Pan Michał Pukaluk
Dyrektor
Departamentu Polityki Cyfrowej
Kancelaria Prezesa Rady Ministrów

Szanowny Panie Dyrektorze,

W odpowiedzi na zaproszenie do składania uwag do treści Rozdziału 3 projektu Rozporządzenia Parlamentu Europejskiego i Rady z dnia 15 grudnia 2020 r. w sprawie jednolitego rynku usług cyfrowych „Digital Services Act", poniżej przedstawiamy uwagi IAB Polska. Część uwag została Państwu przekazana w ramach stanowiska uzupełniającego przy piśmie z dn. 19 lutego br., zaś pozostała stanowi uzupełnienie i rozszerzenie dotychczas zgłaszanych postulatów, które prezentujemy zarówno w formie konkretnych propozycji zmian w przepisach jak i dodatkowych pytań i komentarzy.

Article 10
Points of contact

1. Providers of intermediary services shall establish a single point of contact allowing for direct communication, by electronic means, with Member States' authorities, the Commission and the Board referred to in Article 47 for the application of this Regulation.
2. Providers of intermediary services shall make public the information necessary to easily identify and communicate with their single points of contact, **and ensure that that information is up to date. Providers of intermediary services shall notify that information, including the name, address, the electronic mail address and telephone number, of their single point of contact, to the Digital Service Coordinator in the Member State where they are established. The Digital Services Coordinator shall verify the above mentioned information.**
3. Providers of intermediary services shall specify in the information referred to in paragraph 2, the official language or languages of the Union, which can be used to communicate with their points of contact and which shall include at least one of the official languages of the Member State in which the provider of intermediary services has its main establishment or where its legal representative resides or is established.

EXPLANATION:

Adding to Article 11 paragraph 4 the obligation of the providers of intermediary services to notify the data regarding the single point of contact to the Digital Services Coordinators, and the Coordinator's obligations to verify such data, ensures that only factually existing entities are appointed to perform this function and that the possibility of communication through such single point of contact is real.

Article 11
Legal representatives

1. Providers of intermediary services which do not have an establishment in the Union but which offer services in the Union shall designate, in writing, a legal or natural person as their legal representative in one of the Member States where the provider offers its services.

2. Providers of intermediary services shall mandate their legal representatives to be addressed in addition to or instead of the provider by the Member States' authorities, the Commission and the Board on all issues necessary for the receipt of, compliance with and enforcement of decisions issued in relation to this Regulation. Providers of intermediary services shall provide their legal representative with the necessary powers and resource to cooperate with the Member States' authorities, the Commission and the Board and comply with those decisions.

3. The designated legal representative can be held liable for non-compliance with obligations under this Regulation, without prejudice to the liability and legal actions that could be initiated against the provider of intermediary services.

4. Providers of intermediary services shall notify **valid identification data, including** the name, address, the electronic mail address and telephone number of their legal representative to the Digital Service Coordinator in the Member State where that legal representative resides or is established. They shall ensure that that information is up to date. **The Digital Services Coordinator shall verify the above mentioned data.**

5. The designation of a legal representative within the Union pursuant to paragraph 1 shall not amount to an establishment in the Union.

EXPLANATION:

Adding to Article 11 paragraph 4 the obligation of the Digital Services Coordinators to verify the data of the legal representatives ensures that only factually existing entities are designated to perform this function in order to be held liable, if necessary, for the compliance with the Regulation by the providers of intermediary services which do not have an establishment in the Union but which offer services in the Union.

Articles 13, 23 and 33
Transparency reporting obligations

The transparency reporting obligations imposed on intermediaries are extremely broad. We urge policymakers to carefully consider the objective that each requirement seeks to achieve and define its scope in a proportionate manner, taking due account of what level of transparency is meaningful for users and feasible for intermediaries. For example:

- Article 13: Providing information on any content moderation intermediaries engage in (under Article 13) is likely to (i) result in information overload that is difficult to make sense of, (ii) provide a roadmap for bad-faith actors to game content moderation systems, and (iii) involve a significant amount of engineering

effort and associated costs potentially crippling SMEs. We are particularly concerned about the breadth of Article 13(1)(c) and urge, at a minimum, to have Article 13(1)(c) limited to content that is removed or disabled by the intermediary. We are also concerned about the requirement in Article 13(1)(d) to report average turnaround time, which may be an ineffective metric and could encourage platforms to make hasty decisions rather than work expeditiously but carefully.

- Article 33: It is not clear why users would need to have access to risk assessment reports, risk mitigation measures, audit reports or audit implementation reports under Article 33(2). Obliging very large online platforms to engage in a confidential information redaction process prior to annual public disclosures would be disproportionate, given the level of detail included in those reports is unlikely to be of interest to the average user. In addition, making information on risk exposure and existing vulnerabilities public has the potential to be exploited by nefarious actors. These reports should rather be made accessible to regulators only as a means to ensure accountability of very large online platforms.

Rec. (40)

Providers of hosting services play a particularly important role in tackling illegal content online, as they store information provided by and at the request of the recipients of the service and typically give other recipients access thereto, sometimes on a large scale. It is important that all providers of hosting services, regardless of their size, put in place user-friendly notice and action mechanisms that facilitate the notification of specific items of information that the notifying party considers to be illegal content to the provider of hosting services concerned ('notice'), pursuant to which that provider can decide whether or not it agrees with that assessment and wishes to remove or disable access to that content ('action'). Provided the requirements on notices are met, it should be possible for individuals or entities to notify multiple specific items of allegedly illegal content through a single notice. *Electronic location of information may be submitted in the notification, for instance:*

a) by providing exact URL or URLs of single file, product, information or concrete illegal content, or

b) by providing exact URL or URLs of the website(s) directory or domain name where such directory (ies) or domains contain only the content that is the subject of the notice, or

c) a website(s) directory or domain with a detailed indication of the content in question in cases where such directories or domains contain the content and other content submitted; and the individual identification of uniform resource locators for that content is not possible and, if necessary and appropriate, additional information enabling the identification of illegal content. The means of identifying the electronic location of illegal content should be appropriate to the type of that content and bear in mind that it should be possible to notify multiple specific items of illegal content with a single notification.

The obligation to put in place notice and action mechanisms should apply, for instance, to file storage and sharing services, web hosting services, advertising servers and paste bins, in as far as they qualify as providers of hosting services covered by this Regulation.

Article 14
Notice and action mechanisms

1. Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means.

2. The mechanisms referred to in paragraph 1 shall be such as to facilitate the submission of sufficiently precise and adequately substantiated notices, on the basis of which a diligent economic operator can identify the illegality of the content in question. To that end, the providers shall take the necessary measures to enable and facilitate the submission of notices containing all of the following elements:

   (a) an explanation of the reasons why the individual or entity considers the information in question to be illegal content;

   (b) a clear indication of the electronic location of that information~~, in particular the exact URL or URLs,~~ and, where necessary **and applicable**, additional information enabling the identification of the illegal content **which shall be appropriate to the type of content and to the specific type of intermediary**;

   (c) the name and an electronic mail address of the individual or entity submitting the notice, except in the case of information considered to involve one of the offences referred to in Articles 3 to 7 of Directive 2011/93/EU;

   (d) a statement confirming the good faith belief of the individual or entity submitting the notice that the information and allegations contained therein are accurate and complete.

EXPLANATION:

The notice enabling the platform to identify the illegal content should be appropriate to the type of content and include technology factors. It should also be applicable to the type of intermediary that is supposed to remove the content. **The technical means of identifying illegal content and its location should be futureproof, bearing in mind possible new developments and innovations in this field. A "one size fits all approach" is not recommended, as it will not enable effective removal of illegal content.** Providing the specific URL should be treated as one of the means, but not an obligatory means, of indicating the electronic location or correct identification of the content. The text proposed by the Commission may practically be interpreted as imposing an obligation to indicate the exact URL of each illegal content item in the case of court orders (art.8) and notice mechanisms (art.14). However in cases where a host provider catalogues illegal content, it should be possible to provide the URL to the folder, in case the folder contains only illegal content or in case the vast majority of the content in folder is illegal and indicating the exact URL to every illegal content is not feasible, instead of indicating hundreds of URLs (links) in this folder. In case a website hosts only illegal content, it should be possible to indicate just its domain address (i.e. main URL), without the need to select and indicate hundreds of links for each item of illegal content. This problem has already been identified in the US Copyright Office report of May 2020, Section 512 of Title 17 - regarding the Digital Millennium Copyright Act (https://www.copyright.gov/policy/section512/section-512-full-report.pdf) where the report conclusions state: "The Office concludes that Congress may wish to consider whether the "information reasonably sufficient . . . to locate" provision is

appropriately interpreted as requiring that a rightsholder must submit a unique, file-specific URL for every instance of infringing material on an OSP's service."

Article 14(6) should not require extensive disclosure of details around the automated means used to process or reach a decision on the notice, as this could allow bad-faith actors to reverse-engineer our tools and potentially avoid manual review.

Article 17
Internal complaint-handling system

We consider that providing an internal complaint-handling system for 6 months following the content moderation decision is disproportionate and undermines legal certainty and fundamental rights. For example, a rightsholder would have to wait for 6 months in uncertainty to confirm whether a decision to remove IP infringing content is final or may be appealed by the uploader.

Article 17(5)) - Limits on automation in complaint-handling

The text is too rigid in requiring that no decision on appeal should be taken solely on the basis of automated means.

- This is not reasonable given the scale at which content moderation takes place. Platforms routinely use automation to handle the billions of spam or bad ads content, and want to ensure that the DSA does not risk their ability to handle scaled abuse.
- A more appropriate outcome would be a risk-based approach to appeals, using a combination of human review and automation: for more egregious and nuanced cases online platforms may indeed need to more heavily rely on expert human review.

Article 18
Out-of-court dispute settlement

We understand the importance of users having the ability to appeal content decisions, However, we are concerned about several potential unintended consequences that the DSA provision on out-of-court mechanisms may have:

- Enabling bad actors: Article 18 opens up avenues for abuse and does not scale to the millions of decisions online platforms make. Bad actors could use alternative dispute resolution (ADR) to arbitrate every content removal at a company's expense. They could slow down the process for legitimate seekers of redress. Surely this is not meeting the intent of meaningful user redress.
- National authorities' removal orders: Under the current DSA text, content uploaders may arguably also challenge services' removals made pursuant to national authorities' removal orders (under Article 8), including where those orders may be confidential and appear as the online platforms' own decision. We question whether this was intended. If not, it underscores the implications of ADR provisions that have not been fully thought-through.
- Fragmentation and confusion: The use of ADR by content uploaders to review any content moderation decision is highly likely to result in contradicting decisions by different ADR bodies in different Member States as regards the same issues or policies. Given the scale of content moderation online platforms engage in, trying to make sense

of a patchwork of often contrasting decisions by different bodies across the EU risks paralysing online platforms' content moderation systems.
    - This may incentivize services to make their policies more generic or vague to avoid claims in ADR that they acted inconsistently.

We would also flag that, despite the language included under Article 21(2), Europol does not currently have the authority to take personal data from private parties.

Article 22
Traceability of traders

In addition, we recommend clarifying that the trader should provide all the information required under Article 22 to the online platform (including in particular the information under Article 22(1)(d), given it would be impossible for the online platform to chase information about economic operators down the value chain), and that the online platform should not be held liable for information provided by the trader that ends up being inaccurate.

Article 24
Online advertising transparency

We support giving users greater transparency around ads, but the DSA must set reasonable limits and ensure it doesn't lead to overly-burdensome requirements or disclosure of commercially sensitive information. We indicate that setting the transparency requirements only to online platform can confuse users since for same ad users will not always be provided with meaningful information about the main parameters used to determine the recipient to whom the advertisement was displayed.

Article 27
Mitigation of risks

We are concerned the DSA would lead to regulation via the backdoor of illegal and lawful but harmful content alike. The DSA should neither allow regulators to define risks for businesses (Article 26), nor impose risk mitigation solutions on them (Recitals 59, 68; Article 35).

- Regulators have wide powers to issue rules on illegal and lawful content -- such as content that may have a "negative effect on…civic discourse" -- through Codes of Conduct that are mandatory in practice for VLOPs.
- This has serious implications for fundamental rights, and goes against the Commission's stated intention to protect lawful content. In the DSA's Explanatory Memorandum, the Commission notes that lawful-but-harmful content "should not be subject to removal obligations, as this is a delicate area with severe implications for the protection of freedom of expression," but these provisions risk exactly that result. They could also harm innovation and harm the fundamental right to conduct a business.
- The DSA should remove these provisions that would lead to regulation of lawful conduct through the backdoor, and not through EU democratic processes.

Article 28
Independent audit

We recognise the importance of verifying the risk assessments and risk mitigation measures of VLOPs by independent experts. An audit regime under the DSA should support robust analysis by auditors and provide meaningful insights to oversight bodies into how VLOPs are seeking to comply with DSA obligations. We are however concerned about the ability of the audit regime as currently proposed to achieve these aims. We would therefore make the following suggestions on:

(A) Supporting areas of specific focus in routine audits (Article 28(1)): To support the usefulness of the findings of the independent auditors, especially given the large scope proposed in Article 28(1), the DSA should provide mechanisms to facilitate areas of more specific focus in a given auditing period. For example, this could include Digital Services Coordinators providing an annual plan that identifies to VLOPs and their auditors key areas of interest for the upcoming reporting period.

(B) The frequency and scope of routine audits (Article 28(1)):

- To allow sufficient time for auditing activities, the frequency of routine audits under Article 28(1) should be at least every two years.
- We have underlined the voluntary nature of Codes of Conduct and we have also recommended that Crisis Protocols should not be mandatory. On this basis, we also recommend excluding these frameworks from the scope of audits under Article 28(1). We would instead suggest that reporting and verification processes be tailored to each of the Codes of Conduct and Crisis Protocols.
- We understand that in certain circumstances it will be beneficial to have the remediation plans of VLOPs independently audited (Article 50(3)). Where this does occur, and the relevant assessments and measures taken by VLOPs are deemed adequate, we would suggest that these aspects are excluded from the scope of the next routine audit under Article 28(1).

The timeframe for action plans:
A period of one month is insufficient to develop an audit implementation report (Article 28(4)) or remediation plan (Article 50(2)). We would suggest that the DSA adopt an objectives-based approach, where remediation timelines are based on the scope, severity and complexity of the auditor's recommendations or the decision of a DSC of establishment. We would recommend a mechanism whereby VLOPs would have a minimum of 45 days to acknowledge the recommendations, scope the work and communicate timeline for an action plan. Such an approach would support proportionate process rules, linking the response time on the scope, severity and complexity of the recommendations.

Adopting a risk-based approach to audit findings (Article 28(3))
To support the development of action plans and remediation, we would propose adopting a risk-based approach to audit findings. For example, rather than 'positive, positive with comments, or negative' assessments (as is currently proposed in Article 28(3), the risk-based tiers could be:

- No/limited control gaps/findings, with observations
- Medium control gaps/findings - 12 month remediation timeline
- High control gaps/findings - 6 month remediation timeline
- Critical control gaps/findings - 3 month remediation timeline

Article 29
Recommender systems

We support efforts to give users more information and control around recommender systems, so long as any requirements are flexible, so that they can be tailored to the particular service and protect against bad actors gaming the platform's systems.

- We want to ensure users are "appropriately informed" (Recital 62), while also ensuring that platforms can protect commercially sensitive information. Overly-broad disclosures of "the main parameters used" could enable bad actors to game the platform's systems.
- The way this provision is currently drafted, it could undermine the very essence of many innovative services. Think for example of a service the value of which lies exclusively in offering personalised content to users (e.g. an app that offers a user a list of news content that is likely to interest her/him based on explicitly stated interests the user indicates when installing the app). Users opt for those services precisely because of the personalised experience they offer.

Article 30
Additional online advertising transparency

There are many open questions undermining legal certainty for online platforms. For example: (1) Would ads disapproved because they contained illegal content need to be included in the repository and continue being shown to users? (2) Would length from last data served apply to all ads? What about disapproved ads? (3) Would all ads need to be included in the repository, including ads reaching a low impressions threshold? These are important issues that should be clarified in a manner that strikes a careful balance between (i) meaningful transparency being provided to users, and (ii) proportionate obligations being imposed on online platforms in light of the objective Article 30 seeks to achieve.

Limiting the transparency requirements to those listed in Article 30(2)(a)-(b) would strike this balance. Publicly disclosing the information under Article 30(2)(c)-(e) would not only be burdensome for online platforms; but more importantly it could lead to disclosure of sensitive information of the advertiser, arguably without serving meaningful transparency for the average user.

Article 31
Data access and scrutiny

We recognise that researchers need to be able to access data to scrutinise or investigate issues of societal concern. We are concerned that, as Article 31 is currently drafted, there are virtually no safeguards around what data may be requested, how such data may be accessed, and what may be done with the data. We suggest including safeguards along the following lines:

- Define "reasoned request" to set parameters around what information can be requested and shared with vetted researchers, in line with the GDPR data minimisation principle.
- Allow online platforms to take additional measures to protect the privacy of data subjects (e.g. through pseudonymization), where appropriate.
- Set limits on what can be done with the data and clarify that the data should not be further shared/disclosed, in line with the GDPR purpose-limitation principle.

We also urge policymakers to require transparency on any funding researchers receive as part of their vetting process. "Commercial interests" might not cover researchers who, for example, have major academic projects funded by competitors or critics of the very large online platform

at issue. For the same reason, we ask for a possibility for very large online platforms to appeal the vetting of a particular researcher.

Article 33
Transparency reporting obligations for very large online platforms

Publication of risk assessments:
It is not clear why users would need to have access to risk assessment reports, risk mitigation measures, audit reports or audit implementation reports under Article 33(2). Obliging very large online platforms to engage in a confidential information redaction process prior to annual public disclosures would be disproportionate, given the level of detail included in those reports is unlikely to be of interest to the average user. In addition, making information on risk exposure and existing vulnerabilities public has the potential to be exploited by nefarious actors. These reports should rather be made accessible to regulators only as a means to ensure accountability of very large online platforms.

Article 41
Powers of Digital Services Coordinators

3. Where needed for carrying out their tasks, Digital Services Coordinators shall also have, in respect of providers of intermediary services under the jurisdiction of their Member State, where all other powers pursuant to this Article to bring about the cessation of an infringement have been exhausted, the infringement persists and causes serious harm which cannot be avoided through the exercise of other powers available under Union or national law, the power to take the following measures:

   (a) require the management body of the providers, within a reasonable time period, to examine the situation, adopt and submit an action plan setting out the necessary measures to terminate the infringement, ensure that the provider takes those measures, and report on the measures taken;

   (b) where the Digital Services Coordinator considers that the provider has not sufficiently complied with the requirements of the first indent, that the infringement persists and causes serious harm, and that the infringement entails**:** **(i)** a serious criminal offence involving a threat to the life or safety of persons, or **(ii) the failure of the providers of intermediary services which do not have an establishment in the Union but which offer services in the Union to comply with obligations indicated in Article 11 paragraphs 1, 2 or 3,** request the competent judicial authority of that Member State to order the temporary restriction of access of recipients of the service concerned by the infringement or, only where that is not technically feasible, to the online interface of the provider of intermediary services on which the infringement takes place.

   (…)

EXPLANATION to changes to art. 11 and art. 41 regarding legal representatives*:*

Adding to Article 11 paragraph 4 the obligation of the Digital Services Coordinators to verify the data of the legal representatives ensures that only factually existing entities are designated to perform this function in order to be held liable, if necessary, for the compliance with the

Regulation by the providers of intermediary services which do not have an establishment in the Union but which offer services in the Union.

In order to make enforceable the obligations of the providers of intermediary services which do not have an establishment in the Union but which offer services in the Union to comply with in Article 11 paragraphs 1, 2, and 3, and by this to make the Regulation enforceable against such providers, it is necessary to grant the Digital Services Coordinators powers to request the competent judicial authority to impose effective measures against such providers in case they persistently fail to designate their legal representative, or to mandate the legal representatives in necessary powers required under art. 11 paragraph 2, or to notify the data regarding the legal representative to the Digital Services Coordinator. Otherwise, the enforcement of the compliance by such providers with the Regulation, where the legal cooperation between the Member States' or Unions' authorities with the authorities of the countries of origin of such providers is not established, could turn out to be impossible.

The proposed amendment to Article 41 paragraph 3 letter (b) above aims to flag the problem of the potential lack of enforceability of the Regulation towards the non-EU providers and presents the proposition of the solution of this problem. The non-UE providers that engage in or facilitate illegal activities and address their services to the European Union could in fact benefit from the failure to designate the legal representative. In such situation the enforcement of the Regulation against them would be more complex and extended in time, if possible at all in practice in some cases.

The solution of the possibility to block the services is already known in European Union law. Article 9 paragraph 4 letter g) of *Regulation 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws* empowers the competent authorities with, among other means, the possibility block the services or access to them in order to stop infringements. Polish law also provides for the possibility to block the services, which possibility relates to the services infringing the Polish gambling law (Art. 15f of the Polish act dated 19.11.2009 (as amended)).

Z poważaniem,

Włodzimierz Schmidt
Prezes Zarządu

Związek Pracodawców Branży Internetowej IAB Polska
ul. Puławska 39/77 02-508 Warszawa tel. +48 22 415 54 44 fax + 48 22 212 87 74
www.iab.org.pl