Council of the European Union
General Secretariat

Interinstitutional files:
2020/0361 (COD)

Brussels, 08 October 2021

WK 11970/2021 INIT

LIMITE

COMPET	**PI**
MI	**AUDIO**
JAI	**CONSOM**
TELECOM	**CODEC**
CT	**JUSTCIV**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	ES Delegation
To:	Delegations
Subject:	Digital Services Act: Written Comments from Spain on the 2nd compromise text of the Proposal

VICEPRESIDENCIA PRIMERA

MINISTERIO DE
ASUNTOS ECONÓMICOS Y
TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

DIRECCIÓN GENERAL DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

SUBDIRECCIÓN GENERAL PARA LA SOCIEDAD DIGITAL

SPAIN - Written Comments on the 2º compromise text of the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (doc. 11459/21)

Spain presents the following comments following the 2º compromise text on the DSA proposal circulated by the Slovenian presidency.

I. Foreword: general remarks to the proposal

Spain supports the revision of Directive 2000/31/EC through a new Digital Services Act (DSA) legislative framework aimed at preserving innovation and guaranteeing a balance among all interests involved. Over the last 20 years a plethora of digital services have arisen, some of which have come to play a key role, for example, as fora for public debate. As a result, it is crucial to establish a robust liability regime, since we expect to lay the foundations of digital services regulation for the next decade.

Spain believes that the DSA should be an ambitious initiative that promotes the creation of a true Digital Single Market, with a view to facilitating innovation and effective competition for all types of operators and promoting growth and employment. Some of the principles that should be incorporated into the DSA include: provide legal certainty; a clear characterization of the economic operators and their framework of responsibilities and obligations ensuring a level playing field between "traditional" and new players; effective content moderation and user protection; a set of procedures and coordination mechanisms amongst competent authorities and intermediary services, allowing for an agile, predictable and effective supervision and protection of the general interest.

Spain welcomes that the new legal framework applicable to online intermediaries will become a global international reference and model to follow, in a way that fosters innovation and the development of the digital economy while, at the same time, the rights of users and the democratic values of our societies are respected in the moderation of illegal and potentially harmful digital content.

In the same way, Spain considers that this proposal should contribute to the creation of a true Digital Single Market, in which the plethora of innovative digital services offered in the EU, that have changed our way of relating socially and economically, are developed under conditions of legal certainty and that guarantees equal conditions for all actors, both online and offline, while protecting startups and small platforms.

It is highly appreciated the DSA horizontal approach and the respect for the basic principles of Directive 2000/31/EC, as well as the fact that the DSA does not replace or modify, but rather complements the sectoral legislation applicable as *lex specialis* to certain services, e.g. the Audiovisual Media Services Directive (AVMSD), the Directive on copyright and related rights in the digital single market (Copyright Directive), the proposed Regulation on preventing the dissemination of terrorist content online, or the Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services.

We share the need for the DSA to be broad in relation to its scope, considering its application to the set of intermediary services defined in Directive 2000/31/EC as "mere conduit", "caching" or "hosting". Thus, the DSA will apply to all digital intermediary services, including social networks, collaborative economy platforms, web hosting, cloud services, app stores or marketplaces.

Regarding the application of the regulation, the country of origin principle has been a cornerstone of the e-Commerce Directive (and other legislative acts) since it means that a digital service provider has to comply only with the national law of the country where it is established. Whereas this facilitates provision of services across the internal market, maintaining the country of origin principle requires active and strengthened cooperation among national authorities in order to avoid the fragmentation of the EU digital services market. The DSA should guarantee the effective supervision and implementation of the rules, by reinforcing cooperation mechanisms between supervisory bodies, including carrying out coordination at EU level or, even, enforcement by an EU authority.

Regarding the compromise text, Spain thanks both the Portuguese and Slovenian Presidencies for their drafting and welcomes most of the amendments in the texts. Some initial remarks:

- Spain welcomes that the DSA clarifies in a recital that orders that prevent the reappearance of illegal content previously notified (stay down orders) may be issued by competent authorities.
- We agree that some due diligence obligations must apply to all the services in an intermediary category, irrespective of their size.
- We agree with the need to reinforce cooperation between Member States, the Commission and competent authorities of destination so that the application of the Regulation is effective.
- We consider that a reinforcement of the KYBC principle and its extension to other intermediaries (beyond marketplaces) is required to better protect consumers and other rights.
- We agree that search engines must be explicitly included in the text and that VLOP obligations shall apply to very large search engines.
- We welcome the new provisions in relation to the protection of children rights online.

II. Definitions

After 20 years since Directive 2000/31/EC was enacted, the landscape of digital services has diversified into multiple categories (cloud services, social networks, marketplaces, CDNs, collaborative platforms, etc.). Therefore, definitions should be updated to clearly reflect these new digital services, the scope and criteria to distinguish intermediary services from other categories of digital services.

1. (j) 'online search engine'. We welcome the introduction of the same definition of search engine established in Regulation (EU) 2019/1150, on promoting fairness and transparency for business users of online intermediation services.

2. (i) 'dissemination to the public'. Recital 14. We support the compromise text that clarifies that messenger services that enable broad dissemination of content through public groups or channels where users are admitted without human intervention, by clicking in a link or scanning a QR code, are to be considered online platforms and could, potentially, have to comply with the due diligence obligations laid down in Section 4. Still, we are concerned about large private groups, which require a human decision (admin approval) to grant access to them but behave as a public group.

3. (ia) 'online marketplace'. We support the insertion in the compromise text of a definition of online marketplace similar to the new definition introduced by Directive (EU) 2019/2161 (Unfair Commercial Practices Directive). In order to ensure legal certainty, it was deemed necessary to clarify what a marketplace is, to differentiate it from other websites that redirect the consumer but do not allow them to conclude contracts with a trader.

4. (g) 'illegal content'. In order to clarify that local regulations are part of Member States' legislation, the sentence "or the law of a Member State" should be replaced by "or the national, regional or local law of a Member State".

   Recital 12. The offering of short-term rentals that are illegal according to national, regional or local law of member states should also fall under the concept of "illegal content", therefore we support the inclusion of "the illegal offer of accommodation services" in the compromise text as an example of illegal activity.

5. (p) 'content moderation'. We support the inclusion in the compromise text of the concept 'demonetisation', the removal of monetisation of users' content, as one of the actions that can be taken by providers to moderate content.

III. Liability of providers of intermediary services

1. Recital 20. The new wording clarifies that services whose main purpose is the facilitation of illegal activities are not neutral and, therefore, cannot benefit from the liability exemption. This is an important issue given the existence of intermediary services whose main objective and source of finance is the provision of services that facilitate illegal activities. It is essential to clarify that in no case those are neutral services and, therefore, Spain is totally in favour of the new wording.

2. Recital 22. The new wording includes a last paragraph clarifying that the automatic indexing of user-generated content, search functions and content recommendation do not directly lead to effective knowledge. This issue, not clarified in the e-Commerce Directive, has generated legal uncertainty for intermediary service providers and has given rise to a lot of litigation over the years. The aforementioned features, which could be considered to be the minimum required functionality in most current hosting services, by themselves shall not lead to the loss of the liability exemption of the provider.

   The clarification in the compromise text seems helpful, even though we would emphasize the words “automatic” and “directly” in order to avoid undesired interpretations. For instance, a platform could still be liable if an automatic algorithm recommended illegal or harmful content at large scale yielding to systemic risks. Safeguards in this regard should be taken on board.

3. Article 5 and Recital 22a. Article 5.3 includes, as a novelty in the Commission’s proposal, that the liability exemption shall not apply in marketplaces, when they present a specific item of information or otherwise enable a specific transaction in a way that would lead an average and reasonably well-informed consumer to believe that the information, or the product or service is provided either by the marketplace itself or by a recipient of the service who is acting under its authority or control.

   This provision guarantees that marketplaces do not present third-party products as their own, causing confusion in the final consumer, but the specification of some of the objective criteria and circumstances that would be relevant to elucidate when this situation occurs is missing.

   The presidency has added a new recital to clarify that when a marketplace exercises significant influence over its traders, for example, by determining the price of a product or service, traders are considered to act under the control of said marketplace and, therefore, the liability exemption will not be applicable.

   We welcome the addition, nevertheless, we would prefer to include the concept of significant influence of the marketplace over the trader in art. 5 (hosting), instead of in the recital, together with the relevant criteria to assess whether there is such a significant

influence, established by the European Law Institute (ELI) in its 'Model rules on Online Platforms':

For the assessment of whether the online platform has that control or authority or decisive influence over the trader, relevant criteria shall include:
a) the trader-consumer contract is concluded exclusively through facilities provided on the platform;
b) the online platform operator withholds the identity of the trader or contact details until after the conclusion of the trader-consumer contract;
c) the online platform operator exclusively uses payment systems which enable the platform operator to withhold payments made by the consumer to the trader;
d) the terms of the trader-consumer contract are essentially determined by the online platform operator;
e) the price to be paid by the consumer is set by the online platform operator;
f) the online platform is marketing the product or service in its own name rather than using the name of the trader who will supply it;

4. Recital 27. We share that key services for the functioning of the Internet such as domain name systems (DNS), top-level domain name registries (TLDs), or the certification authorities that issue digital certificates should enjoy the exemptions liability provided for in the DSA. However, it should be clarified in which type of intermediary (mere conduit, caching, or hosting) each one of them is inserted, in order to be able to ensure legal certainty to the providers of such services and avoid divergent interpretations. ICANN, the corporation that administers the registries for top-level domains and IP addresses, shares the same concern.

5. Recital 27a. We welcome that the text of compromise clarifies in art. 4 that search engines enjoy the same liability rules as the caching intermediaries, in order to ensure legal certainty.. This does not apply when a search engine offers a paid referencing service ('sponsored links'), which taken into account the ECJ judgment in Google France, it is considered a hosting service. Therefore, we welcome that, the last text of compromise, clarifies in recital 27a that a paid referencing service is a hosting service.

6. Live streaming platforms. For legal certainty purposes, we think there is room for clarification of the role live streaming platforms play in the DSA, at least, in the recitals.

7. Recital 28. We support the maintenance of the general prohibition of content monitoring, which already appears in article 15.1 of Directive 2000/31, and which could lead to the excessive and indiscriminate elimination of content and affect fundamental rights of users, such as the rights to freedom of expression and access to information. The foregoing is understood without prejudice to specific monitoring obligations, nor does it affect orders from the competent authorities.

The new wording in the recital clarifies that orders may require a provider to remove content identical or equivalent to that which was declared to be unlawful previously, irrespective of who generated the content, i.e. a stay-down order that prevents the reappearance of identical or equivalent content. The text is in line with the content of the CJEU ruling in the Glawischnig-Piesczek case.

It must be taken into account, in this regard, that it is very common for illegal content to be constantly replicated in hosting services and particularly in online platforms, with greater or lesser variation to circumvent the automatic tools. That is, the same illegal content will be uploaded and exposed multiple times with different URLs since the initial removal.

Spain has always been in favour of including a reference to the possibility of issuing a stay-down order based on the criteria of the CJUE ruling, given such an order would be a specific and not general monitoring obligation. Therefore, we support the new wording. However, we consider it would be better to include it in a new article in Section 2, applying to all hosting services.

8. Article 7. We propose to move the following wording from its corresponding recital (28) to art. 7 as we consider important to establish in the article that specific monitoring obligations are not prohibited.

   "This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation, in accordance with the conditions established in this Regulation."

9. Articles 8 and 9. These articles impose the obligation to intermediaries to comply with orders to act against illegal content and to provide information in accordance with national or EU law, issued by competent judicial or administrative authorities, without undue delay.

   This article is positively valued as it introduces a harmonized procedure to the process of the orders by intermediaries at European level without affecting the competent authorities in the respective areas of their competence, provided that its application must be carried out in accordance with and without prejudice to national laws, which could include prior judicial authorization in certain cases and without prejudice of sectoral legislation such as the Regulation against terrorist content online.

   The new compromise text on these articles and respective recitals goes in the right direction but there is still room for improvement. We welcome the new wording on recital 29 clarifying that the DSA harmonizes some specific minimum requirements of the orders and that it does not provide a legal basis for their issuing. Particularly, we also welcome the new wording in recital 30 on the relationship of arts. 8 and 9 with national criminal

procedural laws, clarifying that the obligation to transmit a copy of the order to other DSCs and the obligation to include a statement of reasons explaining why the information is illegal may not apply in the context of criminal proceedings and, in the same manner, that the obligation to inform the recipient of the service may be delayed particularly in the context of criminal proceedings. However, this is not enough to ensure that the DSA does not conflict with procedural regulations when obtaining national or cross-border evidence so that the confidentiality of criminal investigations is not harmed.

Therefore, we propose to add at the end of paragraph 4 of both articles 8 and 9 the following wording: "This Article shall be without prejudice to national and criminal procedural laws. ***In particular, as regards the confidentiality of criminal investigations and the rules on securing and obtaining evidence in criminal matters***".

Likewise, in subparagraph 8.2(a)(i) after "*a statement of reasons explaining why the information is illegal content, by reference to the specific provision of Union or national law infringed"* we propose to add ***"unless such a statement cannot be provided for reasons related to the prevention, investigation, detection and prosecution of criminal offences***" to better state that the statement of reasons should not be provided when there is a risk of interfering with ongoing criminal investigations. This last wording is already present in article 9.2(a)(i) for orders to provide information.

IV. Due diligence obligations applicable to all providers

1. Article 10. This provision was highly needed. It should be taken into account that, for sectoral competent authorities on content removal, the most serious problem in practice revolves around the identification of the service provider, therefore the obligation (art. 10.2) to make public the identity and form of communication with the point of contact, is essential.

   We welcome that the compromise text includes the possibility to communicate with the point of contact in a language broadly understood by the largest possible number of Union citizens apart from, at least, one of the official languages of the Member State of its main establishment.

2. Article 12. The obligation for intermediaries in the DSA to publish their "terms & conditions", which can never be exclusive or arbitrary, and of those measures, automated or not, that the service provider has chosen to use to ensure compliance is fundamental. Regarding the new compromise text, we welcome the new paragraph 1a that ensures the legal language used in the terms & conditions of a service, aimed at children or adolescents, is explained in terms they can understand. We also welcome that T&C must be published in a machine-readable format but it would also help transparency if all past versions of the T&C and the date of application of each of them are available in a searchable repository.

3. Article 13. We consider very appropriate to impose an obligation on intermediaries to publish annual transparency reports on their content moderation practices. Therefore, we welcome that in the new text, small or micro enterprises that are VLOPs must comply with the transparency reporting obligations in art. 13.1.

V. Due diligence obligations applicable to hosting providers

1. Article 14. It is important that all hosting service providers, regardless of their size, adopt harmonized notice & action mechanisms that facilitate the reporting of potentially illegal content. Therefore, we welcome the establishment of rules that harmonize in the EU the procedures for notification of illegal content and consequent action by a hosting provider (notice & action), such as file storage and sharing services, web hosting services, or ad servers.

   We consider individuals, entities and trusted flaggers should be able to use the N&A mechanism to flag incompatible content with the terms and conditions of a service, in addition to illegal content. Therefore, we propose to change all references to illegal content in the article to *"illegal content, or incompatible with the terms and conditions of the service"*. The definition and scope of harmful content deeply depends on context and culture. However we believe harmful content, or rather other content moderated by digital services and included in their community guidelines, could be on the scope of the DSA framework for limited purposes such as the application of the same harmonized notification-and-action procedure that applies to illegal content.

   We welcome that with the new wording in paragraph 14.2(b), not necessarily the URL but any other information that would reasonably allow the identification would be sufficient to identify the location of illegal content.

   We propose to remove the requirement of a name as a compulsory element of a notice in paragraph 14.2(c). We consider it should be possible to submit notifications in an anonymous manner. There are already safeguards in place to avoid the abuse of the system in article 20.

   Finally, we propose to add specific deadlines for notices to be decided upon by providers in paragraph 14(6). All notices shall be decided within a fixed deadline and in case of manifestly illegal content within 24 hours. However, small and micro providers shall be exempted from the 24 hour time limit, so as not to burden them disproportionately.

2. Article 15. We support that the compromise text includes the restriction of visibility or monetisation of content among those decisions taken by hosting services that require the provision of a statement of reasons to the recipient of the service.

3. Article 15a and recital 48. Notification of suspicions of criminal offences. We consider the reporting obligation should not be limited to serious crimes that threaten the life or safety of

persons, but need to be expanded to include other serious crimes. Therefore the sentence "*involving a threat to the life or safety of persons has taken place*" should be removed. Furthermore, recital 48 should list, non-exhaustively, other serious criminal offenses, such as serious forms of racism and xenophobia specified in Council Framework Decision 2008/913/JHA.

We welcome that, in the compromise text, article 15a applies to all hosting providers as these services are often used to distribute illegal content through links open to anyone.

We also welcome that the article now applies to every provider, regardless of its size, including small and micro enterprises. We consider the obligation to report serious crimes is not particularly burdensome. In addition, the obligation only covers the communication of information providers are aware of, not a general supervision or active search for criminal offences, something that the DSA specifically excludes in art. 7.

4. **Dark Patterns.** We believe that the DSA should require that, in the design of online interfaces of hosting providers, **dark patterns are not used to prevent users from exercising their rights, such as deleting an account** (this is already de direction in the industry[1]). Therefore, we propose a new article and corresponding recital:

> *Recital 39a) Providers of hosting services shall ensure that the design and organisation of their online interfaces do not use "dark patterns" to trick the recipients of their service into making choices they don't mean to do, such as choosing a less privacy-oriented setup or providing unnecessary personal data, or make it difficult to access certain functionalities of the platform, such as closing a service account, by requiring too many steps to access it or hiding the functionality.*
>
> *Article 15b Design of online interfaces*
>
> *Providers of hosting services shall ensure that the design and organisation of their online interfaces do not trick the recipients of their service into making choices they do not mean to make or hinder the access to certain functionalities of the platform, undermining the free choice of the recipients.*

VI. Due diligence obligations applicable to online platforms

1. Article 16. Proportionality should be a key principle in order to limit the burdens for startups and SMEs to compete in markets where content moderation rules apply. The principle of proportionality must be taken into account regarding duty of care obligations, timeframes and sanctions for rule infringements. It is positively valued that micro and small companies have fewer obligations, when they still have a small audience and the risks are lower, which allows them to grow. However, criteria to define which obligations apply should not only be based on the size or turnover of the company, but on the risks to society and the reach of the service

[1] https://developer.apple.com/news/?id=mdkbobfo

as well.. Therefore, we welcome the decision to apply due diligence obligations in section 3 (online platforms) to small and microenterprises that are VLOPs according to article 25. It is likely that small enterprises with <50 employees or turnover <10M€ have a large number of users in the EU and, consequently, they should be complying with all due diligence obligations that apply to platforms.

2. Article 17. Internal and independent dispute mechanisms and procedures should be established for users to appeal when their content or account is demoted, demonetized, suspended or removed. This mechanism shall be carefully designed to preserve users' rights to freedom of expression and access to information, as well as to conduct economic activities. We consider internal complaint-handling systems should apply to all providers of hosting services so that users of e.g. file hosting services, also have a right to redress in case its content is removed or its account suspender or terminated.

   On the other hand, we welcome that in the compromise text, both for art. 17 (internal complaint-handling system) and 18 (OOC dispute settlement), an individual or entity that has submitted a notice can also contest provider's decisions to maintain the content online (not to act upon the receipt of a notice) as well as decisions to demonetize its content or restrict its visibility.

3. Article 18. We welcome the new text that establishes that fees charged by OOC settlement bodies must be accessible, attractive and inexpensive for customers and, in the same fashion, that fees paid by platforms to the OOC body may be reimbursed by recipients that acted in manifestly bad faith. We also support the right of online platforms to refuse to engage in dispute settlement when the same dispute has been resolved or is being reviewed by another body. Likewise, we support the new paragraph 2a that establishes that an authorisation awarded to an OOC dispute settlement body shall be valid in all Member States.

4. Article 19. Trusted Flaggers. We regret that in the last compromise text the trusted flaggers provision applies only to online platforms, and not to all hosting services, as these services are also used to distribute illegal content through links open to anyone.

   We think it should be considered if trusted flaggers should be able to notify content that is incompatible with the T&C of a service through the notice and action mechanism foreseen in Article 14.

   We also consider trusted flaggers shall be awarded their status by Digital Services Coordinators of the Member State, unless the Member State has assigned certain specific functions or subjects (e.g. hate speech) to other competent authorities. Therefore, we propose the following wording for paragraph 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, <u>unless the Member State has assigned that function for some kind of illegal content to other competent authorities</u>, where the applicant has demonstrated to meet all of the following conditions:"

Regarding the requirement of independence from a platform in paragraph 2(b), we support that online hosting providers may directly or indirectly support their work through advertising credit or other alternatives. This remuneration may never constitute the main source of financing for trusted flaggers to be compatible with the independence requirement. Therefore, we propose the following wording in recital 46:

"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 are independent from any provider and that they work in a diligent and objective manner. Online hosting providers may directly or indirectly support their work through advertising credit or other alternatives. This remuneration may never constitute the main source of financing for trusted flaggers to be compatible with the independence requirement."

Finally, we support the new wording stating that industry associations representing members' interests should apply for the status of trusted flaggers awarded by DSC, instead of private parties that could otherwise enter into bilateral agreements with platforms.

5. Article 20. We agree that the measures that a platform may apply to protect against misuse of its services should be proportionate to the severity of the infringements and can include the demotion or demonetization of content, apart from the suspension of the account as provided by the new text.

   We also welcome that recital 47 clarifies that the prior warning, sent to the user before deciding the suspension of the provision of the service, includes a statement of reasons and the means of redress against the decision. This will help to better safeguard the right to freedom of expression of the users.

   We wonder if, in cases of frequently provided manifestly illegal content, the termination of the account should not be considered. In that case, providers should establish mechanisms to prevent re-registration by suspended or terminated individuals or entities.

6. Article 24. We welcome the new transparency obligations in online advertising, in addition to those already established by Article 6 of Directive 2000/31. Regarding the compromise text, we support that the information about advertising shall be accessible directly from the advertisement in order to facilitate the access. We also value positively that platforms are required to build a functionality for recipients of the service to declare whether a piece of content provided by them contains commercial communications.

VII. Due diligence obligations applicable to marketplaces

1. Article 24a and Recital 49. The rise of online marketplaces has had clear benefits both for consumers that have a bigger range of product at their disposal and for SMEs that have a wider reach for their inventory. However, marketplaces have also brought with them an

easy medium for nefarious sellers to bring dangerous or counterfeit products or illegal services to the masses. In order to increase safety in commercial traffic carried out in marketplaces, the obligation known as "Know-Your-Business-Customer" (KYBC) is considered very appropriate. This principle forces marketplaces to identify merchants who sell products on their platform, which will allow them to fight against those merchants who sell products non-compliant with consumer protection regulation or counterfeited.

However, the same traceability rules (KYBC principle) should also apply to web hosting, CDN, DNS registries and registrars, payment and advertising services. These rules would facilitate the fight against unlawful activities in those services, given that only recipients who identify themselves adequately will be able to use them. There are organizations that make use those intermediation services, responsible for the massive dissemination of hate speech, violation of rights of intellectual property, alteration of public order, among others.

Besides, to allow local competent authorities to ensure compliance with short-term rental regulations, including when accommodation is offered by individuals and not by traders, this article should apply to all recipients of short-term rental marketplaces, both natural and legal persons. All recipients, individuals and traders, should provide its name, address, telephone, email and registration number issued by local, regional or national authorities. Traders should also provide the rest of the information required in the article.

On the other hand, we welcome that in the new wording, marketplaces shall make some of the information available in the product listing but regret that the word "best" has been replaced with "reasonable" efforts to assess whether the information of the trader is reliable prior to the use of their services. Best efforts should be made to verify the reliability of the information provided by merchants before their inclusion in the marketplace.

2. Article 24b. We support the new article on compliance by design that provides that online marketplaces must build an online interface that enable traders to comply with their information obligations set out by the DSA and the regulations on product safety. We also should underscore that online marketplaces should make best (not reasonable) efforts to assess that the traders have uploaded the mandatory information on the online interface fields. We consider online marketplaces should also ensure that offers can only be uploaded if the design interface has been completed for the legally required information (by setting mandatory fields). It goes without saying that the platform will not be responsible for the content, only it should assess whether or not the information in the mandatory fields is complete.

3. Article 24c. We support the new article on right to information that establishes that online marketplaces shall inform consumers that had acquired illegal product or services about the specific illegality, the identity of the trader and the means of redress.

VIII. Due diligence obligations applicable to VLOPs

1. Article 25 and recital 54. The concept of monthly active recipient may vary greatly depending on the definition. Therefore, we welcome the clarifications made in the recital regarding the notion of active recipient, although it may be later refined by the Commission in a delegated act. In particular, we welcome that it does not coincide with the notion of a registered user and, most importantly, that the number of recipients cumulatively covers the content creators and those that interact with the content.

2. Article 25a. We agree that VLOPs shall determine whether or not a notice submitted by a trusted flagger is of a manifestly illegal content in a maximum timeframe given their wide reach and taking into account that they have the resources to do so. 24 hours seems a reasonable timeframe for the assessment.

   However, we need to make sure that this time limit is not discouraging VLOPs from acting quickly as there is a risk that they will make use of the maximum time allowed instead. This will contradict the current *statu quo*, where many platforms remove content much faster than 24 hours after receiving a notice. Furthermore, **removal within 24 hours would not be sufficient to mitigate the damage caused when intellectual property rights are at stake, e.g. the illegal live streaming of a football match, where an immediate removal action is absolutely required to prevent grave damages to rights holders**. Therefore, we propose the following wording for article 25a:

   "*Providers of very large online platforms shall ensure that they have the means available to determine whether notices referred to in Article 19 relate to manifestly illegal content* ***immediately and without delay,*** *and in any case within a period* ***not exceeding 24 hours*** *on average of the receipt of the notice".*

   Likewise, we propose some changes to recital 55a:

   (55a) In view of the risks posed by the significant reach of very large online platforms, as well as the resources that are typically available to the providers of such platforms, it is desirable and reasonable to expect that very large online platforms have the necessary means, including appropriate human and material resources, as well as procedures, to operate notice and action mechanisms that allow assessing whether notices submitted by trusted flaggers relate to manifestly illegal content without delay and in any case within a period not exceeding 24 hours on average. The expected average time period for the assessing of notices will depend on the context, including the type of illegal content, the details provided by the notifier, the severity of the offence and the damage caused by the availability of the content. ***In particular, the needs of immediacy in the removal of content for the protection of intellectual property rights should be respected.***

3. Article 26. Due to their social and economic impact, and their business model frequently based on advertising, large platforms should carry out annual assessments on three categories of systemic risks: dissemination of illegal content, negative effects on

fundamental rights such as freedom of expression and information, and manipulation against public health, minors, electoral processes or public safety. However:

- Negative effects should also take into account other fundamental rights of the Charter of Fundamental Rights, such as equality between women and men. Therefore we propose the following wording:

  "b) any negative effects for the exercise of the fundamental rights, in particular but not limited 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;"

- Disinformation and misinformation should be included explicitly as systemic risks for assessment. We propose the following wording:

  "c) intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, and dissemination of disinformation or misinformation with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse fundamental rights, or actual or foreseeable effects related to electoral processes and public security."

4. Article 27. We welcome that in order to mitigate systems risks pose by their services, **VLOPs should take, among others, measures to protect children's rights, including age verification, parental control and tools to help minor signal abuse or obtain support of the platform**. The access of minors to lawful for the general public but potentially harmful content for them is already considered in sectoral regulations in relation to the online environment. In this regard, vertical legislation, such as the Audiovisual Media Directive (AVSMD) in its article 28 ter, already provides for the mandatory adoption of mechanisms for verifying the age of users who access video sharing platforms. However, the scope of the Directive is limited to providers established in the European Union. Therefore, the introduction of a provision that regulates conditional access to non-illegal but harmful information for children, such as pornography, through parental control and age verification tools is needed to guarantee that minors do not access this type of content.

5. Article 28. The obligation for VLOPs to carry out an annual independent audit is positively valued. However, it should also be carried out when it is appreciated that the risks have increased considerably due to circumstances or factors that have occurred recently.. Therefore we propose to modify paragraph 1 as follows:

   "Providers of very large online platforms shall be subject, at their own expense and at least once a year or when it is appreciated that the risks have increased considerably by arising circumstances, to audits to assess compliance with the following:"

6. Article 29. Recommendation systems play an important role in the dissemination and amplification information. Consequently, it is positively valued that users can change the parameters in the recommendation systems in VLOPs and in particular that they can receive recommendations not based on profiling.

   However, in order to combat misinformation, large platforms should be encouraged to prioritize relevant and reliable content obtained from authorized sources through transparent procedures. Information that comes from unreliable sources should be treated with lower priority by recommendation algorithms, and even labelled, in such a way as to offer users different points of view and contribute to their education and training in respect, plurality and the diversity of opinions.

   Additionally, recommendation systems and "positive" labeling should be considered and promoted, that is, the labelling by trusted flaggers of content that is verified or that is labelled as of a certain quality by private recommenders, in such a way that users can also freely choose to follow the contents indicated and recommended by these trusted flaggers. It would be a system equivalent to the rating of movies by age, but generalized and open to all types of users of the platform or trusted flaggers.

   On the other hand, Spain welcomes the new obligation for VLOPs to show the parameters and options on recommender systems on a specific section of the online interface where the content is being recommended. This is an important issue given that, frequently, settings are available but out of reach for the average user. However, we consider this obligation should be extended to all online platforms. Besides, we believe users will become more empowered if they are prompted, on the first use of the service, to choose if they want to get recommendations based on profiling, in reverse chronological order or based on other type of parameters.

7. Article 30. The compilation and annual publication in a repository of detailed information on advertising is positively valued. It should be taken into account that online advertising revenue constitutes the bulk of the business model of large platforms, whose intention is to keep users active for as long as possible by maximizing interactions, which encourages the appearance of harmful content such as misinformation. Thanks to this provision, the supervision and investigation of risks in relation to online advertising will be facilitated, especially when it is personalized, in relation to disinformation or other manipulative techniques that may have an impact on public health, public safety or political participation.

   However, we also propose to include the information on the amount spent on an advertisement as part of the information to be stored in the repository. VLOPs should also provide a repository interface that allows to make multi-criterion queries per advertiser based on the information stored on the repository. Also, the data should be stored for five years after the advertisement was displayed for the last time, instead of one, for researchers to have enough time to perform their investigations.

8. Article 31. The data access obligation imposed on VLOPs to vetted researchers, for the purpose of conducting research that contributes to the identification and understanding of systemic risks, is positively valued. Regarding the revised provisions in the new compromise text, we very welcome that the article clearly establishes the procedure and conditions to be awarded the status of vetted researcher and for the termination of the status, in case the researcher no longer meet the conditions. Likewise, we agree that the researchers shall make their research freely and publicly available upon its completion.

   However, certain civil society organizations and journalists should be able to qualify as vetted researchers to access relevant data from VLOPs given the importance of the research they also carry out. This access should always take place in compliance with Regulation (EU) 2016/679, taking into account the rights and interests of the VLOPs and the recipients of the service concerned, including the protection of confidential information, in particular trade secrets, and maintaining the security of their service.

9. Article 32. We agree with the new provisions in the compromise text that brings the figure of the compliance officer closer to that of the banking sector. We believe there is a need to step up the role of the compliance officer to ensure its independence, for example, by reporting directly to the management board.

10. Article 33. We agree that VLOPs should be transparent about the number of human resources in charge of moderating content, but it must be clear that they must specify the linguistic expertise of the staff, specifying the number of staff by language of expertise.

11. Article 33.a. We welcome that the same obligations in section IV that apply to very large online platforms apply to very large online search engines as well, due to the systemic risks they pose by enabling broad access to harmful content in their results. We also agree that other obligations that apply to hosting services and online platforms in Section 2 and 3 of Chapter III will not be applicable to the nature of search engines as the indexed webpages are not recipients of the search service.

IX. Competent authorities and DSCs

1. Article 39 and recital 74. The requirement of independence of the Digital Service Coordinator from the government should be further analysed as it might interfere with internal administrative structures of Member States.

2. Article 41. According to art. 11, providers of intermediary services which do not have an establishment in the Union but which offer services in the Union must designate a legal representative in the UE. However, if they do not designate a legal representative, DSCs are helpless. Therefore, DSCs should have the power to adopt interim measures in case the intermediary service provider repeatedly infringes the obligations set in the DSA. In particular, the power to request judicial authorities to order the restriction of access to the online interface.

3. Article 45. We support the new compromise text that states that 3 DSC of destination may request the Board to recommend the DSC of establishment to evaluate the suspicion of an infringement and take measures to ensure compliance with the DSA. However, we consider that the Board must be able to request (not recommend) the DSC of establishment to assess the matter and take the necessary measures. Therefore we propose to replace "may recommend" with "shall request" and delete all references to "recommendation" in the article.

4. Article 46. We support that the requirements and procedure for joint investigations have been further specified in the compromise text.

5. Article 46a. We welcome that supports that the requirements and procedure for joint investigations of infringements of VLOPS/VLOSES have been further specified. In particular, that three DSC of destination are able to trigger the Board to recommend the COM to launch a joint investigation in case a VLOP/VLOSE is suspected to infringe the DSA.

   We also welcome that, in the compromise text, competent authorities of the Member State in whose territory the intermediary service is established can participate in the joint investigations.

6. Article 46b. We support the new compromise text that allow three DSC of destination to request the Board to recommend the COM to intervene directly, in the case of serious harm to a large number of recipients, without the prior set up of a joint investigation.

X. Supervision of VLOPs

1. Article 50. We welcome that, in the compromise text, the Commission may open proceedings with a view to establish an infringement of the provision in Section 4 Chapter III by a VLOP/VLOSE, as soon as the DSC of establishment does not adopt a decision in the timeframe recommended by the Commission. However, we would prefer the Commission to be able to take action as soon as it has reasons to suspect an alleged infringement.

   Likewise, we welcome that the time period to adopt a decision to investigate a suspected infringement, by the DSC of establishment, is predefined in the recommendation of the Commission,

2. Article 54. We welcome that competent national authorities of the Member State in whose territory the inspections is to be conducted may be able to participate in on-site inspections.

3. Article 57. We welcome the new text in paragraph 2 that states that monitoring actions can include independent experts and auditors from competent national authorities.