shall apply from [date – ***twelve to eighteen*** months after its entry into force].	• DIGITALEUROPE has concerns about the feasibility of the implementation timeline, given the steps expected. Several obligations require significant changes, in-depth legal assessment and even technical implementation work. The DSA should foresee a twelve-to-eighteen-month transition period.