Council of the European Union
General Secretariat

Brussels, 26 March 2021

Interinstitutional files:
2020/0361 (COD)

WK 4265/2021 INIT

LIMITE

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

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:	Presidency
To:	Working Party on Competitiveness and Growth (Internal Market - Attachés) Working Party on Competitiveness and Growth (Internal Market)
Subject:	Digital Services Act: MS questions on Chapter III

Digital Services Act
MS Questions on Chapter 3

Contents

Belgium

Article 11:

Q1 What would be the consequence of the intermediary having to be established in a Member State according to another specific legislation (e.g. tax legislation ?). Would it then be considered **established "de facto"** in that Member State, and would it not have to designate a legal representative?

- As it is already the case with Directive 2000/31, the question as to whether the provider is "established" in a Member State should be determined in conformity with the case-law of the Court of Justice according to which the concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period. The notion of "establishment" may vary depending on the applicable legal framework and must be assessed independently for the purposes of the DSA. The residence for tax purposes may therefore not be relevant.To the extent that such an establishment, that may be required under specific legislation, would constitute an establishment within the meaning of EU law, such a provider of intermediary services would not be required to appoint a legal representative since it would already be established in the EU within the meaning of Article 11 DSA.
- In addition, nothing in the DSA precludes a provider of intermediary services that is not established in the EU, but already has a legal representative in the EU by virtue of a legal requirement under another EU legislation, to appoint the same legal representative under Article 11 DSA.

Article 13:

Q2 We would like to ask practical precisions regarding **the scope** of this Article:

- **Where/to whom and in what language** should this information be provided to and where/ in which language should the transparency report be published ?
  - The reports under Article 13 need to be published by the providers, there is no need to send them to any particular person or authority. Publication means that the reports must be accessible, e.g. on a website. There is no specific language requirement.
- "*including orders issued* ***in accordance with articles 8 and 9***"

  Should an order issued/received under the provisions of another instrument (e.g. TOC Regulation) also be part of the transparency report? Or should the information be limited to the number of orders received according to article 8 and 9 DSA?
  - Article 13(1)(a) covers any and all orders from national authorities. Articles 8 and 9 are mentioned as examples to clarify that they are in scope.
- "*number of notices submitted* ***in accordance with article 14***"

  What about notices received in accordance with another sector specific legislative text (e.g. Copyright acquis, AVMSD)? Should those not be part of the transparency report?
  - The transparency obligation is established by the first sentence of Article 13(1) and it covers "any content moderation". The list of information in points (a)-(d) is non-exhaustive ("in particular") and

its main purpose is to indicate the obligatory categories providers need to break down in their reports. Therefore, the reporting obligation potentially covers other notices, including those provided for in the sector-specific rules.

Article 22.1 f):

Q3 *"a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law."* Does this have **an impact on the liability** of the platform if it turns out that the trader offers products/services that are not compliant with rules of Union law? Are there any **criteria** to be fulfilled for the self-certification **or** would **a mere statement** of the trader suffice?

- This does not have any impact on the liability regime applicable to the platform. The liability of the platform in such circumstances is determined by the conditions of Article 5, which depends on actual knowledge and failure to act in the light of that knowledge, not an inaccurate self-certification.
- In the event an online platform receives an indication that a self-certification provided by a trader is inaccurate and such trader has failed to correct it without delay upon the platform's request, the platform has the obligation to suspend the provision of its service to the concerned trader (Article 22, paragraph (3)).
- Given the horizontal nature of the DSA, Article 22 does not contain any specific requirements for self-certification. The self-certification under this Article corresponds thus to a general statement by the trader that the products or services offered to consumers in the European Union through online platform are compliant with the applicable Union law.

Slovak Republic

Section 2

Q4 *Art 15(2)(a): Does this mean that the removal or disabling of access to illegal content will only be done in the MS from which the notice came while it may remain available in other MSs? Why is it not removed in all MS where it is illegal according EU law once it is reported even from just one of such MSs?*

- Article 15(2)(a) should not be understood as meaning that a decision within the meaning of Article 15(1) may only decide on the removal or disabling of access to specific content for a specific territory from which the notice came.
- This provision simply requires the provider of hosting services to inform the recipient of the service of the territorial scope of the disabling of access, which could be EU wide, such as where a specific item of information would be considered illegal EU wide because for example its illegal nature results from harmonized EU law.

Section 3

Q5 *Art 20(3)(d): How are the platforms expected to objectively assess the intention of the recipient, individual, entity or complainant in the context of notice & action mechanism? Doesn't this run the risk of providing blanket excuse for the online platforms to disregard frequent or repeated notices?*

- The provider needs to assess intention by relying on the available relevant facts and circumstances. This can include, for example, the frequency of misuse or the statements of the recipient, individual, entity or complainant, for instance signalled by a high number of complaints. While the intention of a person is a subjective element, the provider needs to assess it in an objective and non-arbitrary manner. If the apparent facts and circumstances do not allow the provider to determine the intention, this aspect will not be taken into account.

Section 4

Q6 *Art 26: Who will evaluate the quality and accuracy of the risk assessments and the mitigation measures adopted? Will it be required that the risk assessments contain also ex post evaluation of the previously adopted mitigation measures? Can the EC, please explain how exactly the assessment under article 26(1)(b) and rec. 57 should be performed and what should be the framework reference (benchmark) for such an assessment?*

- There are several instances at which the risk assessment and risk mitigation measures taken by platforms pursuant to Articles 26 and 27 are assessed.

  An independent audit will assess compliance with the obligations, under the conditions set in Article 28, and the recommendation of the audit must be duly taken into account, feeding back into the risk management approach of the platform where appropriate.

  Further, the Digital Services Coordinator of establishment is competent for enforcing the obligations and can exert all the relevant powers afforded by Article 41 (for example in requiring information from platforms or auditors, conducting on-site inspections and potentially requiring remedial action plans, also as regards Articles 26 and 27 obligations). Similarly, the Commission can, where relevant, exercise its enforcement powers set in Section 3 of Chapter IV also as regards Articles 26 and 27 obligations.

  Finally, the quality, appropriateness and completeness of the risk assessment and risk mitigation measures taken by platforms is subject to public scrutiny, not least through the additional transparency requirements set in Article 33(2), as a strong accountability measure.

- The risk assessments are part of an iterative cycle embedded in the obligations on very large online platforms. To the extent that the risks remain significant and systemic, they will be identified through the risk assessment under Article 26 and be subject to mitigation measures under Article 27.

- As for all other types of systemic risks considered under Article 26, assessments for negative effects for the exercise of fundamental rights included under 26(1) point b) need to be specific to the service and account for all significant systemic risks. The proposed Regulation is not prescriptive on how precisely to conduct the risk assessment in itself, accounting for not only the great diversity of platforms and situations, but also the systems to be assessed - from algorithmic systems, to internal resource allocation, processes, procedures and tools. Each very large online platform is

required to conduct a risk assessment and, as stated in recital 59, should involve the representatives of the groups most concerned by both the assessment of risks and the design of the mitigation measures.

Germany

Q7. **Re. Art. 10 / 11:** In order to facilitate claims by citizens against "their" providers before independent courts and in order to facilitate criminal prosecution, DEU has made good experiences with an obligation under national law (Network Enforcement Act – NetzDG) that requires large platforms to identify and publish so-called domestic authorised representatives and authorised recipients. These authorised representatives are possible addressees, for example, if documents have to be served in legal proceedings before German courts regarding the dissemination of unlawful content, or if requests for information from domestic law enforcement authorities have to be submitted. This facilitates the enforcement of individual legal claims and criminal prosecution.

- **Does the DSA (in particular Art. 10 / 11) preclude corresponding national provisions on the designation of domestic authorised representatives / authorised recipients?**

- As a general principle, Member States will not be allowed to adopt parallel national provisions on the matters falling within the scope of, and exhaustively regulated by, the DSA, since this would affect the direct and uniform application of the regulation. This consideration also applies to the provisions of the DSA imposing the obligation to appoint a legal representative. A MS cannot impose analogous obligation for the matters falling within the scope of the harmonised rules of the DSA.

- Nothing prevents a provider that may have appointed a legal representative on the basis of the national legislation (that is compatible with EU law) to decide to appoint the same legal or natural person as a legal representative for the purpose of compliance with Article 11 DSA.

Q8. **Re. Art. 12:** The provisions on community standards in Art. 12 are essentially limited to transparency requirements and to an obligation to apply and enforce community standards in a proportionate and non-arbitrary manner. It is therefore still largely up to providers how they deal with the content of their users on the basis of their terms and conditions, e.g. which content they generally do not allow, which content they display particularly prominently or which accounts they block permanently.

- **How can an effective monitoring and enforcement of the very general provisions of Art. 12 be ensured?**

- Article 12 sets the general requirements of diligence, objectivity and proportionality in relation to the measures that intermediary service providers take in applying and enforcing restrictions contained in their terms and conditions, as well as to provide clarity and predictability of restrictions the service provider may take.
- While the provisions of Article 12 impose self-standing obligations, the DSA includes several transparency obligations which pursue a similar objective of increasing objectivity and proportionality in relation to the enforcement by the provider of its terms and conditions, including for, example, statement of reasons obligations towards users whose content is removed (Article

15), reporting such statements of reason in a publicly accessible database (Article 15(4), and transparency reports (Articles 13, 23, 33).

- Alleged violations of the requirements of Article 12 can be invoked as part of the internal complaint and out-of-court dispute settlement mechanisms pursuant to Article 17 or 18 as well as in judicial proceedings.
- The Digital Services Coordinator of establishment can assess compliance with Article 12 based on public information (e.g. terms and conditions together with transparency reports as per above), as well as in exercising its investigatory powers pursuant to Article 41.

Q9. **Re. Art. 14:** DEU welcomes that the COM proposal provides for a simple notice and action mechanism. However, the proposal lacks precise time limits for reviewing any notified content and for deleting (obviously) illegal content. This is a major difference to the current German regime under the NetzDG.

- **To what extent will Member States be able to further specify any notice and action mechanism under national law and, in particular, to set specific time limits for the deletion of certain types of illegal content?**

- As a matter of principle Member States will not be allowed to adopt parallel national provisions on matters falling within the scope of, and exhaustively regulated by, the DSA, since this would affect the direct and uniform application of the regulation. For example, the DSA harmonizes all aspects of the notice and action procedures across the EU (Art. 14).
- The legal basis used, as well as the choice of the instrument (Regulation), already provide that the objective of the legislator is to ensure a high degree of harmonisation in achieving the balance between the proper functioning of the internal market and the definition of uniform rules for a safe, predictable and trusted online environment, where fundamental rights enshrined in the Charter are effectively protected (see Article 1(2) DSA).

- **And can a Member State lay down obligations for platforms to delete certain illegal content in national law?**

- National law and, where relevant, other acts of EU law may confer powers on the national authorities to order platforms to remove illegal content by means of a court or administrative order, as acknowledged in Articles 5(4) and 8 DSA.
- As regards the possibility to provide for a general obligation to delete content as a result of a notice, even apart from the fact that, as explained, Article 14 DSA exhaustively regulates matters relating to notice and action, such an obligation would be inconsistent with the nature of the liability exemption of Article 5, which – in contrast to binding orders of the authorities referred to in the previous bullet – leaves it to the platform to decide whether to take an action upon a notice. In other words, such an obligation would, in effect, turn a notice into an order.
- Furthermore, such an obligation, where it results from the orders referred to above, would need to comply with other relevant provisions of EU law, such as Art. 7 DSA prohibiting general monitoring or fact-finding obligations, Article 3 of the E-commerce Directive which prohibits unjustified restrictions to the cross-border provision of information society services, and the EU Charter of Fundamental Rights, in particular its Article 11 (freedom of expression and information), as such an obligation could create an additional incentive for service providers to take action on notices, even if those that are unfounded.

Q10. **Re. Art. 14:** If a platform becomes aware of illegal content, it is currently (only) obliged to delete the information.

- **How does the DSA ensure an effective and permanent enforcement with regard to illegal content, in particular how does the DSA ensure that dangerous and illegal products can be seized and taken off the market by the competent authorities? Should platforms be obliged to report to the relevant authorities in the Member States in order to ensure that illegal content can also be physically confiscated by the relevant authorities?**

- As touched upon in the reply to previous question, the DSA does not contain an obligation to remove the notified content. Article 5 DSA reproduces the liability regime of Article 14 of the e-Commerce Directive: the consequence of inaction as a result of a sufficiently precise and adequately substantiated notice (see recital 22 DSA) is the loss of the liability exemption, as the provider is considered to have knowledge or awareness of the illegal content and has failed to remove (or disable access to) it expeditiously.
- There are however some related obligations in the DSA:
    - Article 21 requires online platforms to promptly inform law enforcement or judicial authorities of suspicions of serious criminal offences involving a threat to the life or safety of persons.
    - Article 15(4) requires hosting providers to publish – albeit anonymously – their content moderation decisions and the statements of reasons in a publicly accessible database managed by the Commission.
    - Article 8 obliges providers to inform the authority issuing the order of the effect given to the orders, without undue delay, specifying the action taken.
    - Finally, Article 13, 23 and 33 provide for various general transparency obligations tailored to different categories of services.
- Moreover, Article 9 DSA ensures that, where provided for in national law, national authorities can request information from service providers as regards specific users to the extent that this information is necessary to ensure compliance with EU or national rules.

Q11. **Art. 21** of the DSA proposal obliges platforms to provide all information in their possession with regard to the suspicion of a serious criminal offence involving a threat to the life or safety of persons.

- **Are platforms obliged to provide information such as the last log-in IP in order to enable the identification of the content author for the purpose of criminal investigations? Can Member States lay down additional reporting obligations in national law, covering e.g. the use of anti-constitutional symbols or trade in counterfeit goods in order to facilitate criminal prosecution?**

- Article 21 rather obliges the online platform to provide all relevant information, which could if appropriate include last log-in IP (subject to the compliance with EU legislation on the protection of personal data).

- The reference to a "serious criminal offence involving a threat to the life or safety of persons" includes, inter alia, offences specified in the Child Sexual Abuse Directive (Directive 2011/91; see Recital 48). Since criminal offences are mostly set out in national law, the reference is likely to be interpreted taking into account national criminal law. As a matter of principle, Member States will not be allowed to adopt parallel national provisions on matters falling within the scope of, and exhaustively regulated by, the DSA, since this would affect the direct and uniform application of the regulation. This consideration also applies to the provisions of the DSA on reporting on suspicions of criminal offences.
- The legal basis used, as well as the choice of the instrument (Regulation), mean that the objective of the legislator is to ensure a high degree of harmonisation in achieving the balance between the proper functioning of the internal market and the definition of uniform rules for a safe, predictable and trusted online environment, where fundamental rights enshrined in the Charter are effectively protected (see Article 1(2) DSA).

Q12. **Re. Art. 22(4):** According to the results of our preliminary examination, some provisions of the DSA might have effects on procedural tax law, provided that tax law is not excluded from the scope of the Regulation anyway. According to Art. 22(4), the online platform shall only store information for the duration of the contractual relationship with the relevant trader concerned and subsequently delete it. This provision would thus contradict national tax record keeping provisions.

- **Does the DSA affect the field of taxation, particularly procedural tax regulations like information requests or record keeping provisions?**

- The timeframe provided by Article 22(4) is limited to the purposes under this Regulation. This is without prejudice to sector-specific legislation that may establish longer storage requirements for instance for tax purposes. This is also the case with regard to the proposed Directive on Administrative Cooperation, which includes an obligation for some platforms to collect specific information on sellers using their services for tax purposes.

Q13. **Re. Art. 25-33:** Section 4 is currently limited to very large online platforms.

- **Should other important digital service providers, such as search engines, also be subject to Section 4?**

- Search engines are covered by Sections 2, 3 and 4 of Chapter III to the extent that they offer of the services covered by those provisions, notably caching or hosting services within the meaning of the second and third indent of Article2(f). Whether this is the case will depend on a case-by-case assessment, having regard to the technical features of the service provision in question (for instance by hosting thumbnails of pictures, or the index that includes hyperlinks to the original content).

Malta

Q14. The definition of 'intermediary service' seems to be broad and to apply not only to 'information society services'. Consequently, Electronic Communications Services and Networks as defined under the European Electronic Communications Code might also be considered to fall

within this definition as offering a 'mere conduit'. A number of articles (e.g. Article 10 to 13) refer to obligations imposed on 'providers of intermediary' services'. Do these articles apply to Electronic Communications Services and Networks?

- Yes, mere conduit providers may also qualify as providers of electronic communications services, and the corresponding rules are applicable to them in that case. This is also indicated in the European Electronic Communications Code (EECC; Directive 2018/1972) with regard to the current E-commerce Directive, see for instance recital 270 EECC.

Article 14 – Notice and Action Mechanisms

Q15 Article 14(2) contains a list of elements to facilitate the submission of notices. One of these elements is the 'exact URL' identifying the illegal content. Malta notes that an 'exact URL' might not always be easy to extract from certain online platforms (for instance, a post on a social media 'wall' by a user might not have a publicly extractable URL per se, or else the URL might contain characters that identify unique 'tokens' pertaining to the logged in user only). Could the Commission comment on this?

- Article 14(2)(b) DSA requires facilitation of submission of notices that contain "**a clear indication of electronic location**, **in particular** exact URL or URLs".
- As long as a clear indication of the electronic location or any other information that would reasonably allow identification is provided, this would be sufficient. URL is primarily provided as the most common way to identify location of specific information online and has therefore been used the best possible indicator of the electronic location, but it is not the only possibility.

Article 15 – Statement of Reasons

Q16 In non-harmonised areas, Member States might have conflicting interpretations of what content is considered illegal in terms of their national law. In a situation where a content provider has provided content on a hosting service provider, which is considered legitimate and legal in MS 'A' (country of origin) but is deemed to be illegal in terms of the laws of MS 'B' (country of consumption), what safeguards are in place to ensure that the content provider has adequate safeguards or means of redress that can be sought in terms of the law of their country of origin?

- The illegal nature of content will continue to be determined by relevant EU and national laws, and, especially in the absence of common EU rules, national laws may indeed differ in this regard. It is possible that a certain piece of content is legal in one Member State, but illegal in another Member State.
- Depending on the provisions applicable to the content at stake and the legal grounds for illegality, the hosting service provider must assess the territorial scope of the disabling of access and explain it in the statement of reasons (Article 15(2)(a)).

- This means in practice that the service provider may have to disable access to the content from the Member State where the content is illegal upon obtaining knowledge that the content is illegal there, while keeping it accessible in other Member States.

Austria

Q17 Art. 18 para 3: Does "any fees and other reasonable expenses" of the recipient also include the fees of a lawyer?

- The term "reasonable expenses" can include the cost of legal representation where such costs have been reasonably incurred, which is to be determined on a case-by-case basis.

Q18 Art. 18: What is the relationship between Art. 18 DSA and Directive 2008/52/EC of 21 May 2008 on certain aspects of mediation in civil and commercial matters?

Background of the question: Art. 18 para 1 DSA stipulates that Online Platforms shall be bound by the decision taken by the settlement body. As a consequence, the result of the out-of-court dispute settlement which obliges the Online Platform to undertake a certain conduct would be enforceable, whereas according to Art. 6 of the above mentioned „Mediation Directive" a written agreement resulting from mediation can only be made enforceable if both parties agree.

- Article 18 establishes a different procedure to Directive 2008/52/EC, to the extent that it requires platforms to engage, in good faith, with the dispute settlement body, the decision of which is binding.
- In other words, Article 18 intends to tackle the imbalance between the parties by making the dispute settlement binding upon the online platforms and thus going beyond pure mediation regulated by Directive 2008/52/EC.

- Why is the person that notifies an illegal content to the provider neither involved in the internal complaint-handling-system according to Art. 17 nor in the out-of-court dispute settlement according to Art. 18?

Background of the question: It is possible that the person that notifies an illegal content pursues a claim that concerns personal circumstances of this person (e.g. libel, use of copyright protected content) and who therefore has an interest to participate in the dispute resolution procedures. As the notifying person cannot participate in these procedures she or he likely pursues her/his interest in a judicial or administrative proceeding that could result in an order of this authority, which could be contrary to the result of the mechanisms foreseen in Art. 17 or Art. 18. This could lead to contradictory outcomes, which both are binding (e.g. if the judicial or administrative order imposes that a certain content has to be taken down, while the procedure according to Art. 18 comes to the result that the content has to stay online).

- Typically, disputes covered by Article 17 and 18 are between the online platform and the recipient of the service whose content has been removed or whose access to the service has been restricted.
- At the same time, the DSA does not prevent the involvement of the notice provider in the dispute. Since diligence and objectivity are required when handling complaints, it may in certain cases be necessary to take account of the views of the notice provider.
- Article 14(5) requires the hosting service provider to notify the notice provider of the content moderation decision, providing information on the redress possibilities in respect of that decision. Even if such redress does not include the internal complain mechanism under Article 17 or the out-of-court dispute settlement under Article 18, the notice provider may always turn to the courts or other competent national authorities, in accordance with the relevant national rules, if it disagrees with the decision of the hosting service.

Q19 **Art. 20 para 2**: Why is paragraph 2 obligatory and not optional for platforms, since the ratio seems to be that platfoms do not have to (but may if they wish) proceed with unfounded notices and complaints?

- The obligation in Article 20(2) is to stop the processing of notices and complaints coming from an individual or entity that misused the notice and action mechanisms. This covers not only manifestly unfounded notices and complaints already submitted, but also notices and complaints submitted later – during the period of suspension – regardless of whether those are unfounded or not.
- The practical relevance is that, during the period of suspension, platforms do not even have to assess the notices and complaints to determine whether they are unfounded or not.

Croatia

Q20 It may be necessary to clarify Art. 21 in the part relating to "a serious criminal offense involving a threat to the life or safety of persons". Namely, the preamble (48) of the introductory part of the Regulation describes cases of finding out about committed criminal offenses or intent to commit "serious criminal offenses threatening the life or safety of persons, such as the offenses listed in Directive 2011/93 / EU of the European Parliament and of the Council. This directive refers precisely to the suppression of sexual abuse and sexual exploitation of children and child pornography. Does this explanation include the offenses of sexual abuse and sexual exploitation of children in Article 21. in accordance with the proposed Regulation?

- This is just an example of a serious criminal offence involving a threat to the life or safety of persons within the meaning of Art. 21, but it should not be considered the only one.
- In addition, it should be clarified that DSA does not define what content shall/may be considered illegal: this depends on other acts of EU law and national law (see Art. 2(g) DSA).

Slovenia

Q21. With regards to Article 12 we would like to get clarification of the terms and conditions from the perspective of self-initiated content moderation, especially algorithmic decision-making in different phases of intermediary service usage. What kind of information should be included in the terms and conditions that we could consider a user of services is appropriately informed about the conditions under which the services could be used? Which type of content should be primarily blocked or deleted, to ensure that fundamental user rights are respected?

- Recital 38 clarifies the intention of the information requirements in Article 12 – 'in the interest of transparency, the protection of recipients of the service and the avoidance of unfair or arbitrary conditions'. The information presented in the terms and conditions, including as regards the use of algorithmic decision-making tools, should be sufficient to enable this objective. It should be set out in clear and unambiguous language, publicly available and easily accessible.

  Given the diversity of restrictions covered, Article 12 cannot list all possible information categories that should be provided, but this requires a case by case interpretation. In addition, as regards automated tools, Article 12 requirements are also mirrored in transparency requirements such as those on content moderation in Article 23(1) point (c).

- Article 12 does not regulate the type of content that can be removed by a service provider, leaving the freedom of contract of the service provider unrestricted in this regard. It requires, however, the provider to inform the user of any restriction that may be imposed, and to act in a diligent, objective and proportionate manner in applying and enforcing these restrictions. Consequently, the removal of content which is not illegal under applicable law and which is not covered by a restriction included in the terms and conditions pursuant to paragraph 1, would not be in compliance with paragraph 2.

Q22. Does the European Commission see any room for a more precise definition of content moderation at the providers' own initiative? With the aim to minimize risk for possible interference with fundamental human rights.

- Article 12 is broad in scope and applies to all types of intermediary service providers, from mere conduits to very large online platforms, and not all of them exercise content moderation in a same manner. Article 12 respects the contractual freedom of the service provider, which is a fundamental right too (as part of the freedom to conduct a business, protected under Art. 16 Charter) and acknowledges the legitimate interests of service providers in imposing certain restrictions in the provision of their service. Given the horizontal scope of the DSA, further limitations to the freedom of contract of service providers did not appear necessary and justified.

- With regard to very large online platforms, where societal impacts and the impacts on fundamental rights is different in nature and scale, the risk assessment and mitigation measures pursuant to Articles 26 and 27 amount to further obligations as regards the content moderation systems of the provider. In particular, in view of Article 26(1), point b), the service provider needs to assess the risks its systems pose for any negative effects for the exercise of certain fundamental rights and, following Article 27, bears an obligation to mitigate these risks.

Q23. What is the relation of the content moderation approach in DSA in comparison to AVMS Directive? From this point of view, what is the position of video sharing platforms like e.g.

youtube.com? Does self-initiated content moderation of such platforms fall under the legal provisions of DSA?

- The DSA will be complementary to sector-specific legislation such as the AVMSD, which will apply as lex specialis (see Art. 1(5) DSA). The obligations of the AVMSD imposed on video-sharing platform providers as regards audiovisual content and audiovisual commercial communications will continue to apply. However, the DSA's horizontal rules will also apply to those service providers where the AVMSD does not contain more specific provisions.
- Voluntary content moderation of video-sharing platform providers will fall under the provisions of the DSA (e.g. Article 6, Article 15, as well as the due process and transparency obligations), and the horizontal rules will apply, unless the AVMSD lays down more specific provisions.

Denmark

Q24. Due diligence requirements according to type of service

Chapter III introduces an array of due diligence requirements for digital services dependent on whether they fall under broader categories like intermediary services or more narrow ones such as online platforms. In order to clarify which requirements are applicable to the different types of intermediaries, could the Commission elaborate on what types of services fall under the category of hosting services (i.e. cloud services, domain name registries etc.)?

The examples given below should be understood as illustrative, non-exhaustive and need to be subject to a case-by-case appreciation. However, in general it is currently accepted that the following services fall in principle under these categories. The Commission had two studies carried out, on hosting[1] and non-hosting services[2], which are publicly available and give more details on the methodology.

- 'Hosting': e.g. cloud computing, web hosting, services enabling sharing information online, file storage and sharing, referencing services, Infrastructure as a Service, Platform as a Service[3];
- Online platform: e.g. online marketplaces, social networks;
- Domain name registries would normally not fall under the 'hosting' category but could fall either under the 'mere conduit' or 'caching' categories; some registrars might fall under the 'hosting' category, but exact categorisation has to be assessed on a case-by-case basis and depends on particular technical functionalities provided by the particular service provider.

Q25. Article 11: Legal representatives

As we understand the article, it applies to all providers of intermediary service established outside the EU but offering services to European citizens. Can the Commission elaborate on what a 'significant number of users' and 'targeting activities towards one or more Member States' in this

[1] Hosting intermediary services and illegal content online https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en

[2] Legal analysis of the intermediary service providers of non-hosting nature: https://op.europa.eu/en/publication-detail/-/publication/3931eed8-3e88-11eb-b27b-01aa75ed71a1

[3] For more details, second part of the IA accompanying proposal for a DSA elaborates on these examples on p. 170-172.

regard constitutes (definition from article 2 (d))? Does this mean that for instance a small video sharing platform based in Japan or Australia should either close access to EU users or have a legal representative within the Union regardless the size of the platform?

- Pursuant to Article 2(d), in the absence of an establishment in the Union, the assessment of a "substantial connection" to the Union is based on specific factual criteria. A significant number of users or the targeting of activities towards one or more Member States are examples of such factual criteria. Whether there is a "substantial connection" to the Union would have to be established on a case-by-case basis.
- Not every platform whose services may be available in the EU has a significant number of users or actually targets its activities to one or more Member States; the mere availability of the service does not mean that such service is targeting one or more Member States.

Q26. Article 14: Notice and action mechanisms

Article 14 obligates every hosting service to put mechanisms in place to allow individuals or entities to complain regarding specific items of information that they consider to be illegal, as well as obligates the hosting services to process the complaints. Could the Commission please elaborate on why this requirement is made of all hosting services rather than solely online platforms? Has the Commission looked into whether the applicable hosting services all have the technical ability to remove specific items of information or whether perhaps some would only have the ability to remove a wider array of content?

- Online platforms are essentially hosting service providers which not only store but also disseminate information to the public at the request of the recipient of the service (Art. 2(h) DSA).
- The DSA imposes the obligation to put in place a notice-and-action mechanism to all hosting service providers, not only platforms, regardless of their size, because it is considered as a minimum requirement which is necessary to ensure that users can effectively flag allegedly illegal content they encounter online. Given the importance of this objective and that the costs of putting in place such a mechanism can be reduced by using standardised technologies, this obligation is proportionate.
- Furthermore, other provisions, such as those on notices being sufficiently precise and adequately substantiated (Art. 14(2) and (3) DSA), as well as on the prohibition of general monitoring and active fact-finding obligations (Art. 7 DSA) also contribute to a proportionate approach on these matters.
- The DSA also promotes a proportionate approach to the tackling of illegal content online by noting that *"where it is necessary to involve information society services providers in tackling illegal content online, including providers of intermediary services, any requests or orders for such involvement should, as a general rule, be directed to the actor that has the technical and operational ability to act against specific items of illegal content, so as to prevent and minimise any possible negative effects for the availability and accessibility of information that is not illegal content"* (recital 26). Recital 22 makes clear that "the removal or disabling of access should be undertaken in the observance of the principle of freedom of expression".

Q27. Article 17 Internal complaint-handling-system and article 18 out-of-court dispute settlement

As we read article 17 and 18 they only provide recipients of the service with the possibility for internal complaint handling and out-of court dispute settlement. Could the Commission elaborate on the possibilities for a user to complain about a decision from the platform not to remove content, which is considered illegal by the user?

> Article 17 and 18 are applicable in relation to the decisions of online platforms to remove or disable access to the information. While the proposal does not require them to do so, online platforms may allow a user that sent a notice under Article 14 to submit an internal complaint or initiate an out-of-court dispute settlement when the platform decides not to take down the content. In any event, users should have the possibility to turn to the courts or other competent national authorities in such a case, in accordance with the relevant national rules.

Q28. Article 18 Out-of-court dispute settlement

Could the Commission elaborate on the jurisdiction concerning the body referred to in this article? For instance: can a recipient in country A refer a decision from a platform established in country B to a body in country A?

> Recipients of the service can select any out-of-court dispute settlement body certified by any Digital Services Coordinator regardless of the place of establishment of the service provider and the residence or place of establishment of the recipient.

Q29. Article 19: Trusted flaggers

We are currently looking into the exception of micro and small enterprises from the scope of the provisions. We are worried that illegal content will end up on the smaller marketplaces, if the] provision does not apply to them. Has the Commission made any assessments in this regard?

> Article 19 requires online platforms to take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers are processed with priority. The purpose of this provision is to speed up the processing of "trusted" notices, which is particularly relevant in case of larger service providers hosting a large amount of content and receiving a large amount of notices.
>
> Micro and small enterprises are not exempt from the notice and action mechanism of Article 14, which also requires the timely processing of notices. While trusted flaggers would not benefit from a 'priority channel' from these smaller service providers, their notices will still have to be processed and acted upon in a timely manner (as required by Article 14 DSA). The logic behind this distinction is that an online platform that is not a micro or a small enterprise, nor a 'mere' hosting service provider, might receive a higher number of notices and should, whilst still meeting the requirements resulting from Article 14, prioritise the treatment of those notices issued by trusted flaggers within the meaning of Article 19 DSA.
>
> Requiring smaller online platforms or hosting service providers that do not qualify as online platforms to invest in the necessary technical and organisational measures for trusted flaggers was judged to be a disproportionate administrative burden.

Q30. Article 22: Traceability of traders

While the requirements in Article 22 may very well be considered highly burdensome when imposed on smaller platforms, excluding the smaller platforms may on the other hand have negative consequences, where for instance fraudulent sellers migrate to these platforms. Has the Commission assessed the consequences of excluding micro- and small enterprises from the scope of this article?

- After a thorough impact assessment, the Commission concluded that the duties imposed by Art. 22 would constitute significant administrative, organisational and technical costs, and thus impose a significant financial burden for small and micro enterprises. One of the main problems identified in the proportionality test carried out in the Impact Assessment are legal barriers preventing smaller companies from scaling up and expanding. The Impact Assessment further shows that these barriers hit especially smaller online platforms that are dependent on larger players.
- More specifically, the costs related to compliance with Article 22 would mean:
  (1) Costs of technical design and maintenance consisting of a necessity to adapt internal systems to appropriate technical solutions
  (2) Costs related to administrative and organisational measures, lying in necessary costs to cover additional human resources
- However, nothing prevents small and micro companies from complying with the traceability of traders requirement under Article 22 on a voluntary basis.

Q31. Article 22: Traceability of traders

It is important that relevant authorities i.e. market surveillance authorities may require the information on traders for enforcement purposes. As we read article 22(5) it will be possible for national authorities to require such information. However, we are not sure how to understand the last part of article 22(5) cf. "any orders issued by Member States' competent authorities or the Commission for the performance of their tasks under this Regulation". Market surveillance authorities would have a great benefit of access to information on traders selling goods to the EU via online platforms. Since the online platforms are obligated to obtain different information on the traders, the online platforms should also be obligated to provide the information to any competent market surveillance authority that works under any EU product legislation. Therefore we would like the Commission to clarify, whether Member States' market surveillance authorities can require information as listed in article 22(1)(a-f) when the competent authorities makes decisions in accordance to any EU product legislation ?

- Market surveillance authorities can, where provided in EU or national law, request specific information from online platforms on the identity of individual traders under Article 9 DSA.
- The last sentence of Article 22(5) does not exclude such a request but specifies that platforms can disclose information to authorities based on:

a) an order under Article 9 for the purpose of determining compliance of the recipients of the intermediary services with applicable Union or national rules (this option can be used by market surveillance authorities); or

b) a request from competent authorities and the Commission for the purpose of their tasks provided for in the DSA, listed respectively in Article 41 and 52 DSA.

Finland

Q32 Article 15, Statement of reasons (art. 15 para 2 f)

According to Article 15 when a provider of hosting services decides to remove or disable access to specific items of information provided by the recipients of the service, the provider shall inform the recipient, of the decision and provide a clear and specific statement of reasons for that decision.

According to para 2 f) the statement of reasons shall contain information on the redress possibilities available to the recipients of the service in respect of the decision, in particular through internal complaint-handling mechanisms, out of court dispute settlement and judicial redress.

What is the "judicial redress" here? What is the judicial redress based on? Does the "judicial redress" reference to a civil law case based on the contract (or terms and conditions of the service) between the hosting service provider and the recipient of the service? Is the concept "judicial redress" correct here?

- 'Judicial redress' refers to the right for recipients of the service to have access to a national court, in the light of the fundamental right to an effective remedy and to a fair trial, as anchored in the EU Charter of Fundamental rights (Article 47). This primarily refers to the possibility of challenging the decisions of a service provider before a court in situations where the provider allegedly infringed the rights of the recipient under the DSA.
- Accordingly, whilst the disputes in question may indeed also be contractual disputes resolved by civil courts, that is not necessarily so, since, as indicated, the case may also turn on the alleged infringement of rights derived from the DSA. One could think, for instance, of an alleged failure by the provider to act diligently and objectively.
- Furthermore, Art. 15(2)(f) DSA may include, for example, information about the ways of contesting the order of a national authority that led to the removal of illegal content by the hosting service provider.
- Thus, the concept of judicial redress is used in a broad sense in the text to cover the different possibilities available at national level.

Ireland

Q33 Ireland is particularly concerned about Article 14 sub Article 3. It states that a hosting service can be considered to have knowledge of illegal material on its site based solely on the basis of the

opinion of an individual albeit an opinion held in good faith. We do not believe that this is a sufficiently robust basis for effectively fixing the service provider with liability for that material. Will the Commission consider dropping sub Article14.3. The point that the maker of the notice has alleged illegality and brought that to the attention of the service provider can be made in any attempt to hold the service provider liable in a court of law but to make a presumption of liability on the basis of one person's belief that something is illegal is to weight such a debate unfairly against the service provider. Alternately if the Commission will not remove sub Article 14.3, will they consider making the requirement in sub Article 14.2 para (i) stronger than merely to be based on the consideration of the individual or entity such as the necessity to cite the particular law that it is considered has been broken.

- Article 14(3) should be understood in conjunction with Recital 22, which makes clear that the hosting service provider can obtain actual knowledge or awareness through, in particular, notices *in so far as those notices are sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and where appropriate act against the allegedly illegal content*. As a consequence, the notice does not only need to fulfil the conditions under paragraph 2, but this information needs to allow the provider to reasonably identify the illegality of the content. The standard for 'sufficiently precise and adequately substantiated' notices is placed sufficiently high to protect the platform and the content provider from giving course to any abusive and deceitful, or simply mistaken, notices.
- Article 14(3) should not be understood is if a mere flag/allegation from the notice provider, as long as it contains elements listed in Article 14(2), would lead to actual knowledge in sense of Article 5 DSA.

Q34 The approach taken in Chapter 3 to base due diligence obligations on either the function of the provider or the reach of its service has benefits with regard to proportionality but may not be the most effective. Will the Commission reconsider introducing the element of risk that is created by certain situations particularly where those risks, if realised, are liable to result in very serious harm to large numbers of citizens or society as a whole. It is appreciated that the Commission has consulted with Europol as to the number of instance of finding groups making structural use of smaller platforms to carry out clandestine illegality and have been assured that that number is low. However, there is an alternative explanation which would be to suggest that such groups are particularly successful in such clandestine use. Furthermore as the authorities in the US are beginning to address these issues using a similar approach, there are already examples of extremist groups migrating their activities to smaller platforms.

- The approach in Chapter III reflects a careful proportionality and necessity analysis for the due diligence obligations imposed on the different types of service providers. This stems from an analysis of risks they bear, as well as of their capacity to intervene.
- Measures included in Sections 2 and 3 of Chapter III already provide for a step-change in the ability to tackle the spread of illegal content through providers that do not qualify as very large online platforms. Cooperation with trusted flaggers, for example, and reporting of serious criminal offences, are key measures for addressing such concerns.

- As regards micro- and small enterprises, the notice and action obligations, together with the obligations in relation to orders from national authorities, constitute both effective and proportionate regulatory obligations, considering the risks their services pose.
- This approach of differentiated obligations depending on the size of the service provider is a balanced approach to achieve the policy objectives of the proposed regulation. Moreover, small service providers that are not legally obliged to take certain measures – e.g. trusted flagger cooperation – can and are encouraged to voluntarily deploy the measures most appropriate for their specific case, and will benefit from the best practices and existent infrastructure, for example through standards, guidelines and codes of conduct. In addition, Chapter II removes significant legal disincentives for such small players to adopt the necessary measures, in accordance to their respective needs.

Q35 Finally, Ireland is particularly concerned to ensure that the ability to enforce against service providers who are responsible for infringements are not hampered by imprecision in the specifications in the obligations as set out in the Regulation. Instances of situations where this could happen are the use of the word "may" which suggests an optional approach in Article 29 to create what the Commission has confirmed in Working Party is considered to impose a requirement and the need to qualify certain requirements with qualitative elements such as at Articles 26 and 28. Will the Commission reconsider the way that due diligence obligations are expressed in the text to assist in ensuring that DSCs are able to enforce the Regulation effectively.

- In particular as regards Articles 26 to 28, the risk mitigation approach needs to preserve its adaptive nature, allowing for the appropriate measures to be tailored to each situation. Such interpretations are qualitative in their very nature and must be adjusted depending on elements like the specific risks, the type of platform, and the need to avoid unnecessary restrictions on the use of the service, taking due account of potential negative effects on the fundamental rights of their users.
- An exhaustive or prescriptive list of measures would not be case-specific or future-proof. As proposed, the rules can be adapted to emerging risks, as reflected in the publication of comprehensive annual reports by the Board (Article 27(2)) and the guidelines issued by the Commission in cooperation with Digital Services Coordinators (Article 27(3)). The guidelines will be anchored in public consultations and evidence-based and potentially also take account of independent research on the evolution of risks, as enabled through Article 31.

Romania

Q36 Chapter III Section 1 provides the rules applicable to all providers of intermediary services. Article 13 para 2 stipulates that para 1 shall not apply to micro or small enterprises. Should we understand that only the reporting obligations are excluded but not the action itself as provided in art.14 ?

- Yes, while micro and small enterprise would not be subject to the obligation laid down in paragraph 1 of Article 13, they would still need to comply with the obligations laid down in Article 14, as long as they are providers of hosting services within the meaning of the DSA (i.e. Article 13 applies to all providers of intermediary services, while Article 14 (and 15) apply only to providers of hosting services).

Q37 The provisions of Chapter III Section 3 are not applicable to micro or small enterprises (art.16), including art.21 (notification of suspicions of criminal offences). Could a MS regulate in the national law that also SMEs has the obligation to inform law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion?

- As noted above, as a matter of principle, Member States will not be allowed to adopt parallel national provisions on matters falling within the scope of, and exhaustively regulated by, the DSA, since this would affect the direct and uniform application of the regulation.
- The legal basis used, as well as the choice of the instrument (Regulation), already provide that the objective of the legislator is to ensure a high degree of harmonisation in achieving the balance between the proper functioning of the internal market and the definition of uniform rules for a safe, predictable and trusted online environment, where fundamental rights enshrined in the Charter are effectively protected (see Article 1(2) DSA). National legislation that alters the scope of the obligations laid down by the DSA, for instance by imposing heavier obligations on SMEs than those imposed by the DSA, would run against the harmonization objective underpinning the DSA.

Q38 Recital 43 stipulates that the exemption of micro- and small enterprises from those additional obligations should not be understood as affecting their ability to set up, on a voluntary basis, a system that complies with one or more of those obligations. Is this voluntary system in line with MS national criminal law systems?

- In order to avoid disproportionate burdens, Article 16 states that the obligations of Section 3 of Chapter III do not apply to online platforms qualifying as micro or small enterprises. Recital 43 explains essentially that, in as far as the DSA is concerned, this exclusion should not prevent the platforms in question from taking the measures set out in Section 3 on a voluntary basis.
- It cannot be stated in the abstract whether this approach is in line with national criminal law systems or not, since those systems – and the requirements they provide for - differ between them and may be case specific. In general, provided they are compatible with the DSA, the DSA leaves requirements resulting from national criminal laws unaffected.

Q39 Recital 68 provides that the refusal without proper explanations by an online platform of the Commission's invitation to participate in the application of such a code of conduct could be taken into account, where relevant, when determining whether the online platform has infringed the obligations laid down by this Regulation. If the participation is voluntary, why an explanation is needed and how come a refusal without explanation is taken into account when determining an infringement? Some examples of proper explanations will be helpful to understand the limits in the determination.

- Codes of conduct pursuant to Article 35 are intended to contribute to the proper application of the DSA, including as regards compliance with risk mitigation obligations by very large online platforms.

In this regard, measures taken in alignment with a Code of conduct may contribute to compliance with the obligations of the service provider as laid out in the DSA.

- The service provider may comply with its obligations under the DSA through other measures and means not stipulated under the Codes of conduct, and, consequently, is free not to participatee in a Code. However, a proper explanation in this regard may in some cases be important to facilitate the Digital Services Coordinator's or the Commission's precise assessment of the effectiveness of those alternative measures. Codes of Conduct meeting the aims specified in Article 35 DSA can be expected to alleviate burdens and facilitate compliance.

Q40 Article 18 regarding Out-of-court dispute settlement provides for institutional responsibilities. Can you explain what competencies need to have the Digital Services Coordinator in order to certify the out of court dispute settlement bodies? Can you explain how the body seeking certification from DSA will prove the conditions listed in par 2. ? RO considers the para 4. is unclear and burdensome. What is the purpose of having two types of certification and how the support of activities is provided "of some or all out-of-court dispute settlement bodies".

- Article 18(4) clarifies that Member States may decide to establish out-of-court dispute settlement bodies or to support the activities of existing out-of-court dispute settlement bodies. Under Article 18 Member States are not obliged to establish such bodies; their primary task under Article 18 is rather to certify - through their Digital Services Coordinators – bodies that applied for certification and that meet the requirements of Article 18(2).
- Therefore, there are not two types of certification under Article 18; rather, there is only one.
- Article 18(2) indicates that it is for the body applying for certification to "demonstrate" that it meets the requirements set out therein. The burden of proof is therefore on the body. The DSA does not specify precisely how a body can do so. That indicates that all reasonable means of providing the required proof are available to it. It will be for the Digital Services Coordinator concerned to assess whether the proof provided in a given case is sufficient.
- Member States cannot prevent out-of-court dispute settlement bodies established in their territory from applying to their Digital Services Coordinator for certification.
- The DSA does not prescribe how out-of-court dispute resolution bodies should demonstrate the conditions of Art. 18(2), but this would typically involve the qualifications and experience of the decision makers, statements on conflict of interest, presentation of the electronic accessibility, and the rules of procedure, including language regime, fees and expected duration of the dispute settlements.
- Article 39(1) provides a general requirement for Member States to "ensure that their Digital Services Coordinators have adequate technical, financial and human resources to carry out their tasks."

Q41 Having regard to the Codes of conduct for online advertising, should the aim "for a fair environment in online advertising" as prescribed in art. 36 be read in conjunction with the principle of fairness as codified in the DMA ? Also, does the reference to competition law mean that these [Codes of conduct] will need to take into consideration the relevant national and EU-level case-law under art. 102 TFEU, in terms of online advertising ?

- While DSA and DMA are coherent and part of the same legislative package, they have different objectives and their scope is different. Therefore, the objective of fairness in Article 36 DSA should not be understood as being equal to the objective of ensuring fair and contestable markets in digital sector.
- As with regard to all activities by undertakings on the market, also in the context of drawing up codes of conduct under Article 36, signatories need to ensure that their behaviour and the Code of Conduct as such do not lead to restrictions of competition within the meaning of Articles 101 or 102 TFEU as interpreted by the Court.

Czech Republic

Q42 Article 12: Paragraph 2 says that the terms and conditions (TaC) shall be applied and enforced with regard to the fundamental rights, however, how is it ensured that the TaC themselves respect EU principles? Unless resolved, it creates potential for conflict.

- Terms and conditions must comply with applicable Union and national law. Article 12 leaves such regulatory obligations resulting from other legal instruments unaffected.
- Article 12 does not regulate the scope of potential restrictions on the use of their service that the providers may establish through their terms and conditions and does not limit the freedom of contract in this respect, but instead imposes certain obligations to ensure transparency, the protection of the users and the avoidance of arbitrary or disproportionate outcomes.
- All restrictions must be clearly and unambiguously presented in the terms and conditions, and must be enforced in an objective and proportionate manner. Moreover, pursuant to Article 15(2)(d)-(e) providers of hosting services must provide a specific statement of reasons for their decisions to remove content or suspend an account, either by making a reference to the legal ground relied on or a reference to the contractual ground relied on, and by explaining why the information is considered to be incompatible with that ground.
- Hence, Art. 12 should be read in conjunction with other provisions of the DSA, providing users with redress and appropriate information to exert their rights (e.g. statement of reasons in Article 15, but also redress mechanisms in Articles 17 and 18).

Q43 Article 18 + rec. 44: What mechanism and at what stage can the platform use in case it disagrees with the outcome of the out of court dispute result? How can it bring the matter to court?

- Article 18(1) DSA provides that decisions taken by the out-of-court dispute settlement bodies are binding upon the online platforms. The provision does not contain any particular rules on the online platform's judicial redress against such a decision.
- Since this matter is not expressly regulated, it falls within the procedural autonomy of the Member States, subject to the EU law principles of effectiveness and equivalence and the requirements resulting from Article 47 of the Charter.

Q44 Online advertising transparency (art. 24 and 30): If the advertising system on the platform is run by a third party, i.e. the platform does not decide about the content of the advertisement, Cion confirmed that the platform is liable for the advertisement according to Article 24. As raised by CZ at the WP, how can the platform receive this information from the third party? Which system is

currently working in practise? Our stakeholders were not aware of such a system in place. (CZ has raised it at WP but the justification provided by Cion was not convincing enough for us.) As mentioned at the working party, we are of the opinion that repositories in Article 30 may reveal business secrets and knowhow of advertising companies for example by having the possibility to see the sequence of different adverts on one product in time or by revealing the profiling techniques used. Therefore, we see this obligation as unnecessary and potentially harmful. How can the DSA ensure that business secrets are not revealed? Furthermore, the declared research purpose does not seem justified enough given the big dangers associated with giving out business secrets.

- As regards the content of advertisements served on an online platform, Articles 24 and 30 do not regulate the liability for the content of the advertisement. Under Article 24, the platform bears an obligation to 'ensure that the recipient of the service can identify' the information requested. Under Article 30, the very large online platform must 'compile and make publicly available' the respective information. As such, the legal obligation is to ensure access, not to intermediate or host the information.
- There are already some industry examples for providing such information to users, both as regards platforms that maintain their own advertising systems, and for intermediated banner or in-app advertising (e.g. https://youradchoices.com/)
- As regards Article 30, there are also industry examples, either of platform-pushed information, or third party collection of data on a sample-base. Information required in Article 30 is relatively limited, both in scope and in time it is made available, and purposely excludes business-sensitive information such as price paid or received for the display of ads. At the same time, the public policy benefits are considerable, for example in allowing the detection of illegal ads, of discrimination of vulnerable groups, or manipulation and misuse of advertising to drive disinformation campaigns.

Estonia

- Q45 Are the digital services providers responsible for supervising that an out-of-court dispute settlement body is conformity with the criteria set out in Article18(2) after they have been certified? If not, how are their independence and impartiality guaranteed?

    - The out-of-court dispute settlement body needs to comply with the criteria set out in Article 18(2) at all times. The DSA does not expressly provide for a specific supervisory responsibility, but the "effet utile" of this provision would be endangered if the Digital Services Coordinator could not revoke the certification if it becomes aware that the body does not meet the criteria anymore.
    - For instance, the parties may inform the relevant Digital Services Coordinator of their concerns about the independence, impartiality or any other criteria set out in Article 18(2). The latter may then take appropriate steps to verify that the applicable requirements continue to be met and if not, revoke the certification where appropriate.

- Q46 Are the decisions considered to be authentic instruments under Brussels I Regulation, or if not, what is the legal character of these decisions and the mechanism for their cross border enforcement?

[To be checked/clarified by DG JUST]. The out-of-court systems laid down in the DSA are indeed certified by public bodies (the DSCs). The decision binds the online platform concerned (Article 18(1)) and hence violations of the terms of the decision could trigger its liability, and may be enforced before the national courts..

Poland

art. 18

Q47 What is the relation of the procedure described in art. 18 to already exisiting consumer regulations on ODR/ADR?

The main purpose of Article 18 is to oblige online platforms to engage, in good faith, with the certified out-of-court dispute settlement body of the recipient's choice, the decision of which shall be binding upon them. This provision thus creates a specific procedure, whereby the certification of the body by Member States in view of the requirements listed in Article 18(2) is a key element. In that regard, Article 18(4) explicitly allows Member States to establish out-of-court dispute settlement bodies or support already existing bodies, including potentially those that have been established on the basis of other rules on alternative dispute resolution, although any such steps taken by a given Member State may not affect the certification activities of its Digital Services Coordinator under Article 18(2). Article 18(6) and Recital 45 clarify that the rules of the DSA on out-of-court dispute settlement are without prejudice to Directive 2013/11/EU of the European Parliament and of the Council, including the right of consumers under that Directive to withdraw from the procedure at any stage.

art. 24

Q48 How to define intermediary service provider in the area of online advertising? Is every online advertiser an intermeriary? Is the term „advertising intermediation services" in art. 34.1f) od DSA synonymous with the term „advertising intermediation services" mentioned in art. 2.2 h) of DMA?

- In the DSA, the concept of advertising intermediaries is explained in recital 70, referring to any intermediary that connects publishers with advertisers. This is intended as a broad notion, allowing to remain technology-neutral and accommodate any model of online advertising. Such services can cover, for example, supply side platforms, demand side platforms or ad exchanges. Advertisers themselves are not considered to be advertising intermediaries, but rather content providers.
- While both the DSA and DMA make reference to advertising intermediaries and advertising services, respectively, there is a conceptual difference of scope: whereas the DSA notion does not require a given link between the advertising service and the platform service (as publisher of the advertisement), advertising services in the DMA are provided by a core platform service listed in Article 2(2) points a) to g).

art. 27

Q49 Will it be possible to impose an obligation on a VLOP to take additional measures to mitigate the identified risks? How will this obligations be enforced?

- Article 27(1) imposes an obligation on the service provider to put in place 'reasonable, proportionate and effective mitigation measures' for the identified systemic risks. The list of measures provided in paragraph 1 represents broad categories of measures, whereas the requirement refers to measures addressing the specific risks identified.
- The risk mitigation measures will be assessed by independent audits, including recommendations for further or different measures, as appropriate. The choice and applications of the measures is supervised by the DSC and the Commission to ensure that the requirements of the DSA are complied with. Further details on the enforcement of the measures are provided in reply to question 4.
- As regards additional measures, the Digital Services Coordinator of establishment, as well as the Commission, have powers to impose interim measures and remedies in the context of the non-compliance procedure or to adopt commitments decisions.

Luxembourg

Q50 In article 14, can the Commission confirm that a valid notification, meeting the requirements of paragraph 2, automatically engages the liability of the intermediary because it is deemed to have actual knowledge? Can the Commission explain why this change to the e-Commerce Directive was necessary (from removal-based liability to procedure-based liability)?

- Article 14(3) should be understood in conjunction with Article 14(2) and with Recital 22, which makes clear that the hosting service provider can obtain actual knowledge or awareness through, in particular, notices *in so far as those notices are sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and where appropriate act against the allegedly illegal content*. A notice is generally considered to be sufficiently precise and

adequately substantiated, where it meets the specific requirements of points (a) to (d) of Article 14(2). The standard for 'sufficiently precise and adequately substantiated' notices results from the case law of the Court of Justice of the EU related to Article 14(1) of Directive 2000/31, and hence will be relevant for the interpretation of Article 5 DSA.

- Accordingly, although in this regard the DSA is more specific than current law (e-Commerce Directive, as interpreted in the Court's case law), there is no fundamental change. The further specifications provided for in the DSA on this point serve to increase legal certainty and are a logical consequence of the decision to lay down rules on notice and action mechanisms.

Q51 Can the Commission elaborate how the delegated act in Article 25(3) on VLOPs which could modify the scope of application of the DSA, does not modify essential elements of the DSA, which would be contrary to the Treaty and the Comitology Regulation? Where does the provision define the objectives, content, scope and duration of the delegation of power?

- The scope of delegation in Article 25 meets the requirements of the Treaty (Art. 290 TFEU) and existing case law as regards the delegation of powers to the Commission. The Comitology Regulation (Regulation 182/2011) is not applicable to delegated acts.
- In particular, the definition of the power conferred upon the Commission under Article 25(3) is:
- **sufficiently precise**: Article 25(3): adoption of a delegated act to lay down a specific methodology for calculating the number of average monthly active recipients of the service. Such methodology shall specify how to determine Union's population and criteria to determine average monthly active recipients of the service. In other words, the legislative act defines the criteria, scope and objectives of the delegated act, as the latter shall merely specify the specific methodology that applies the basic criterion laid down in legislation (average monthly active recipients) in view of different accessibility features of different services. The duration is defined in Article 69 DSA.
- **indicates clearly the limits of the power,** i.e. inability for the Commission to adopt delegated act if conditions in Article 25 (see above) are not met;
- enables the Commission's use of the power **to be reviewed by reference to objective criteria fixed by the EU legislature**, i.e. criteria are set in Article 25 and appropriate safeguards are set in Article 69.
- The scope of the DSA will not be impacted by the specific methodology, which should, in addition to the abovementioned requirements, follow the clear policy intent set inter alia in recital 53 for measuring the actual 'reach' of a platform 'in facilitating public debate, economic transactions and the dissemination of information, opinions and ideas and in influencing how recipients obtain and communicate information online'
- The scope of the delegated act refers to the specific methodology for calculating the threshold of average active monthly users: this includes precise information for determining the Union's population, and precise criteria for computing the number of users to account for the different manners in which a 'user' can be technically counted.
- Accordingly, Article 25(3) specifies the objectives, content and scope of the delegated power and Article 69 provides the necessary details on the exercise of the delegation.

Q52 Given that the scope of the DSA appears to be broader than that of the AVMSD - including inter alia political advertising - could the Commission confirm that commercial advertising would

fall under the AVMSD and only political advertising would be assessed under the DSA? (cf. Art 24 DSA)

- Obligations under Article 24 DSA are different from obligations included in the AVMSD on audiovisual commercial communications, in particular as regards information requirements in Article 24 points b) and c). In addition, the scope of the services covered as video-sharing platforms in the AVMSD is narrower than the broader notion of online platforms in the DSA.
- At the same time, not all types of 'audiovisual commercial communications' within the meaning of the AVMSD Article 1, point f) are necessarily advertisements within the meaning of the DSA, since the latter contains its own definition (Art. 2(n) DSA).
- The DSA applies to all types of advertisement, including commercial communications, covered by the definition of advertisement in Article 2(n). However, where there is an overlap in scope and obligations, the DSA rules are without prejudice to the AVMSD (see Art. 1(5) DSA) – this can be the case as regards obligations on video-sharing platforms to take appropriate measures to ensure that audiovisual commercial communications are readily recognisable as such.

France

Q53

La lutte contre la diffusion en ligne de contenus illicites peut être efficacement accompagnée par des actions visant à assécher le financement, très souvent issu de la publicité, de ces contenus selon la logique du « follow the money ».

Le risque de monétisation de contenus illicites peut être considéré comme figurant parmi les « risques systémiques » définis aux articles 26 et 27 du « Digital Services Act ».

Ne serait-il pas souhaitable que la section 4 inclue, sous une forme à convenir, des obligations appropriées à la charge des très grandes plateformes en ce qui concerne leur politique de prévention visant à assurer que la publicité n'est pas associée à des contenus illicites (« Brand safety ») ?

- Measures to demonetise content can be covered in Article 27(1) point b); where reasonable, proportionate and effective, these could take the form of 'brand safety' type of implementations, but are not limited to this model.

Q54, relative au caractère ciblé des obligations :

Si la plupart des obligations du DSA sont formulées comme portant sur des processus, certaines dispositions sont formulées comme portant sur le traitement d'une notification ou d'un recours individuel.

Le DSA prévoit-il de sanctionner uniquement les manquements systémiques ou bien prévoit-il des sanctions pour les manquements individuels ?

The DSA establishes rights and obligations directly applicable to platforms and users of the services, generally linked to the set-up and functioning of systems to handle illegal content. In general, these provisions may be directly actionable in particular where they confer individual rights on the recipients of

services. It will be in principle for the Member States to establish the system of remedies safeguarding the individual rights derived from the DSA (which in any case does not regulate the illegality of the individual content as such). Moreover, in line with other rules that can be subject to both private and public enforcement (such as consumer protection rules), the enforcement system of the DSA by public authorities is not meant to pursue the protection of individual rights/interests to the respect of the obligation, but rather to ensure "adequate oversight and enforcement" (Recital 72). Similarly, recital 81 on complaints stresses that *"[l]es plaintes pourraient donner un aperçu fidèle des préoccupations suscitées par un fournisseur de services intermédiaire déterminé quant au respect du présent règlement et pourraient également informer le coordinateur pour les services numériques de toute autre problème de nature transversale* » and therefore Article 43 establishes certain rights related to the filing and good administration in handling complaints, but does not establish a right to enforce through public enforcement the rights of individuals eventually breached by the platform in a specific case.Public enforcement indeed should rather pursue the task to ensure the general interest to adequate oversight and enforcement of the DSA rules in line with the principles of effectiveness and proportionality.

Q55

La proposition DSA ne vise expressément la protection des consommateurs, pour ce qui concerne les contrats qu'ils concluent avec des professionnels par l'intermédiaire des plateformes en ligne, qu'à son article 22 relatif à la traçabilité des vendeurs. Cet article complète utilement les obligations de transparence inscrites à la directive (UE) 2011/83 relative aux droits des consommateurs, en particulier son article 6 bis. Néanmoins, les autorités françaises peinent à comprendre en quoi cet article suffirait à répondre aux risques sérieux posés par les places de marché en ligne pour la santé et la sécurité des consommateurs, ainsi que pour l'effectivité de leurs droits. Elles rappellent, à cet égard, l'objectif que s'est fixé la Commission dans son nouvel agenda « consommateur » d'arriver au même degré de protection des consommateurs en ligne qu'hors ligne.

Par conséquent, la Commission peut-elle indiquer dans quelle mesure elle a envisagé ou non des obligations supplémentaires pour les places de marché en ligne, notamment, pour la prévention et la gestion des offres de produits dangereux ou, encore, de diligence face à des vendeurs peu scrupuleux, afin de permettre l'application effective des droits légaux des consommateurs et de garantir la sécurité des produits et s'il ne convenait pas de consacrer une section du chapitre 3 aux opérateurs de places de marché compte tenu du rôle spécifique qu'ils jouent dans les relations entre professionnels et consommateurs ? Si oui, la Commission peut-elle faire part de l'analyse d'impact réalisée (ou des projections) afin d'éclairer pourquoi elles n'ont pas été retenues ?

- The concept of "online marketplaces" is evolving and different business models converge. A static definition could undermine the effectiveness of some obligations. For instance, as noticed in the Europol and EUIPO report on "Intellectual property Crime Threat Assessment 2019"[4], social media platforms have emerged as key actors for the trade of counterfeited products. The Commission has

[4] Europol and EUIPO "Intellectual property Crime Threat Assessment 2019", p.37

therefore decided not to include a narrow and static definition but rather to impose the relevant obligations on all online platforms allowing traders to conclude distance contracts with consumers.

- Articles 5(3) and 22 DSA aim at ensuring a safe, trustworthy and transparent online environment for consumers. On the one hand, in the event where a specific item of information is presented in such a way that an average and reasonably well-informed consumer believes that the information or the product or service that is the object of the transaction in question is provided by an online platform, the liability exemption provided for in Article 5(1) will not apply. On the other hand, Article 22 ensures that consumers can know the identity of and other information relating to traders with whom they are concluding distance contracts and that competent authorities can enforce the law more easily by having access to relevant information.
- The DSA is without prejudice to sector-specific legislations, including consumer protection laws (Art. 1(5) DSA). In this regard, the Commission is currently working on a revision of the General Product Safety Directive, which is aimed at ensuring that product safety rules can be effectively enforced also in the online environment.

Netherlands

The Netherlands appreciates the opportunity provided by the Portuguese Presidency and European Commission to submit written questions with respect to Chapters III of the DSA. Please find below the three questions we wish to submit for further explanation by the Commission:

Article 22: Know Your Business Customer (KYBC) obligation

Q56 Article 22 requires online platforms - that enable consumers to conclude distance contracts with traders - to obtain certain information from them prior to these third parties being allowed to use the platform; **How is it to be decided whether that third party is a trader or (just) a consumer?** Can this be based on the declaration made to the online platform by the third party as required in the new Article 7(4)(f) of the UCPD, as amended by the Directive (EU) 2019/2161 (the 'Omnibus' Directive)? And would this article supersede article 22.2, which additionally compels online platforms to verify the 'reliability' as to whether the submitted declaration of the trader indicating it is either a professional trader or simply a consumer?

- A service provider falling within the scope of Article 22 must ensure the traceability of any third party, irrespective of whether it is a natural or legal person, which falls within the definition of a trader (Article 2(e))). In assessing whether a person is a trader, the services provider may take into account, in particular, the declaration provided in accordance with Article 7(4)(f) of Directive 2005/29/EC (Directive on Unfair Commercial Practices) as amended by Directive 2019/2161/EU (Omnibus Directive).
- The obligation for online platforms to make reasonable efforts to verify the reliability of the information provided by traders operating on their platforms is limited to the items of information mentioned in Article 22(2) DSA. This obligation is further explained in Recital 50 DSA.
- Under Article 22(2) of the DSA, the online platform is required to verify the reliability of the information referred to in points (a), (d) and (e) of paragraph 1. Declarations requested under the Consumer Right Directive or the Directive on Unfair Commercial Practices are therefore not included. Directive 2005/29/EC on unfair commercial practices has specific blacklisted practices prohibiting traders from pretending that they are non-traders. This would apply in the case of a

false declaration of being a non-trader under the Consumer Right Directive (Article 6a(1)(b)) and the Directive on Unfair Commercial Practices (Article 7(4)(f). The DSA leaves the rules of EU law on consumer protection unaffected (Art. 1(5) DSA).

Article 25: Very large Online Platforms (VLOPs)

Q57 It is unclear which criteria will be used to determine if an online platform has on average 45 million monthly active recipients of its service. Although we appreciate the Commission's intention to base the definition on an adjustable threshold that takes a percentage of the EU's population as its starting point it does mean that it is unclear who might be covered under the provisions for VLOPs. The Commission has provided some insights during the CWP of 22 February but that still left questions unanswered. **Can the Commission share insight into its latest thinking of the criteria which might define what an active recipient of a service is, how individual companies and/or groups will be treated, or otherwise share the available data & sample of services that it has used as a basis for her claim that it will encompass 20+ services?**

- Further explanations on the reasoning for the further implementation of the definition and precision through delegated acts is presented in the reply to question 51 above. The technical definitions will need to specify the methodology 'taking into account different accessibility features' – i.e. accounting for the different types of access rights on different platforms and in line with the objective pursued under Recital 53.
- Available data on user base of average monthly unique users of platforms is approximate and is presented on p. 65 of the annex to the Impact Assessment for the Digital Services Act, including graphic metadata. This is based on SimilarWeb data and cannot be taken as absolute figures, in particular bearing in mind that there is no agreed methodology as per Article 25 DSA.

Article 26: Systemic risk assessment VLOPs

Q58 The Netherlands favors using uniform conceptual definitions across different EU platforms and policies. **Can the Commission explain why the definitions given in the European Democracy Action Plan were not used for the type of systemic risks mentioned in art. 26(1)(c)?**

- The European Democracy Action Plan explains the differences between substantially different phenomena such as misinformation, disinformation or other types of coordinated efforts and foreign interference, and explains the need for different policy responses to these phenomena, in accordance with fundamental rights and democratic standards.
- In coherence with this approach, Article 26(1) point c) DSA does not seek to provide a legal definition of disinformation. It provides the parameters for a particular category of significant systemic risks stemming from the intentional manipulation of a service with actual or foreseeable negative consequences on a series of public policy-related issues. By the nature of the manipulative practices, very large online platforms are best placed to assess the risks and to design and implement measures to address the manipulation of their services and mitigate the risks, subject to supervision by public authorities as specified in Chapter IV DSA. As such, Article 26(1) point c) DSA is somewhat flexible in terms of techniques and behaviours covered, in light of evolving risks.

Hungary

Q59 With regard to Article 30 (2) (b), under additional online advertising transparency rules, very large online platforms will have to make publicly available a repository containing the information on advertising, including the name of the advertiser as well. However, with regards to Article 24, online platforms that display advertising on their interfaces will not have to disclose data on the advertiser, it is sufficient to state that the advertiser is a natural person. **We would like to ask for further clarification on the reason for the difference between the two articles.**

- There is no intention to distinguish between the two articles as regards the disclosure of the advertiser. Indeed, the user should see the name of the advertiser when they are presented an advertisement on an online platform, as per the requirement in Article 24 point b) DSA. The same information should also be included in the advertising repository, pursuant to Article 30(2) point b) DSA. This is also consistent with the obligations provided in Article 6 point b) of the E-Commerce Directive.

Italy

Q60: on Art.12 para 2:

The Copyright directive refers to: "high industry standards of professional diligence", which is the rational for a different wording in art. 12.2?

- Article 12(2) DSA applies horizontally and requires all intermediary service providers to apply any restrictions contained in their terms and conditions in a diligent, objective and proportionate manner. With regard to those restrictions, they must also provide information in those terms and conditions (Art. 12(1) DSA). Due to its horizontal nature and the different content and context of

Article 12 DSA as compared to Article 17 of the Copyright in the Digital Single Market Directive (Directive 2019/790), this provision does not refer to industry standards.

Q61 on Art. 20, para 3, letter (d): "…the intention of the recipient, individual, entity or complainant." How could online platforms and online services providers check "the intention"?

- See the response to Q5 above. The provider needs to assess the intention relying on the available relevant facts and circumstances. This can include, for example, the frequency of misuse or the statements of the recipient, individual, entity or complainant, for instance signalled by a high number of complaints. While the intention of a person is a subjective element, the provider needs to assess it in an objective and non-arbitrary manner. If the apparent facts and circumstances do not allow the provider to determine the intention, this aspect will not be taken into account.

Q62 on Art. 28 para 4: *"[…] Where they do not implement the operational recommendations, they shall justify in the audit implementation report the reasons for not doing so and set out any alternative measures they may have taken to address any instances of non-compliance identified."* What happens if these alternative measures are not deemed sufficient: sanctions?

- Audit reports issued by the independent auditor may include recommendations the very large online platform must take due account of, in view of taking the necessary measures (Art. 28(4) DSA). However, the very large online platform remains at all times responsible for compliance with the DSA, and the independent auditor does not substitute the role of the supervisory authority.
- Under Article 28(4), the very large online platform will have to explain why it did not implemented a particular audit recommendation. They may make this information public and transmit it to the competent Digital Services Coordinator and the Commission.
- The measures taken by the very large online platforms to comply with their obligations under the DSA are supervised by the Digital Services Coordinator of establishment and the Commission in accordance with the rules set in Chapter IV. Failure to comply can lead to the initiation of a procedure for non-compliance and the imposition of penalties.