Council of the European Union
General Secretariat

Interinstitutional files:
2020/0361 (COD)

Brussels, 06 July 2021

WK 9006/2021 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:	DE Delegation
To:	Delegations
Subject:	Digital Services Act: DE comments on the key issues of the first compromise text

30 June 2021

DEU

Written comments on the key issues of the first compromise text as examined in the CWP meeting on 10 June 2021

We thank the PRT Presidency for drafting and presenting the compromise proposal on Chapters I and III and the Slovenian Presidency for taking our comments into account in the future discussion of this file.

Please note that the deadlines for comments on the compromise proposal are too short and do not allow for careful consideration and comprehensive coordination of comments within the federal government. Thus, we still have a scrutiny reservation on the proposed amendments. As we had already initiated the inter-governmental consultation before the last CWP meeting, we could also not take the PRT Presidency's instructions to insert our comments into the compromise text into account. Accordingly, we hereby submit written comments with some (framed) drafting proposals only.

Our initial impression is that the draft still lacks **sufficient safeguards to protect users from hate speech** on the one hand but also **from overblocking by online platforms** on the other hand. Also more ambitious measures are needed to **protect consumers**, especially after the experience of the Covid 19 pandemic.

In general, we refer to our previous, very **detailed comments on the proposed Regulation**, which remain largely valid.

Table of Contents

A. Scope of the DSA (Comments on Art. 1 – rec. 1-11 – Subject matter, objectives and scope)

We welcome the new wording in para. 3 which refers to intermediary services "offered" rather than "provided" to recipients and the definition of "place of establishment of a service provider" contained in the new rec. 8a. However, we would suggest to align the wording in rec. 8a with Art. 1(3) and thus refer to services "offered" rather than "provided" as well.

We also welcome the clarification on full harmonisation in rec. 9. It is now clear to us that an explicit derogation in the DSA is required for additional national requirements on matters falling within the scope of the Regulation. In our view, those derogations are needed, especially regarding the notice and action mechanism and the notification obligations. When it comes to protecting freedom of expression and democracy, we should not follow the logic of the lowest common denominator; there has to be room for well-considered national safeguards (e.g. parts of the NetzDG).

For all further considerations and designs of the DSA, the following should be taken into account: There must be an exception to the harmonization for the area of child and youth protection in order to meet the structural, systemic national precautionary measures required by international, European and constitutional law (as laid down notably in CRC/C/GC/25).

We welcome the fact that, according to rec. 9, other national legislation applicable to providers of intermediary services in accordance with Union law, including the ECD and in particular its Art. 3, which pursue "other legitimate public interest objectives", remain permissible (in particular with regard to the protection of minors).

However, we are – in view of the wording "in particular its Art. 3" – wondering whether Art. 1(6) ECD would thus still apply to intermediary services under the DSA or whether we need, for the sake of legal certainty and as a precaution, an explicit derogation for cultural and media diversity inserted as a new para. 6.

In the meeting of 10 June 2021, we have tabled a "virtual room document" (doc. WK 7638/2021 INIT) which contains a detailed reasoning for the following proposal:

> **"6. Member States may take appropriate measures other than those taken into consideration by this Regulation to protect plurality of the media. Any such legislation shall be compatible with the general principles and other provisions of Community law."**

We also welcome the clarification in rec. 10 that "this Regulation should be without prejudice to other acts of Union law regulating other aspects of the provision of intermediary services". However, in particular re. the AVMSD, the precise delimitation between both acts in specific cases is not entirely clear to us: We wonder whether the Regulation or the AVMSD does apply

to “illegal audiovisual media content” covered by Art. 2 lit. g under national law and disseminated on video sharing platforms.

We would like to see a clarification of the relationship of the DSA to Directive 2004/48/EC in Art. 1(5) and would like to know why Directive 2004/48/EC is still not mentioned.

We take note of the deletion of the reference to intellectual property rights in rec. 46. It is our understanding that Art. 17 DSM Directive conclusively regulates this aspect for copyright matters.

We welcome the clarification in rec. 10 that “the protection of individuals with regard to the processing of personal data is solely governed by the rules of Union law on that subject, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC”.

We understand that the last sentence of rec. 9 has now been moved to the end of rec. 10. We wonder whether our understanding is correct that the wording “these rules” does not only refer to the penultimate sentence (“rules of Union law on working conditions and the rules of Union law in the field of judicial cooperation in civil and criminal matters”) but to the entire rec. 10 and whether “these rules” thus also refer to all other legal acts according to Art. 1(5).

The wording of rec. 10 raises questions with respect to the area of judicial cooperation in criminal matters, specifically the E-Evidence Regulation:

- First of all, the recital seems to start from the assumption that the E-Evidence Regulation is an “act of Union law regulating other aspects of the provision of intermediary services”. We do not think that this is accurate. The E-Evidence Package is part of the norms on judicial cooperation in criminal matters which are addressed at a later stage in rec. 10 (“without prejudice to…”).
- Most importantly, we do not think that the provisions of the DSA (Art. 9) may be considered as “lex specialis” in relation to the E-Evidence-Regulation.
- As we have noted before, it must be very clear that the information obligations that Art. 9 foresees for the service providers are only ancillary to the obligations flowing from the E-Evidence package. While the E-Evidence Regulation contains empowering provisions providing for cross-border effect of production orders with respect to electronic evidence, Art. 9 provides for a – secondary – information obligation on the receipt and handling of such orders. This information obligation is of an entirely different nature than the primary obligation provided for under the E-Evidence Regulation.
- The term “lex specialis”, however, implies that the norms at stake are of the same order and vary only as to their degree of specificity.

We also would like to highlight that matters of taxation are important public and financial objectives of the EU and the MS (see Art. 23(1) lit. e GDPR). It is therefore essential to clarify in an appropriate way the scope of the Regulation insofar that it (including Art. 9 and 22) does not affect EU and national tax provisions. This applies in particular to obligations to cooperate

and provide information on taxable persons and third parties, but also to the competence of tax authorities to determine taxable events. It is irrelevant for taxation whether the taxable event is unlawful or even criminally relevant. We would thus be grateful for a corresponding clarification of the text of the Regulation.

Should the Regulation (especially Art. 9 and Art. 22), in contrast, also affect the field of taxation, especially procedural tax regulations like information requests or record keeping, we urge the Presidency to include a corresponding exemption in the text of the Regulation, e.g. in Art. 1 as follows:

“This Regulation shall not apply to the field of tax law of the Member States.”

B. Exemption for micro and small enterprises

I. Art. 15a – Notification of suspicions of criminal offences

We regret that the notification obligation has not been further clarified. From our view, it is still unclear what offences shall be covered and what information has to be transmitted. In our view, Rec. 42a does not provide sufficient clarity.

Furthermore, we believe that the provision needs to be expanded to include criminal offences beyond those involving a threat to the life or safety of a person or persons.

Also, we advocate that MS must be able to provide for further notification obligations regarding certain illegal content, like hate speech, under national law.

II. Art. 16 (rec. 43) – Exclusion of micro and small enterprises

We welcome the fact that the addition “and which are not very large online platforms in accordance with Article 25” has now been inserted into the text of Art. 16.

We regret, however, that the numerous comments made by MS on the definition of SMICE based on the Annex to Recommendation 2003/361/EC were not taken into account. As already stated, we are of the opinion that at least additionally (just as with the qualification of the VLOPs) the number of recipients and the associated reach of the online platforms should also be taken into account. We would thus prefer to see appropriate amendments to the criteria for SMICE.

Also, to ensure that smaller online platforms do not develop into so-called “safe havens” for the dissemination of illegal content, it should be examined whether individual due diligence obligations from Chapter III Section 3 should also apply to micro and small enterprises.

C. Obligations related to content moderation

I. Art. 12 – Terms and conditions

First, it should be clarified that the provider's right to restrict the use of the service must either be effectively contractually agreed or that such a right must result from statutory regulations. The current version of Art. 12 only requires the provider to include relevant information in their terms and conditions (T&C). T&C are used to conclude contractual agreements. T&C are therefore not a tool for merely conveying information. The mere provision of information in the T&C – without a contractual or statutory right – cannot entitle the provider to restrict the use of the service.

Second, in our view, it must be generally clarified to what extent platforms are free to set the parameters for content moderation through community standards of the platforms and thus are free to decide which content and accounts they block. If a platform has a certain relevance for public communication, it should not be an exclusively internal decision which content can be blocked and which not (so called private ordering).

We advocate for more procedural and substantive regulatory requirements in this regard, at least for VLOPs and search engines. The proposal follows a very limited approach which is no longer appropriate given the market power and the massive importance / reach of some providers for the public debate. This is especially valid for media service providers exercising editorial responsibility over their information. It should be noted that, for example, audiovisual content from broadcasters is already subject to EU-wide regulation (minimum standards) under the AVMSD.

Under this regime, compliance is ensured by the supervisory authorities of the broadcaster's country of origin and the broadcaster´s content should in principle be distributed unhindered in the EU, free from further scrutiny by other MS. For the media sector, including all editorial media such as news media, as well as the broader audiovisual sector, it should apply that content that can be legally distributed offline should also be permissibly distributed online.

It needs to be assured that the decision of the providers of hosting services to delete or block a content of a media service provider exercising editorial responsibility over their information does not lead to the unjustified deletion of a content protected by the media freedom and the freedom of expression of the media service provider. We will provide a corresponding wording proposal in due course.

Although Art. 12(1) stipulates that T&C must be provided in a clear and unambiguous language, this does not take into account the special needs of children or adolescents who will probably face special difficulties understanding legal provisions. The best way to ensure that also children and adolescents comply with terms of use is to ensure that they understand the meaning and the effect of such provisions. Therefore, service providers whose services are

primarily aimed at children or adolescents or are predominantly used by this group should be obliged to explain their terms and conditions to minors. We therefore suggest to add a new Art. 12a:

"Article 12a

Protection of minors

1. **If a service is primarily aimed at children or adolescents or is used predominantly by children and adolescents, the providers of intermediary services shall explain conditions and restrictions for the use of the service in a way that children and adolescents can understand.**
2. **The design and online interface of services aimed at children or adolescents or mainly used by children or adolescents must take into account the special needs of children and adolescents."**

II. Art. 13 (rec. 39) – Transparency reporting obligations for providers of intermediary services

We have a legal remark re. para. 1 lit. b: Section 1 of Chapter III (Art. 10 to 13) refers to all providers of intermediary services, including providers of hosting services. Only Section 2 (Art. 14, 15) contains specific, more comprehensive due diligence obligations for providers of hosting services. For systematic reasons, consideration should therefore be given to moving Art. 13 para. 1 lit. b to Section 2.

We welcome the fact that the addition "and which are not very large online platforms in accordance with Article 25" (which is in line with the amended Art. 16) has now been inserted into the text of para. 2.

We also welcome the insertion of a new para. 3 which gives the COM the power to adopt implementing acts to lay down templates concerning the form, content and other details of reports pursuant to para. 1. These templates ensure the comparability of the transparency reports.

III. Art. 14 (rec. 40, 41, 41a NEW) – Notice and action mechanisms

The mandatory requirements still relate solely to notices for illegal content. We regret that the requirements of Art. 14 thus still do not refer to notices for violations of community standards / T&C. Different reporting channels, one for illegal content and one for content that violates community standards / T&Cs, should be avoided.

We still feel the need to clarify that a notification that does not include all the information mentioned in para. 2 still has to be considered by the service provider. E.g., if the explanation why some content is illegal is reasonable, but the notifying person did not enter a name or electronic email address, appropriate actions have to be taken. In its current form the provision (together

with Rec. 41a) restricts the possibilities for anonymous notices, i.a. in the illegal trade of goods (e.g. illegal wildlife trade) or illegal content (e.g. illegal nazi-memorabilia). We therefor suggest to replace the last sentence in Rec. 41a ("Except for the submission […] intellectual property rights.") by the following sentences:

> "In cases where the name and the electronic mail address is not necessary to assess the legality of the content in question, submission of this data shall be optional. Should a service provider consider the submission of that data necessary (for the avoidance of misuse or other reasons), he may make it mandatory, provided this is in line with other regulations, such as Regulation (EU) 2016/679."

We also suggest to amend para 14 II c as follows:

> "if necessary to assess the legality of the content in question 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 of the offences referred to in in Articles 3 to 7 of Directive 2011/93/EU;

Also, the proposal still lacks clarification, in which language the notice and action mechanism has to be provided. Especially given that the notices have to be substantiated, it is crucial, that users can supply notices in every language in which the service is offered. We therefore suggest the following insertion in para. 1:

> "Those mechanisms shall be easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means **and in the language of every Member State, the provider operates in."**

Rec. 41 contains some additional remarks to the obligation of the provider to act upon notices in a timely manner. However, as already requested several times, we would also have liked to see concrete processing deadlines for the assessment of the reported content and deletion of the (obviously) illegal content. We therefore suggest the following insertion in para. 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, **expeditiously,** in a **timely,** diligent and objective manner. **All notices shall be decided within seven days the latest, in case of manifestly illegal content within 24 hours.** 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. **Micro and small providers of hosting services shall be exempted from the 24 hour time limit."**

Rec. 41a states that only manifestly illegal content (i.e. where it is evident to a layperson, without any substantive analysis, that the content is illegal) shall be removed by the provider.

We wonder what this means and whether other illegal content should not be deleted. We have substantial objections to this.

The current so-called notice and action mechanism according to Art. 14 is still not sufficient in our view. It still lacks any element of action. For this reason, we need derogations for national measures to implement additional obligations regarding the action mechanism, i.e. an actual obligation to examine and to delete illegal content. In order to ensure that illegal content, especially hate speech, is effectively removed, intermediaries must be obligated not only to receive notifications but also to process the notified content and to delete or block it if it is illegal. We therefore suggest to add a new para. 7:

> **"7. Member States, in which the provider operates, may regulate that the notice and action mechanisms must ensure that certain illegal content, like illegal hate speech, is removed or access to it is blocked within their territory."**

Whether or not a content is illegal shall be determined by the law of the country of destination that can vary from MS to MS. The intermediaries have to take this into account and have to respect the applicable law in the case concerned. This should be clarified in the DSA as well.

In addition to the notice and action mechanism and with respect to offers of illegal products, providers of e-commerce platforms and market places should also be obliged to notify the digital services coordinators. They could then forward the information about the illegal product and contact details of the retailer to the respective competent national authorities. The notification obligation would thus ensure that these illegally traded products can be seized and all other necessary enforcement measures can be taken by the competent authorities. This would significantly facilitate the implementation and enforcement of the DSA, as it would reduce the likelihood that the illegally traded products are offered on another platform or under another name shortly after the removal of an illegal offer. Simply deleting the illegal posts is not enough. Authorities must be put in a position to actually remove the illegally traded products from the market. In doing so, one key incentive for using the internet for illegal trade would be removed. If such a reporting obligation should not be made mandatory in the DSA, MS should at least have the right to provide for such an obligation under national law.

Finally, we regret that the decision not to delete illegal content despite notification is still not subject to any obligation to give reasons. We therefore suggest the following insertion in para. 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 **and a clear and specific statement of reasons for that decision."**

IV. Art. 17 (rec. 44, 45) – Internal complaint-handling system

Different from Art. 14 and 15, we welcome the fact that Art. 17 now extends to decisions by online platforms not to delete content.

V. Art. 18 (rec. 44, 45) – Out-of-court dispute settlement

Different from Art. 14 and 15, we welcome the fact that Art. 18 now extends to decisions by online platforms not to delete content.

We welcome the insertion of a new para. 4a, which sets out the conditions under which the DSC can revoke its decision to admit an out-of-court dispute resolution body.

However, in our view, it would be desirable if the general principle of voluntary participation was preserved in Art. 18. We therefore suggest that the ADR body should not submit binding decisions, but rather non-binding proposals.

To ensure the constitutional judicial rights of online platforms, we also ask to include an additional sentence clarifying that the platforms have a right to appeal the decisions made by the out-of-court dispute mechanisms.

VI. Art. 19 (rec. 46) – Trusted flaggers

In Art. 19(2) lit. b, the requirement that the trusted flagger must represent “collective interests” has been deleted. Please explain the background of the deletion. We wonder whether individual interests, e.g. of trademark owners, are now also covered by this provision.

VII. Art. 20 (rec. 47) – Measures and protection against misuse

With regard to the time frame, Art. 20(3) lit. a and b no longer refer to the “past year”, but contain a softer wording (“submitted in a given time frame”). This time frame must be determined by the platform itself. We wonder what the background to this change is.

We welcome the addition in rec. 47 which sets out the requirements for a prior warning before deciding on the suspension, such as the reasons for the possible suspension and the means of redress against the decision. However, we still wonder whether stronger safeguards are necessary, e.g. the involvement of a body, other than the platform – at least in cases that are especially sensitive regarding freedom of speech and democracy.

VIII. Art. 23 (rec. 51) – Transparency reporting obligations for providers of online platforms

With a view to business and trade secrets, we still examine the new requirement that providers of online platforms shall, according to para. 2, publish information on the average monthly active recipients of the service in each MS in a publicly available section of their online interface.

In addition, we advocate that the transparency reports also have to include a description of the platforms' examination processes. Since there is a lack of requirements for the detailed design of the testing procedure and qualification of the personnel, transparency requirements could be helpful to promote certain minimum standards. We therefore suggest to add a new para. 1 lit. d:

> "**(d) organisation, personnel resources, specialist and linguistic expertise in the units responsible for content moderation and processing notices and complaints, as well as training and support of the persons responsible for content moderation and processing notices and complaints."**

Also, with regard to the special vulnerability of specific groups of users, e.g. women, existing information regarding the groups of users that are particularly affected and those that share particularly frequently illegal content, should be displayed in the report. We therefore suggest to add a new para. 1 lit. e:

> "**(e) information about which groups of users are particularly affected by illegal content and information about which groups of users share illegal content particularly frequently or make it available to the public and whether and how users have coordinated to disseminate illegal content."**

IX. Art. 29 (rec. 62) – Recommender systems

In our view, recommender systems should not to be preinstalled by default. Users of VLOPs should opt in rather than opt out to the use of a recommender system. Users when using the service for the first time should be presented all the information and options for recommender system and should make their own choice. A crucial point re. the protection of minors: Recommender systems on the basis of profiling within the meaning of Art. 4(4) of Regulation (EU) 2016/679 may not be used on children and adolescents. We therefore suggest to add a new para. 3:

> "**3. Recommender systems shall not be preinstalled by default. Before providing their consent to a recommender system, users have to be provided with the information and options pursuant to paragraph 1 in a clear and unambiguous manner. Recommender systems on the basis of profiling within the meaning of Article 4 (4) of Regulation (EU) 2016/679 may not be used on children and adolescents."**

The proposal also still lacks a set of minimum standards for recommender systems, such as fairness, neutrality and freedom from discrimination.

Besides that, we welcome the insertion that providers of VLOPs shall make information re. recommender systems directly and easily accessible on a specific section of the online interface where the information is recommended. However, it should be further specified which

parameters of the recommender systems have to be named by the platforms. This should include at least all parameters that are directly or indirectly linked to discrimination characteristics such as gender, sexual orientation, age or origin. The same applies to relevant payments by the content author (in particular commission payments) or other business relationships or ownership structures between the platform and the content author. We suggest in addition to the draft, that the information should also be found in a prominent place on the website.

We wonder whether VLOPs should be required to display whether a product or service offered has been awarded a Type I environmental label (ISO 14024), and whether they should be required to offer a filter function for users to search for products and services with such labels ?

D. Obligations concerning online marketplaces

With regard to due diligence obligations, we have always called for a separation of interaction and transactional functionalities. We thus expressly welcome the insertion of a new Section 3a into Chapter III which applies only to providers of online marketplaces as defined in Art. 2 lit. ia NEW.

We also welcome the definition of an “online marketplace” in Art. 2 lit. ia NEW.

However, we still see a great need for discussion on the respective due diligence obligations for these online marketplaces.

The new Section 3a focuses on transparency and more information of the consumer. However, this is in our view not sufficient and clear obligations should be introduced instead.

In addition, abusive, fraudulent and misleading web-design (dark patterns) is a severe problem for many users. To fight “dark patterns” we need a prohibition of those practices and clear design obligations as proposed by DEU should be introduced.

I. Art. 24a (rec. 49, 50) – Traceability of traders

In particular with regard to procedural tax regulations, we welcome the fact that the obligation of providers of online marketplaces to store the information received by traders for six months leaves unaffected potential obligations to preserve certain content for longer periods of time, on the basis of other Union law or national laws, in compliance with Union law.

We welcome that para. 2 imposes providers of online marketplace not just to make “reasonable” but “best” efforts to assess whether the information about the traders is reliable. In our view, if no such freely accessible database exists in a MS, platforms that are not micro or small enterprises should be required to also use databases of reference at moderately priced costs.

It also remains unclear how verification of the commercial user is carried out by platforms for traders established in third countries and how traders can be prevented from disguising themselves as private users in order to circumvent the obligation to provide information.

We would like to ask the Presidency to explain why the word “sufficient” was inserted in Art. 24a(3),.

In our view, the proposal, still lacks a clear set of responsibilities of the platforms for combating illegal content. We advocate for more obligations of the online market places to act proactively against infringements, such as fake shops and other (clearly illegal) or fraudulent offers. We therefore suggest the following insertion of a para. 7:

> ***"7. The online platform shall take reasonable, technically and organisationally possible and, where appropriate, automated measures to prevent that illegal content in relation to the promotion of messages on or the offer of products or services to consumers will be disclosed on its online interface."***

In this respect, it is not clear why this section at times uses the term "consumer" instead of "recipient of the service"; compliance with the law extends beyond consumer protection.

We welcome the clarification in recital 50 with reference to the retention obligations of Art. 24a. However, it must also be noted that the clarification on the unaffectedness of Union and national tax provisions (e.g. other retention obligations for platform operators in the Directive on Administrative Cooperation DAC 7) should be inserted in the mandatory text of the Regulation and not only in the recitals.

We wonder how it can be ensured that traders do not pretend to be private users / consumers to avoid providing the information under Art. 24a. In our view this risk of misuse is not remedied by the Unfair Practices Directive, because the offering and sale of illegal products is not only relevant from a consumer law perspective. Many products are offered on platforms in violation of public laws, such as protected plants and species or prohibited substances that are harmful for the environment. We also wonder how the traceability of such traders (specifically if the recipient of the product has little or no interest in private law enforcement through the Unfair Practices Directive) will be ensured.

Finally, we wonder about the mechanisms to ensure compliance by platforms with their obligations under Art. 24a.

II. Art. 24b (rec. 49, 50) – Compliance by design

We welcome the online marketplace's obligation set out in para. 2 to allow for the unequivocal identification of the products or the services offered, and, where applicable, the publication of information concerning the labelling in compliance with rules of applicable Union law on product safety and product compliance.

However, we have already proposed that the online platform should not only allow for certain information of the trader but also ensure by design that offers for products or services to consumers can only be uploaded on the online platform if the relevant design interface for the obligations regarding pre-contractual information and product safety information under applicable Union law are filled out.

III. Art. 24c (rec. 49, 50) – Right to information

We welcome the online marketplace's duty to either inform the recipients of its service that had acquired a product or contracted a service which constitutes an illegal content during the last

six months or to make publicly available and easily accessible on their online interface the information about the illegality, the identity of the trader and any means of redress.

In addition, providers of online marketplaces should also be obliged to notify the digital services coordinators or market surveillance authorities of these products or services. They could then forward the information about the illegal product or service and contact details of the trader to the respective competent national authorities. This is important for the reasons set out under D. I., namely that private law enforcement (through consumer protection law) is insufficient in cases where public law is violated, e.g. illegal wildlife trade.

The notification obligation would thus ensure that these illegally traded products can be seized and all other necessary enforcement measures can be taken by the competent authorities.

This would significantly facilitate the implementation and enforcement of the DSA, as it would reduce the likelihood that the illegally traded products are offered on another platform or under another name shortly after the removal of an illegal offer.

The legal consequences of a breach of the information obligation remains unclear.

E. Further remarks relating to other issues and provisions

I. Art. 2 (rec. 14) – Definitions

We expressly welcome the clarification made in rec. 14 on interpersonal communication services which generally includes emails and private messaging services in the definition of online platforms (lit. h) insofar as the content is disseminated to the public (lit. i), i.e. disseminated to an unlimited number of recipients (esp. through public groups or open channels).

However, it still needs to be clarified in Art. 2 lit. g whether the "illegality of content" is determined by the law of the country of origin or (also) by the law of the country in which the provider provides its services. While there seems to be some agreement between MS which statements are tolerable and which are criminal there are also substantial differences in a lot of cases.

Criminal law assessments of MS in which the effects of a statement/content occur may not be ignored, especially since the effects of any unhindered dissemination of unlawful content can have a direct impact on national democratic systems. The proposal should clarify that the illegality of the content is also determined by the law of the country in which the provider provides its services and what consequences a request of deletion of that country and its authorities will have (unionwide deletion of the content?).

The DSA is mainly aimed at commercial platforms. In our view, it should be clarified whether and to what extent not-for-profit scientific and educational repositories are covered by the proposal. Currently, they would either qualify as online platforms (Art. 2 lit. h) or as hosting service providers (Art. 2 lit. f). From a research and education perspective, it is important that these do not face additional or disproportionate burdens and investments to comply with the DSA requirements. Many of them are smaller repositories and many of them are promoting Open Science. In many cases, they would not have the capacity to deal with the requirements of the Regulation due to small budgets and staffing. As an unwanted result, the number of repositories could be reduced, which contradicts the idea of Open Science with many different initiatives.

II. Art. 10 (rec. 36) – Electronic point of contact

We welcome the insertion, that at least one language broadly understood by the largest possible number of Union citizens, can be used for communication with providers.

However, we think it should be possible to use any language commonly spoken in a MS of the EU where the provider operates. Furthermore, we advocate for an obligation of the provider to appoint domestic contact persons in every MS it operates in, e.g. authorised agents for legal proceedings. This is crucial e.g. to make it easier for citizens to bring disputes with "their" providers before independent courts.

III. Art. 24 (rec. 52) – Online advertising transparency

Art. 24 provides for new transparency requirements for personalised advertising. In our view, these requirements do not go far enough. Considerable questions arise about the practice of personalised advertising.

Some online platforms rely on a business model of comprehensive tracking and profiling of users in order to generate revenue through personalised advertising. Instead of personalised advertising, however, platforms could generate revenue with context-based advertising or with new technological solutions. Users should at least have a right to use online platforms without personalised advertising. We also have to take into consideration the ongoing trilogue re. the ePrivacy Regulation.

We should ban personalised advertising in particular towards minors (i.e. under 18). Any additional identification obligation for all users should however not be introduced. Minors are even less aware of the existence of personalised advertising and how businesses use them to generate revenue. Because of the business inexperience of children and young people, rules on transparency with regard to personalised advertising only are not sufficient.

IV. Art. 31 (rec. 64) – Data access and scrutiny

We welcome that rec. 64 now includes “appropriate training data and algorithm”. This is an important clarification.

According to the wording, the purpose limitation pursuant to para. 2 in conjunction with Art. 26 is intended to be an exhaustive catalogue of legitimate research purposes that justify access to data. It should be ensured that new research questions can also fall within the scope of Art. 31 in order to create a future-oriented sustainable data access regulation. The characteristic of "expertise" in paragraph 4 appears fundamentally problematic for various reasons:

- On the one hand, it is not plausible why a certain expertise should be a prerequisite for data access at all?
- If the requirement is intended to counteract a possible risk of abuse, the researcher’s membership of an academic (non-commercial) institution should exclude this risk.
- On the other hand, it is not clear how the proof of expertise pursuant to paragraph 4 is to be provided. What objective criteria are to be used here?
- This criterion is also problematic with regard to young researchers. It would be difficult for them to provide such proof and they would be effectively excluded from access to data.

Are we correct in assuming that – in any case for research purposes – no personal data are collected from this? If personal data are collected, this must be in accordance with the GDPR (cf. also Art. 1(5)(i)). In all cases, care must be taken to ensure that research access cannot be abused to obtain certain data for one's own purposes.