Council of the European Union
General Secretariat

Brussels, 17 February 2021

Interinstitutional files:
2020/0361 (COD)

WK 2289/2021 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: Presidency Selection of questions sent by Member-States on Chapter I and II

Presidency Selection of questions sent by Member-States on Chapter I and II

Recitals

Recital 12

1. Please clarify the term immaterial in the context of recital 12) "... In this regard, it is immaterial whether the illegality of the information or activity results from Union law or from national law that is consistent with Union law and what the precise nature or subject matter is of the law in question."

Use of a word "immaterial" in recital 12 of the proposal for the Digital Services Act ("DSA") should be understood in a sense of "irrelevant" in relation to the fact whether the illegality of particular information or activity is based on EU or national law; while the latter one has to be consistent with EU law. In other words, both of the above mentioned legal basis could be used to determine illegality of the particular information/activity.

Recital 14

2. Recital 14 states that Interpersonal Communications Services as defined under Directive (EU) 2018/1972 (European Electronic Communications Code) fall outside the scope of the Regulation. However, this seems not to have been replicated within the articles of the Regulation. Could the European Commission clarify?

Firstly, as the Commission noted during the Council Working Party meeting, this part of the recital 14 contains a mistake: Interpersonal Communication Services as defined under Directive 2018/1972 fall within the scope of the Regulation. The intention of the Commission was to include wording that …"interpersonal communication services fall outside the scope of definition on online platforms." This mistake should be clarified either when issuing corrigendum to the text of the proposal (together with corrigendum to all translations into official EU languages) or during the legislative process.

Secondly, also elsewhere in the recitals the proposal gives examples of services that should be understood as falling within the scope of the Regulation (e.g. recital 27). These examples should be perceived as illustrative and non-exhaustive, clarifying the manner in which the corresponding article of the Regulation is to be interpreted. In the context of recital 14, the Commission perceived it important to clarify further duties of some information society services providers that might be understand as being involved in "dissemination to the public". Correct wording of the recital should clarify that interpersonal communication services approach content differently from the other service providers quoted in the recital and do not disseminate it publicly.

Recital 26

3. It is important to act on illegal content and focus action on the actor who has the best technical and operational ability to act and to minimize any negative effects. Is availability and accessibility to legal content (not illegal content), which has been removed, the only negative effect?

The purpose of this wording is to recall that, generally speaking, requests or orders should address the information society service provider which is best-placed, so that the request or obligation is specifically targeted, balanced and proportionate and unintended consequences are avoided. In this regard, the recital aims to clarify that, as a general rule, some intermediary service providers, mostly those establishing and facilitating the underlying architecture and proper functioning of the Internet, do not have the technical possibility to approach and tackle individual items of illegal content online to minimize potential negative effects. Requesting or ordering, for instance, internet service providers to act might be therefore, in some cases, be disproportionate and affect negatively fundamental rights and legitimate interests of other affected parties.

Chapter I

Article 1

4. Does the DSA pursue the goal of full harmonization so that the Member States are not allowed to make any regulations at national level that go beyond or deviate from those rules? If so, in which precise areas (scope of application) would there be scope for Member States' regulation (e.g. national reporting systems in case of a criminal offence, additional requirements for complaint filing systems, fixed timelines for deletion of illegal content)?

Being a Regulation, the DSA pursues the goal of harmonization for the issues covered by it. Member States shall therefore not impose on providers of intermediary services within the meaning of the DSA further obligations by way of laws, regulations or administrative actions for the matters falling within the scope of, and exhaustively regulated by, the DSA.

For example, the DSA harmonizes all aspects of the notice and action procedures across the EU (Art. 14). Rules on notice and action laid down in the DSA provide for a full harmonization of horizontal notice and action mechanism, which includes any aspect of such horizontal mechanism that is considered necessary to ensure safe, predictable and trusted online environment in full respect of fundamental rights. However, as another example, although it does contain certain rules in this regard, the DSA does not exhaustively regulate orders to act against illegal content (Art. 8). That is because Article 8(1) makes it clear that the legal basis to issue such orders is to be found in national law (or other acts of Union law). Moreover, Article 8(4) expressly states that the article is without prejudice to requirements under national criminal procedural law in conformity with Union law).

This is without prejudice to specific provisions under national legislation that may pursue a different objective and regulate issues not falling within the scope of the DSA. In respect of such issues, the DSA leaves the possibility of national legislators to regulate them unaffected. In any event, such national laws must comply with other provisions of EU law. In particular, if they restrict cross-border provision of information society services, they must comply with the conditions under Article 3 of the E-commerce Directive 2000/31/EC ("ECD").

5. Will Member States be free to take measures at national level, e.g. to promote cultural and linguistic diversity and to ensure the protection of pluralism provided for in Art. 1(6) of the eCommerce Directive (see recital 9)?

The ECD establishes that "this Directive does not affect measures taken at Community or national level, in the respect of Community law, in order to promote cultural and linguistic diversity and to ensure the defence of pluralism". As the ECD's rules on country of origin (Article 3), prior authorisation (Article 4), commercial communications (Article 6), etc., continue to apply, this reference remains unaltered.

The DSA is not intended to interfere with Member States' competences regarding cultural and linguistic diversity or media pluralism. The DSA will provide a horizontal framework and will only complement, not affect the sector-specific rules referred to in its Article 1(5) – such as the AVMSD – which should prevail as lex specialis over the new Regulation there where the scope of both instruments coincide (recital 9).

6. The text provides that the regulation lays down *''harmonized rules on the provision of intermediary services in the internal market''…'' in particular''* The bundling of diverse problems as copyright infringement, illegal speech, advertising under the same umbrella of '' intermediary services'' could be problematic. Experience has proven that the difference between these problems justify differences in the regulatory approach (telecoms, audio-video and e-commerce have their own regulatory frameworks) thus a precise scope is needed to justify and explain the intention of the Regulation. We wish to understand what message we provide with the expression "in particular", in fact what do we regulate?

The scope of the DSA follows the similar, horizontal approach to the twenty-year-old ECD, although the DSA is more narrowly targeted at intermediary services. Also some telecoms and some audiovisual services are information society services (covered by the ECD) or even intermediaries, today.

As regards the types of intermediary services, the DSA – due to its horizontal nature – covers them all to a certain extent. However, within Chapter II (liability rules), the DSA carries on the established differentiation between different services, and under Chapter III on the due diligence obligations, the DSA follows an asymmetric approach, distinguishing between categories for a tailored and proportionate intervention.

On the other hand, as regards the type of content (e.g. copyright protected works, advertising, hate speech etc.), the DSA remains neutral – as much as the ECD is neutral and horizontal in this respect. The DSA aims at establishing a horizontal, procedural framework, and the definition and regulation of specific types of illegal content is left to national or other EU law.

In fact, the DSA is designed in a way to leave space for the Union legislator to provide for specific rules on specific areas that require different or complementary regulatory approaches.

The expression “in particular” in the second sentence of Article 1(1) of the DSA specifies the foregoing sentence, which states in a general manner what sort of rules the DSA lays down. As such, the second sentence lists the three main issues regulated. The use of the expression “in particular” indicates that the list is meant as a high-level summary and is not exhaustive, in the sense that rules on general and ancillary issues are not listed, notably “General provisions” (Chapter I) and “Final provisions” (Chapter V).

7. Paragraph 1c) provides that the Regulation establishes *''rules on the implementation and enforcement of this Regulation, including as regards the cooperation of and coordination between the competent authorities''.* Read together with the provisions of Article 8 and 9 could raise some questions about the legal basis.

Articles 8 and 9 do not exhaustively regulate the validity and procedure for issuing orders, which remains regulated by the specific legal basis (if any) underpinning them at national or European level. The two articles only set out certain complementary requirements applicable in situations where such a legal basis exists and the national judicial or administrative authorities concerned decide to exercise their powers resulting from that legal basis. The overall aim is to ensure that any such orders can be complied with in an effective and efficient manner, so that the authorities can carry out their tasks, the providers are not disproportionally burdened and the rights and interests of third parties are not unduly affected (recital 29). Furthermore, recital 33 recalls that such orders in principle do not constitute restrictions to the cross-border provision of intermediary services pursuant to Article 3 ECD. This is fully in line with the objectives of the Regulation spelled out in Article 1 as well as with the proposed legal basis (114 TFEU).

Article 1 (5)

8. Could the Commission further summaries for which articles in which legislation is DSA *lex specialis* and *lex generalis*?

The DSA is intended to be the general framework regarding liability and due diligence of providers of intermediary services. It is without prejudice to the acts of EU law referred to in Article 1(5). As regards other sector-specific EU legislation, whether Regulation or Directive, the EU legislator may decide to provide that its provisions prevail over the conflicting DSA provision. At the same time, the DSA is complementary in nature: for issues not (or not fully) covered by the sectoral legislation referred to in Article 1(5), the relevant DSA provision will apply as a complement. This is expressed in the "without prejudice" formulation and explained in recital 9.

At the same time, in some sector-specific EU legislation, its rules apply "without prejudice to Articles 12 to 15 ECD" (GDPR, AVMSD…). Following Article 71 DSA, "references to Articles 12 to 15 of Directive 2000/31/EC shall be construed as references to Articles 3, 4, 5 and 7 of this Regulation, respectively". In that respect, such rules should still apply without prejudice to the relevant DSA provisions. At the same time, for instance Article 28b AVMSD provides for specific obligations to vídeo-sharing platforms which apply as lex specialis to the proposed DSA.

Where secondary law instruments derogate from Article 14 ECD (as it is the case of Article 17 of the Copyright Directive), this remains unaltered under the DSA. In other words, that derogation continues to apply, also in relation to Article 5 DSA.

9. Could the Commission provide a table explaining for each legislation listed in Article 1(5) how the articulation with the DSA would work? I.e. is the DSA « without prejudice » to specific provisions, or entire issues? Is there complementarity or exclusivity between the DSA and these other texts?

The purpose and objective of Article 1(5) is to clarify that in circumstances where sector-specific rules lay down specific regulatory solution that deals with the same subject matter as the proposed DSA, those rules remain unaffected. On the other side, this does not exclude the application of the horizontal rules of the DSA on a complementary basis. For example, if the provider of online intermediation service, such as for example an online marketplace, would decide to suspend the service to its business user, independently of the obligations under the DSA, it would need to provide statement of reasons based on Article 4 of the P2B Regulation. However, if the same provider of online marketplace would suspend the service to end user, it could suspend its service only temporarily and it would not be subject to Article 4 of the P2B Regulation, but rather Article 20(4) of the DSA.

Another example is Article 28b of the AVMSD, which obliges providers of video sharing platforms to take appropriate measures to protect different groups of recipients of their service. However, whilst said provision makes reference to mechanisms for users to report or flag certain content, it does not specifically refer to notice-and-action mechanism. At the same time, the DSA does introduce an obligation to put such a mechanism in place for all providers of hosting services. In that context, in situations where the AVMSD and the DSA are both applicable, while DSA does not alter obligations in Article 28b, it does complement it by obliging providers of hosting service to ensure safety of users online by putting in place an effective and easy to use notice-and-action mechanism (Art. 14).

10. As the DSA is without prejudice to several pieces of EU legislation, such as the Audiovisual Media Services Directive or the Copyright Directive, that among other things constitute exceptions to the liability exemption, we fail to see how the DSA can address the fragmentation of EU-legislation regarding online platforms. How will the Commission address this problem? Do you expect to issue guidance for platforms on their liability and requirements according to all the relevant EU-legislation?

The DSA is intentionally designed as a horizontal piece of legislation; a lex generalis in relation to the sector-specific legislation mentioned in its Article 1(5). This is a conscious policy choice, explained in the Impact Assessment: including all rules on intermediary liability and diligence solely in the DSA would have the benefit of full legal certainty, but the disadvantage of losing the flexibility and agility of sector-specific regulation would by far outweigh these gains. Finding a single common solution or finding all the solutions for all sectors within the DSA would not be feasible.

Nevertheless, the DSA will approximate national rules and users and the digital economy will benefit from the legal certainty ensured by an updated liability regime, the fully harmonised due diligence obligations and strengthened rules on cross-border enforcement.

11. La directive e-commerce: Le considérant 9 énonce que la directive e-commerce est une *lex specialis* par rapport à la proposition de DSA. Comment articuler cette affirmation avec le fait que plusieurs considérants de la proposition de DSA énoncent que la notion de service de la société de l'information au sens de la directive e-commerce est un genre incluant l'espèce du service intermédiaire au sens de la proposition de DSA ?

The ECD has a wide scope since it establishes rules for all information society services. The proposed DSA provides for specific rules for a subcategory of information society services, namely, intermediary services. Moreover, the DSA amends the ECD by deleting certain provisions of the ECD and incorporating them in the DSA (see Art. 71 of the DSA). As Article 1(5)(a) DSA makes clear, the DSA is to apply without prejudice to the rules contained in the DSA (as amended). That being so, whilst the term 'lex specialis' is indeed not the most suitable to describe the relationship between the ECD and the DSA, the reference to the ECD in the first sentence of recital 9 means that intermediary services will continue to be regulated by the ECD for matters falling within its scope (e.g. the prohibition of prior authorisations for information society services, including intermediaries).

12. Are the exclusions from the scope of Directive 2000/31/EC (the "e-commerce directive"), in terms of Recitals 12-16 and Article 1 paragraph 5 of the e-commerce directive, still equally excluded from the scope of the DSA. ?

Article 1(5) ECD sets out the fields to which the ECD does not apply. These fields are not specifically excluded from the scope of the DSA and there is nothing in the legislative proposal for the DSA which would point at the exclusion of these fields. In its Article 1, the DSA has its own rules on scope. Therefore, in as far as the matters in question fall within the scope of the DSA, the DSA applies also to the fields excluded from the scope of the ECD pursuant to its Article 1(5).

13. Several MS asked why CDSM, MSR, AVMS and EECD are not referred to in this article.

The list in Art. 1(5) DSA reflects the most relevant pieces of EU legislation where the interplay between the DSA (as lex specialis) could lead to confusion if left unclear. In respect of the acts of EU law specifically mentioned in Article 1(5), it was deemed important to provide clarification as to the relationship between those acts and the DSA. This does not mean that DSA necessarily affects any other EU law which is not listed explicitly in Art. 1(5). The relationship between those other acts and the DSA would have to be assessed in each case.

Article 2

a)

14. Pour quelle raison l'article 2 du DSA ne précise pas le lien entre le service de la société de l'information et le service intermédiaire, alors que la définition des services d'intermédiation en ligne dans le DMA, par renvoi à l'article 2 du règlement 2019/1150, comprend une articulation plus précise entre le service de la société de l'information et le service d'intermédiation en ligne ? Pourquoi les articles 3, 4, 5 font référence à la notion de services de la société de l'information et non à celle de services intermédiaires ?

It should be recalled that the terms "online intermediation services" within the meaning of Article 2(2) of the Regulation (EU) 2019/1150 and "intermediary services" within the meaning of Article 2(f) of the DSA do not have the same scope. Within this context Article 2(2) of the DMA refers to online intermediation services within the meaning of Article 2(2) of the Regulation (EU) 2019/1150 and not intermediary services within the meaning of Article 2(f) of the DSA. In addition, the definition of different types of intermediary services in Article 2(f) of the DSA does not refer to information society services, because it is clarified in Articles 3-5 respectively that different types of intermediary services (as defined in Article 2(f) of the DSA) represent information society services (as defined in Article 2(a) of the DSA). Finally, the changes to Articles 3-5 of the DSA as compared to Articles 12-14 of the ECD have been limited to the minimum necessary. Indeed, apart from Article 5(3) DSA, those changes are limited to those necessary to take account of the fact that the ECD is a directive and the DSA a regulation. The DSA therefore defined the notion of "intermediary services" in the DSA, which is missing in the ECD but which can be found in Section 4 of Chapter II of the ECD, while keeping the provisions of Articles 3-5 of the DSA unaltered in most respects.

b)

15. How would the Commission explain the main difference between the concept, hence meaning of the definition of the "recipient of the (intermediary) service" as defined in Art. 2(b) and that of the "trader "determined as per Art. 2 (e)? *Reasoning: For instance, it might be the case, when a company uses an online platform to offer its services, but at the same time receives an intermediary service/services from this online platform to be able to access its customers. Recipient of the intermediary service and a trader – same status at the same time?*

As a general rule, all traders offering products or services through intermediary services are recipients of those services, whereas not all recipients of intermediary services are traders.

In the DSA, the notion of "trader", as defined by Article 2(e), is mentioned in the context of: (i) the rule relating to the liability regime in Article 5(3); and (ii) the obligation on the traceability of traders in Article 22. The common denominator of these obligations is their application to "online platforms allowing consumers to conclude distance contracts with traders", also defined as "online marketplaces" by the Directive on consumer rights 2011/83 as amended by Directive

2019/2161. The aforementioned Directive on consumer rights requires online marketplaces to specify to consumers whether the third party offering a good or service is a “trader”, on the basis of the declaration of that third party to the provider of the online marketplace.

d)

16. What is considered as a “significant number of users”? How and by which means is it possible to identify whether the activities target one or more Member States? Does this refer to a specific number or percentage of the population?

The definition of ‘offering services in the Union’ makes reference to the assessment of a substantial connection with the EU on the basis of factual criteria, such as the significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The same definition has been used in the Terrorist Content Online Regulation and the e-evidence proposals. The assessment of ‘significant number of users’ must be done on a case-by-case basis. Recital 8 clarifies that the targeting of activities towards one or more Member States must by assessed on the basis of all relevant circumstances and it further lists examples of relevant factors.

e)

17. Does the definition of “*trader*” include a provider of residential space for the purposes of short-term tourist rental?

The DSA provides for the definition of ‘trader’ in line with other EU laws. A provider of short-term rental accommodation services who fulfils the conditions set out in the definition of ‘trader’ in the DSA, could fall within the scope of the definition of ‘trader’. It is important to note that, as stated above, the providers of online marketplaces must inform their consumers whether the third party offering goods, services or digital content is a trader or not on the basis of the declaration of that third party to the provider of the online marketplace (Directive (EU) 2019/2161 added Art.6a in Directive 2011/83/EU).

f)

18. Clarification on the legal status of digital platforms by determining what requirements a service must meet in order to be considered an *‘intermediary service provider’* within the remit of the DSA. If - for instance - a product is sold on an online marketplace by a seller, but the delivery is carried out by the online marketplace itself. Will the online marketplace be covered by the liability exemption in article 5?

Whether the service could be considered as one of the intermediary services within the meaning of Article 2(f) of the DSA would have to be assessed on a case-by-case basis against the requirements laid down in the respective definition and corresponding provision. For example, a provider of hosting services, such as online marketplace may be, could benefit from the liability

exemption in Article 5 of the DSA if it fulfills the conditions laid down in Article 5(2) in general and Article 5(3) in particular as regards the liability under consumer protection laws in relation to conclusion of distance contracts with traders.

Pursuant to Article 5(3), the online platforms in question may be liable under consumer protection law, if an average and reasonably well-informed consumer would believe, based on how online platform presented the specific item of information or otherwise enabled the specific transaction, that the information, or the product or service that is the object of the transaction, is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control. It appears that the mere fact that an online platform provides part or whole of the fulfilment service, such as delivery service, does not in itself lead to a conclusion that this condition would be met. For example, the online platform may clearly provide information to consumer that while it provides the fulfilment service, including delivery, this is done on behalf of the trader on its platform. In any event, as noted, the applicability of Article 5(3) will have to be assessed on a case-by-case basis.

19. Les autorités françaises relèvent que les hébergeurs, à qui sont applicables d'une part le régime de responsabilité de l'article 5, et d'autre part les obligations du chapitre III, section 2, sont définis à l'article 2 (f) comme des services consistant à stocker des informations fournies par un destinataire du service, à la demande de celui-ci. Elles s'interrogent sur le cas des moteurs de recherche, et rappellent qu'elles estiment indispensable que ces acteurs soient soumis à des obligations dans le cadre du DSA. Selon la Commission, l'activité de référencement des moteurs de recherches correspond-elle à cette définition, et si oui, les personnes éditant les sites internet référencés par le moteur doivent-elles être regardées comme des destinataires du service, malgré l'absence de relation contractuelle ? Dans le cas contraire, les moteurs de recherche relèvent-ils d'une autre catégorie d'acteurs identifiée dans le DSA, et laquelle ?

The mere fact that the recipient of the service, such as an end user, does not pay for the service rendered by the provider of intermediary services or there is no contractual relationship does not mean that the service may not constitute an intermediary service.

Having said that, it is not possible to provide one-size-fits-all reply whether a provider of an online search engine will always provide hosting services or always provide some other type of intermediary services within the meaning of Article 2(f) of the DSA. Such a categorization will very much depend on the nature of the service and activities performed by the provider of online search engine. As shown in Joined Cases C-236/08 and 238/08, the Court did not exclude that a referencing service as described in recital 23 of that judgement could indeed be considered as a hosting service within the meaning of Article 14 ECD. At the same time, this should not be understood as if any referencing service would necessarily constitute a hosting service within the meaning of Article 14 ECD (or Article 5 DSA), since it may not exhibit same features as the Court observed in relation to AdWords as paid referencing service.

20. Do reverse proxy providers fall within the definition of caching or mere conduit?

The question whether the individual reserve proxy service providers are intermediaries and DSA obligations apply to them has to be assessed on the basis of their technical functionalities, on a case-by-case basis. According to an external legal analysis1 of various intermediary service providers establishing and facilitating the underlying logical architecture and proper functioning of the internet, reverse proxy service providers could generally fall under the category of 'caching' internet service provider, although it is provided as a part of the hosting service.

21. Could the Commission provide concrete examples for the different definitions in Article 2(f) (intermediary services) and sub-bullets (mere conduit, caching, hosting), (h) (online platform)?

The examples given below should be understood as illustrative and non-exhaustive, and as complementary to the examples given by the Commission during the Council Working Party meeting:

'Mere conduit': Internet exchange points, Wi-Fi access points, virtual private networks (VPN), Voice over IP and other interpersonal communication services
'Caching': content delivery networks (CDNs), reverse proxies, content adaptation proxies
'Hosting': cloud computing, web hosting, services enabling sharing content and information online, file storage and sharing
Online platform: online marketplaces, social networks

As noted above, it will however always have to be decided on a case-by-case basis, having regard to all relevant facts and circumstances, whether a given service qualifies as an intermediary service as defined in the DSA and if so, within which of the three categories of intermediary service the service in question will fall. That holds true in respect of the above services, but for instance also in respect of services such as Domain Name Systems services, services relating to IP addresses, messaging services, search services or live-streaming.

22. What is the Commission's take on the definition of a "*hosting service*" as defined as a subset of *intermediaries* under Article 2(f) in relation to the status of *online advertisement intermediaries*? Can the hosting definition be construed to include these types of intermediaries? If so, does the Commission believe the hosting definition is future proof to legal appeals, such as a recent case whereby a court ruled against the argument of a social media company to be classified as a "*hosting provider*" in relation to fake bitcoin ads that appeared on the platform?

---

[1] This legal analysis is quoted in the Impact Assessment accompanying proposal for the DSA as well and is available on the following link: https://op.europa.eu/en/publication-detail/-/publication/3931eed8-3e88-11eb-b27b-01aa75ed71a1/language-en/format-PDF/source-179885922

For the purpose of the DSA, the term ‘advertisement’ is defined in Article 2(n) and online advertising intermediaries are referred to broadly as ‘services that connect publishers of advertising with advertisers’ (recital 70). This preserves a broad flexibility and wide coverage: online advertising follows multiple models with varying levels of centralisation, and can involve a range of services, from direct transactions between advertisers and publishers, to complex interactions between several types of intermediary services interacting with each other.

Depending on the role they play and functions they offer in the delivery of advertisements, some of these services could qualify as ‘hosting services’. For example, a so-called ‘ad server’ will likely store the content of an advertisement provided by and at the request of a recipient - within the meaning of the definition in Article 2(f), third indent. The CJEU interpreted2 the role as hosting service within the meaning of the ECD for ‘internet referencing services’ that store keywords provided by the recipient of their service for displaying ads according to those words. These are two examples of hosting services in the broader category of ‘advertising intermediaries’; they each ‘host’ different type of content, in this regard.

When advertising intermediaries are hosting services, the eligibility for the liability exemption needs to be determined on a case-by-case basis, according to the conditions set in Article 5 of the proposal. This approach responds precisely to the evolution and diversity of services and functions in this dynamic field.

g)

23. Concerning the broad variety of “illegal content” and the different rights and values at stake, why does the COM not differentiate between illegal information on the one hand and illegal goods and services on the other hand?

Articles 3 to 6 DSA (as much as Articles 12-15 ECD) establish a liability regime protecting certain providers from liability arising from the illegal nature of the information provided by and stored at the request of recipients of their services. This applies to information related both to goods, services or “speech” (non-commercial information), as unlawfulness and liability can concern any of those categories.

Where necessary, the DSA refers to the illegality of the information in particular, as action by an intermediary can only be limited to remove or disable access to the relevant information stored in their service, but they cannot act against the illegal activity behind. For instance, a listing of a counterfeit product can be removed, but the counterfeit activity itself – which happens in the offline world - cannot. In those cases, the DSA makes such distinction.

Furthermore, in some specific instances where the particular risks identified in certain online marketplaces is at stake, the DSA establishes specific rules (Articles 5(3) and 22).

---

[2] See C-236/08 Google France and Google http://curia.europa.eu/juris/liste.jsf?num=C-236/08

24. Is the “illegality of content” determined by the law of the country of origin or (also) by the law of the country in which the provider provides its services?

The illegality of an individual piece of content is to be identified by any competent authority or court under applicable EU or national law.

The principle is not in contrast with the country of origin principle. The Court has already established that “in the event of an alleged infringement of personality rights by means of content placed online on an internet website, the person who considers that his rights have been infringed has the option of bringing an action for liability, in respect of all the damage caused, either before the courts of the Member State in which the publisher of that content is established or before the courts of the Member State in which the centre of his interests is based. That person may also, instead of an action for liability in respect of all the damage caused, bring his action before the courts of each Member State in the territory of which content placed online is or has been accessible. Those courts have jurisdiction only in respect of the damage caused in the territory of the Member State of the court seised. Article 3 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’), must be interpreted as not requiring transposition in the form of a specific conflict-of-laws rule. Nevertheless, in relation to the coordinated field, Member States must ensure that, subject to the derogations authorised in accordance with the conditions set out in Article 3(4) of Directive 2000/31, the provider of an electronic commerce service is not made subject to stricter requirements than those provided for by the substantive law applicable in the Member State in which that service provider is established.” (Joined Cases C-509/09 and C-161/10).

25. Does this wide concept of illegal content demand too much knowledge and expertise on a smaller hosting service provider? Illegal content was not defined in the e-commerce directive. Because of the proposed wide definition of illegal content, is the conditional liability rule in article 5 really the same as it used to be in art. 14 of the e-commerce directive? Can the Commission explain (once again) the rationale behind the proposed wide concept of illegal content?

The objective of the definition of ‘illegal content’ in Article 2(g) DSA is to provide legal certainty and clarify that the question whether specific information or activity may be considered illegal is to be determined according to the applicable EU or national law. However, the fact that DSA provides this clarification does not change the fact that the existing regime under the ECD is exactly the same; i.e. whether a specific information or activity is to be considered illegal is to be determined based on the applicable EU or national law. In this regard, neither the ECD nor the DSA are defining what content may be considered illegal, but simply provide for a framework of conditional liability exemption for providers of intermediary services in case of illegal activity or information by the recipients of the service (Section 4 of Chapter II of the ECD; Articles 3-5 of the DSA).

26. Le concept de « contenu illicite » défini à l'article 2 (g) renvoie à toute information contraire au droit de l'Union ou d'un Etat membre, que l'illicéité concerne l'information elle-même ou l'activité à laquelle il est fait référence, y compris la vente de produits ou la fourniture de services. Est-ce que cette définition recouvre bien, outre les offres pour des produits interdits, contrefaisants ou dangereux, le cas des annonces publiées sur les places de marché méconnaissant les droits des consommateurs. En outre, le texte ne précise pas si, et selon quels critères, une information devrait être qualifiée de contenu illicite lorsqu'elle renvoie à des contenus, biens ou services qui ne sont pas directement accessibles via ce service. Il serait souhaitable de clarifier, par exemple, dans quels cas une application disponible sur un magasin d'applications qui donne accès à des contenus illicites, ou encore un lien référencé par un moteur de recherche qui pointe vers un site comportant des contenus illicites, doivent être regardés en eux-mêmes comme des contenus illicites. Les autorités françaises souhaiteraient donc clarifier la portée du concept de contenu illicite, d'une part, s'agissant des annonces ne respectant pas les droits des consommateurs, et d'autre part, dans les cas où le contenu renvoie à des informations illicites qui ne sont pas directement accessibles sur le service proposé par le fournisseur.

Notice and action obligations apply for potentially illegal ads, as for any other type of content. This means that any ad that is considered as illegal by national or Union law as not compliant with consumer protection rules can be considered as "illegal content" within the meaning of the DSA and therefore subject to the mechanisms provided by the DSA.

Concerning content that refers to illegal information that is not directly accessible on the service offered by the provider, the illegality of such content should be assessed on a case-by-case basis.

For instance, in a 2018 case on the application by Magyar Jeti ZRT, a Hungarian online news portal, against Hungary, the European Court of Human Rights issued a judgement finding that the Hungarian law on objective (strict) liability for disseminating defamatory material, which had excluded the possibility of any meaningful assessment of the applicant company's right to freedom of expression, violated Article 10 of the European Convention on Human Rights[3].

[3] CASE OF MAGYAR JETI ZRT v. HUNGARY (Application no. 11257/16) http://hudoc.echr.coe.int/fre?i=001-187930

h)

27. Why did the Commission choose not to include the definition of very large online platforms in Article 2?

In order to define a very large online platform, it is necessary to specify in the legal text a series of substantive and procedural provisions for determining the reach of an online platform qualifying as a 'very large online platform'. As such specifications are normative provisions, they are to be included in the main articles and not in the definitions. The proposed text provides for all the necessary specifications in Article 25 and builds on transparency and disclosure obligations for all online platforms, as set out in Article 23(2) and (3). That being so, it is neither appropriate nor necessary to include a definition to this effect in Articled 2.

28. Do the provisions of the draft DSA which are applicable to all providers of intermediary services (Chapter III Section 1) and to providers of hosting services (Chapter III Section 2) apply to interpersonal messaging services and what (public) messaging services are additionally covered by the definition of "online platform" in Art. 2 lit. h of the draft DSA?

The DSA may apply to interpersonal communication services, including messaging services. Indeed in some cases, these service providers provide functions beyond communication exchange. It would have to be assessed on a case-by-case basis of their technical functionalities whether the service fulfils the definition of an 'online platform', particularly whether it intermediates dissemination of information to public.

29. La proposition de règlement « *Digital Services Act* » (DSA) ne fournit pas, à ce stade, de typologie des services que recouvre le concept de « plateforme numérique » défini à l'article 2 (h). Par comparaison, la proposition de règlement « *Digital Markets Act* » (DMA) liste au contraire de façon exhaustive les « services de plateforme essentiels » visés par le texte (article 2). Il s'agit des services d'intermédiation en ligne (magasins d'applications inclus), des moteurs de recherche, des réseaux sociaux, des services de partage de vidéos, des services de communications interpersonnelles non fondés sur la numérotation, des systèmes d'exploitation, des services informatiques de *cloud* et des services de publicité (dont les services d'intermédiation des offres publicitaires en ligne). Les autorités françaises souhaitent obtenir de la part de la Commission davantage de visibilité sur les «plateformes numériques» visées par le DSA, au regard notamment de ce qui est prévu par exemple par le DMA. Elles se demandent, en particulier, quelles catégories d'acteurs recouvre la notion de « plateforme numérique » du DSA, et notamment ce qu'il en est des moteurs de recherche, des magasins d'applications, des systèmes d'exploitation, des services d'intermédiation publicitaire, des services de messageries utilisés pour la diffusion d'information au sein de groupes étendus, ou encore des plateformes d'hébergement d'espaces collaboratifs (blogs) ?

The notion of "core platform services" laid down in Article 2(2) DMA seeks to define those services that meet specific criteria, feature specific characteristics and where unfair practices by gatekeepers are more prominent (see in particular point 128 of the IA accompanying the DMA).

The Commission identified several services (i.e. core platform services), which meet these criteria and where absent regulatory intervention the identified problems concerning unfair behavior by gatekeepers could effectively remain un-addressed. To ensure that the regulatory intervention in the DMA is limited to those instances where this is justified and necessary it was necessary to clearly and unambiguously define specific services that fall within its scope.

On the other side, irrespective of the nature of the service that could potentially fall within the scope of the definition of the online platform within the DSA (e.g. online marketplace; social media platform), the nature of the problem associated with the dissemination of potentially illegal content and measures to tackle these would not differ depending on the type of online platform, but rather on its size and reach in the society. To that end, it is more important to differentiate between online platforms in general and very large online platforms in particular. Having said that, it is important to note that it is for the case by case assessment to show whether a specific service constitutes an online platform service, because it meets the requirements laid down in Article 2(h).

i)

30. It is the Danish Government's assessment that both militant groups and extremist political groups are increasingly using closed groups/channels and alternative platforms (which are characterized, among other things, by offering a high degree of anonymity and a low degree of content moderation) for communication and dissemination of violent extremist and terrorism-related online content. It’s important, that the definition of "dissemination to the public" (article 2 (i)) does not preclude the Regulation from also covering the spreading of violent extremism and terror-related online content, which takes place via closed groups/channels. Therefore, we would appreciate further clarification and definition of the distinctions between public vs. private communication and what is meant by closed and open groups/channels respectively.

The DSA applies to all intermediary services, including those which constitute interpersonal communication. As such, the obligations set out in Chapter III, section 1, apply to these services and where these services may constitute hosting, the obligations set out in Chapter III, section 2, also apply. However, it is important to note that all obligations in the DSA are without prejudice to the ePrivacy Directive and the GDPR as set out in Article 1 (5)(j). Obligations set out in Chapter III, sections 3 and 4 apply to those intermediary services which constitute online platforms or very large online platforms, respectively. Notably, these are services which disseminate information to the public. Article 2(i) defines the term “dissemination to the public”. Further explanation as to what constitutes dissemination to the public can be found in recital 14, which clarifies that interpersonal communication services fall outside of the scope of this concept. Note that, as noted above, recital 14 includes a small mistake for which a corrigendum may be issued: it notes that those services fall outside the scope of the DSA, whereas it should state that they do not fall within the concept of ‘dissemination to the public’.

k)

31. Does Article 2(k), i.e. *"online interfaces"*, in conjunction with articles 24 and 30, apply to advertisements displayed on third party websites (e.g. on social media platforms owned by an online ad intermediary)?

The scope of Articles 24 and 30 is directly linked to the definition of 'advertisement' as set out in Article 2(n). In particular, that definition refers to advertisements 'displayed by an online platform on its online interface'. Consequently, all ads in scope of the provisions in Articles 24 and 30 are ads served (displayed) on the online platform, irrespective of the online ad intermediary/ies involved in the process between the advertiser and the platform.

While an online interface, as defined in Article 2(k), is not limited to the online interface of an online platform, the qualification for online advertisements in Article 2(n) excludes from the scope of the provisions ads displayed on third party websites through advertising intermediaries.

o)

32. According to Art. 2 (o), recommender systems of online platforms do suggest in their online interface specific information to recipients. Can we assume, that the term "specific information" determines not only information as such, but also displays a personalized offer of goods and services?

Yes. 'Information' in this definition is understood within the meaning of the reference to 'information' in Article 2(f), third indent. It refers to any information hosted by the platform, including information containing offers for goods or services, as well as other types of content.

p)

33. Les autorités françaises souhaitent clarifier si la définition de la modération recouvre les mesures de déréférencement de sites par des moteurs de recherche.

To the extent that such measures taken by online search engines would affect the availability, visibility or accessibility of illegal content online they would be considered as content moderation measures. For the DSA's obligations to apply, the provider concerned will naturally also have to fall within the personal scope of the relevant provisions of the DSA.

Chapter II

34. What does the announced "modernization of the rules" for the responsibility of platforms consist of, if rules from the eCommerce Directive are taken over verbatim? Why do online traders and sales platforms not have to assume more responsibility, especially despite the negative experiences of users in the COVID-19 crisis?

The DSA maintains the principles underpinning the E-commerce Directive, and in particular the safe harbour for the liability of intermediaries. The modernisation however consists in

complementing such basic fundamental principle with a detailed set of due diligence obligations for these intermediaries, graduated on the basis of their role in the internet stack and, as regards platforms, their reach. Moreover, the DSA provides also a number of clarifications, e.g. as regards voluntary measures undertaken by the intermediaries as well as liability pursuant to consumer protection law where the role of a platform in concluding a distance contract is such that it blurs the distinction with the trader effectively providing the service according to an average and reasonably well-informed consumer.

35. Can Member States determine in which cases hosting service providers must delete illegal content?

As a matter of principle Member States are under EU law not required to - and are in fact prevented from - legislating in the area and in relation to the objectives pursued by the harmonizing rules of the EU legislation.

Member States therefore in general will not be allowed to adopt parallel national provisions on the matters falling within the scope and the areas addressed by the DSA, ie which are regulated by its provisions, 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 esnhrined in the Charter are effectively protected (see Article 1(2) of the Regulation).

The precise scope of the remaining legislative competence of Member States, on the other hand, cannot be defined in abstract, as it may also depends on the intensity of harmonisation of individual provisions. For exemple, as pointed out earlier, as especially Articles 5(4) and 8 make clear, Member States retain the possibility to empower judicial or administrative authorities to order hosting service providers to remove or disable access to specific items of illegal content. Moreover, as also pointed out earlier, the DSA leaves the obligations resulting from the other acts of the EU law mentioned in Article 1(5) unaffected.

36. To which intermediary service liability regime type (“mere conduits”, “caching” or hosting) exactly does each of intermediary service providers that are mentioned in the regulation (including Recital 27) belong? If possible, can this be indicated in tabular form? Given mentioned considerations, to which of the service provider liability regime type (“mere conduits”, “caching” or hosting) do domain registries, registrars and other domain name system service providers belong and why?

Any general rule should leave a certain margin of appreciation, as business models (and the technological features behind) evolve constantly. For that reason, the DSA retains the existing categories of “mere conduits”, “caching” and “hosting”, based on the technical features of the

service. Recital 27 intends to clarify that some examples of services of the Internet's underlying logical structure (understood as illustrative and non-exhaustive) could also fall within these categories, which is to be determined on a case-by-case basis. For instance, Wi-Fi access points have already been considered by the Court as "mere conduits" (C-484/14, McFadden).

Annex 9 of the Impact Assessment accompanying the DSA, in particular its chapter 4, contains numerous examples and categorisation of services anticipated to be covered by Articles 3, 4 and 5 DSA, without prejudice to the required case-by-case assessment. The Commission has also commissioned studies with this purpose in mind.

37. Les autorités françaises s'interrogent sur la pertinence de l'approche concentrique proposée par le *Digital Services Act* (DSA) qui conduit à identifier les plateformes numériques, soumises au régime d'obligations le plus contraignant, forcément comme une sous-catégorie des hébergeurs, concept qui renvoyait dans la directive sur le commerce électronique à un régime de responsabilité, et qui fait ici l'objet d'une définition positive. D'abord, ceci revient à créer un lien entre deux questions qui devraient, selon elles, être traitées de façon distincte : d'un côté, celle du régime de responsabilité au regard des contenus mis en ligne par des tiers (éventuel bénéfice du « *safe harbor* »), et de l'autre, celle des obligations positives en matière de modération des contenus. Ensuite, ceci exclut toute possibilité d'imposer à certains acteurs les obligations correspondant à une certaine catégorie sans que leur soient également appliquées les obligations relevant de toutes les catégories plus larges. Pour ces raisons, elles demandent à la Commission de fournir des indications sur la justification, d'une part, d'un lien systématique entre régime de responsabilité et obligations positives de modération, et d'autre part, de l'approche concentrique conduisant à définir les plateformes numériques comme un sous-ensemble de la catégorie des hébergeurs.

There is no direct link between the protection from liability and the imposition of due diligence obligations. The definition of "hosting service" (under Article 2(f)) is of a technical nature: "a 'hosting' service that consists of the storage of information provided by, and at the request of, a recipient of the service". Storage is the technical feature of hosting bits and bytes remotely in a server, which is to happen at the request by the recipient of the service. A given provider could, for instance, be excluded from the exemption of liability (for instance because the recipient of the service is under its authority or control – Article 5(2)), and still subject to the relevant due diligence obligations (under Chapter III).

Online platforms –as defined for the purposes of the DSA (Art. 2(h)) - include among their features the storage and further dissemination to the public of user-generated content. This is the main feature behind the key issues that the DSA intends to tackle, such as the use of platforms to spread illegal content, private moderation of user generated content or its use by third party traders to make business. This is the particular feature that the DSA focuses on, hence the need to sub-categorise them within the broader category of hosting services.

38. What is the EC's position in principle regarding additional exceptions with regard to certain platforms (e.g. educational platforms, platforms that are not for profit but very much have the character of a service)?

One of the key elements of the Impact Assessment accompanying the DSA is the evaluation of the ECD; the DSA is built on it conclusions. The Commission found that the conditional liability regime established in 2000 was still fit for purpose, therefore, apart from certain necessary clarifications and adjustments, Articles 12-15 of the ECD are almost verbatim transferred to the DSA. This includes the established categories of exempted intermediary services (mere conduit, caching, hosting), on which 20 years of jurisprudence have been built.

In this context, the idea of creating new categories for the liability exemption was not underpinned by evidence. This does not mean that such an approach could not be justified in certain situations. For example, the 2019 DSM Copyright Directive's Article 17 expressly excludes certain services, such as not-for-profit online encyclopaedias, not-for-profit educational and scientific repositories, open source software-developing and-sharing platforms from its scope. Consequently, those services will fall under the scope of the DSA, as the horizontal legislation, naturally only in as far as the requirements for the DSA to apply are met. For instance, the service must be one that is normally provided for remuneration; otherwise it is not an 'information society service' as defined in Article 2(a) of the DSA. The Court's case law makes clear that the concept 'normally provided for remuneration' is interpreted rather broadly, covering also situations where remuneration is not obtained from the end-user but from a third party.

Also, it is worth recalling that Articles 12-14 of the ECD, as well as Articles 3-5 of the DSA are conditional liability exemptions. If a service does not meet the conditions it will not benefit from the exemption, even if it is educational in nature.

39. Could the Commission provide an example of how the "service-based" liability would work in practice (as opposed to provider-based liability), particularly if an intermediary provides several different services?

A typical example would be a provider of "bundle" Internet services, such as commercially available in all Member States. The same provider can, at the same time, provide several "mere conduit" services (the Internet connection, a public wifi hotspot…); "caching" services (to ensure continuity of the signal to for instance watch a VOD service), "hosting" services (XXGB cloud space for private use), in addition to several other services (their VOD service, TV "on demand" or "à la carte"; interpersonal communication services, such as webmail services, etc.). The liability exemption under Article 3, or 4, or 5, only cover the particular services covered under such category, but not the others. Services involving content that is not provided by recipients, but in respect of which the provider has editorial responsibility for instance, are not be covered by the liability exemptions.

Article 3

40. Why is the mere conduit no longer obliged, upon obtaining such knowledge or awareness, to act expeditiously to remove or to disable access to the illegal content upon obtaining such knowledge or awareness?

The liability exemption under Article 3 DSA (and today's Article 12 ECD) is not subject to any knowledge standard. This has been the traditional legislative technique – also under the United States' DMCA system for copyright notices. The main reason behind this, traditionally, is that mere conduits, such as Internet service providers, cannot act with the necessary granularity against a particular item of illegal content. They can merely block access to a full website, and leaving this to a normal "notice" standard could lead to the undesired blocking of legal speech. The Court has itself referred to this difference in Case C-484/14 (McFadden): (57) "It appears from a comparison of Article 12(1), Article 13(1) and Article 14(1) of the directive that the exemptions from liability provided for in those provisions are governed by different conditions of application depending on the type of activity concerned. (59) […] Article 12(1) of Directive 2000/31 does not subject the exemption from liability that it lays down in favour of providers of access to a communication network to compliance with such a condition. (60) […] the position of an internet website host on the one hand and of a communication network access provider on the other are not similar as regards the condition laid down in Article 14(1) of Directive 2000/31. […] (62) Nevertheless, the service provided by an internet website host, which consists in the storage of information, is of a more permanent nature. Accordingly, such a host may obtain knowledge of the illegal character of certain information that it stores at a time subsequent to that when the storage was processed and when it is still capable of taking action to remove or disable access to it. (63) However, as regards a communication network access provider, the service of transmitting information that it supplies is not normally continued over any length of time, so that, after having transmitted the information, it no longer has any control over that information. In those circumstances, a communication network access provider, in contrast to an internet website host, is often not in a position to take action to remove certain information or disable access to it at a later time."

Article 4

41. What kind of rules, as per Art. 4 (1) (c), on updating the information are here referred to? What does updating information substantially entail?

This rule exists since 2000 and, while it has not been interpreted by the Court, it intends to reflect industry standards regarding the frequency under which stored information ("cache memory") is duly "refreshed" in order to mirror exactly the source where the original content is hosted.

Article 5

42. L'article 5(2) du « Digital Services Act » (DSA) écarte l'exemption de responsabilité dans l'hypothèse où le destinataire du service agit sous le contrôle ou l'autorité du fournisseur du service. L'article 5(3) du « *Digital Services Act* » (DSA) codifie au sein de la définition du statut des hébergeurs, pour sa part, la jurisprudence de la CJUE s'agissant des places de marché en ligne agissant ou se comportant comme le vendeur. L'article 5 (3) envisage deux hypothèses, à savoir, la croyance du consommateur en la fourniture du produit ou du service par la plateforme et la croyance du consommateur en la fourniture du produit ou du service par un destinataire de services agissant sous l'autorité ou le contrôle de la plateforme. Par ailleurs, le projet de règlement tend à reprendre, dans son considérant 18 les termes d'une jurisprudence quant au « rôle actif » mené par la place de marché dans la transaction. Les autorités françaises estiment que ces termes et critères de jurisprudence, ciblés sur les places de marché appellent une clarification législative. Les autorités françaises souhaiteraient que la Commission précise selon quels critères le rôle du vendeur tiers ou du prestataire de services tiers peut concrètement être considéré comme faible ou nul de fait et engager la responsabilité de la place de marché en ligne ?

Whether a service provider remains neutral as regards the relationship between the two sides (in particular in a transaction between a trader and a consumer) or goes beyond an intermediary role needs to be assessed on a case-by-case basis. As explained in Annex 9 of the Impact Assessment, in the view of the Commission services, "there is still an important uncertainty as to when it is considered that an intermediary, and in particular, a hosting service provider, has played an active role of such a kind as to lead to knowledge or control over the data that it hosts. The fact that there is no such thing as an "active host", but that a provider might play an active role regarding some listings, but not others (for instance because it presents it or recommends it in a special manner) does not lead to the necessary legal certainty to provide legal intermediation services without risking claims for damages or even criminal liability. Many automatic activities, such as tagging, indexing, providing search functionalities, or selecting content are today's necessary features to provide user-friendly services with the desired look-and-feel, and are absolutely necessary to navigate among an endless amount of content, and should not be considered as "smoking gun" for such an "active role"."

The Court might soon clarify this question in two upcoming cases, regarding YouTube and Uploaded. In his Opinion, the Advocate General favours the following interpretation of when this "active role" comes into play: "the 'active role' envisaged by the Court quite rightly relates to the actual content of the information provided by users. I understand the Court's case-law to mean that a provider plays an 'active role' of such a kind as to give it 'knowledge of, or control over' the data which it stores at the request of users of its service where it does not simply engage in the processing of that information, which is neutral vis-à-vis its content, but where, by the nature of its activity, it is deemed to acquire intellectual control of that content. That is the case if the provider selects the stored information, if it is actively involved in the content of that information in some other way or if it presents that information to the public in such a way that it appears to be its own. In those circumstances, the provider goes outside of the role of an intermediary for

information provided by users of its service: it appropriates that information." The Advocate General further puts the bar on the necessary confusion created on "an average internet user who is reasonably circumspect", to the extent that he or she does not know whether the files stored do originate from the operator or from a third party.

This interpretation seems aligned with similar interpretations by the Court in the Wathelet case, where the CJEU has explained that it is "essential that consumers are aware of the identity of the seller, and in particular whether he is acting as a private individual or a trader, so that they are able to benefit from the protection conferred on them". It follows therefore that, in the circumstances in which an online marketplace act as an intermediary on behalf of a third party trader, the absence of knowledge of a consumer on the capacity in which the online marketplace acts would deprive him/her of his/her consumer rights. In this regard, according to the CJEU "a trader may be regarded as a 'seller' […] where he fails to duly inform the consumer that he was not the owner of the goods in question".

Finally, in an older case, relating to the liability by an online newspaper, the Court applied the "active role" test and decided that "since a newspaper publishing company which posts an online version of a newspaper on its website has, in principle, knowledge about the information which it posts and exercises control over that information, it cannot be considered to be an 'intermediary service provider' within the meaning of Articles 12 to 14 of Directive 2000/31, whether or not access to that website is free of charge". This suggests that where the service provider's involvement with the content is so extensive that the content in question is no longer 'user content' but should instead be 'co-attributed' to the provider, the latter can no longer reasonably be called an intermediary.

Today, the ECD refers in recital 44 (for mere conduits and caching services; for hosting services see also Article 14(2)) to a sort of "vicarious liability" for those cases where the service provider deliberately collaborates with one of the recipients of its service in order to undertake illegal acts or is integrated with the content provider, and as a result it should not benefit from the liability exemptions established for intermediaries. This idea exists also in other legal systems (DMCA in the US). This has also been stressed recently in Advocate General Øe's Opinion, who proposes that where the provider deliberately facilitates the carrying out of illegal acts by users of its service, and where objective factors demonstrate the bad faith of the provider, such provider loses the benefit of the exemption from liability under Article 14(1) of Directive 2000/31.

43. In Article 5(1)(b) relating to Hosting, the statement "acts expeditiously" is open to interpretation. Why did the European Commission not qualify the actual time or time-range in this regard? Will parameters be further defined to precisely determine how fast a hosting service provider should act to remain within the parameters of acting "expeditiously" vis-à-vis the illegal content?

As the Impact Assessment accompanying the DSA (p. 119) shows, it can be concluded that national courts interpret "expeditiously" on a case-by-case basis taking into account a number of factors

such as: the completeness of the notice, the complexity of the assessment of the notice, the language of the notified content or of the notice, whether the notice has been transmitted by electronic means, the necessity for the hosting service provider to consult a public authority, the content provider, the notifier or a third party and the necessity, in the context of criminal investigations, for law enforcement authorities to assess the content or traffic to the content before action is taken. A one-size-fits-all timeline would not be fit-for-purpose, as it would not allow for the necessary flexibility to adapt to the particular circumstances of a given case.

However, the consequent transparency reporting requirements introduced by the DSA (in particular as regards the average time taken to take action) will provide important information on the average time taken and a comparative overview of "slower" and "faster" action.

44. Could you explain the liability regime and the meaning of "under the authority or the control of the provider" stated in art. 5, par. 2?

As stated above (see the answer to question 42), today, the ECD refers in recital 44 to a sort of "vicarious liability" for those cases where the service provider deliberately collaborates with one of the recipients of its service in order to undertake illegal acts or is integrated with the content provider, and as a result it should not benefit from the liability exemptions established for intermediaries. This idea exists also in other legal systems (DMCA in the US). It can also put in relationship with the Pappasavas case (C-291/13), where the Court established that "consequently, since a newspaper publishing company which posts an online version of a newspaper on its website has, in principle, knowledge about the information which it posts and exercises control over that information, it cannot be considered to be an 'intermediary service provider' within the meaning of Articles 12 to 14 of Directive 2000/31, whether or not access to that website is free of charge.

Article 6

45. The Commission explained that an intermediary service can still acquire "actual knowledge" as a result of conducting own initiative investigations. If the intermediary service discovers illegal content through such voluntary measures and still does not remove the content, it can be held liable. Should Article 6 be understood as establishing a kind of "presumption" for intermediary services, i.e. that the latter do not acquire "actual knowledge" solely by carrying out voluntary own-initiative investigations? In the affirmative, would it be possible to "reverse" this presumption if it can be proven that the intermediary service effectively had actual knowledge of the illegality on the basis of the information obtained through own-initiative investigations and omitted to take adequate action?

Article 6 of the DSA does not intend to provide any rebuttable presumption as the question suggests. It rather explictly provides that the provider of intermediary services shall not be ineligible to benefit from the conditional liability exemption laid down in Articles 3-5 respectively, simply because it carries out voluntary measures with an objective of detecting, identifying and

removing/disabling access to illegal content or takes the necessary measures to comply with the requirements of Union law.

This clarification does not preclude any interested party to seek to prove that the provider of intermediary services has obtained an actual knowledge of illegal content or activity by means of voluntary measures it has implemented.

46. Does Art. 6 of the draft DSA stipulate that a provider who has uncovered illegal content as a result of voluntary investigations can still lose the exemption from liability if he does not act expeditiously to remove or to disable access to the illegal content?

Article 6 seeks to provide explicitly that voluntary measures in sense of this provision as such do not preclude the benefit from the conditional liability exemption for providers of intermediary services. However, if the provider of hosting services has obtained such actual knowledge in the context of the voluntary measures employed, the provider can only benefit from the liability exemption if it acts expeditiously to remove or disable access to such content. This consequence derives from combined reading of Articles 5 and 6 DSA respectively and not solely from reading of Article 6 DSA. In addition, the Commission would like to refer to recital 22 of the DSA, which, in line with the existing case law, clarifies that provider of hosting services can obtain actual knowledge or become aware of the illegal information or activity online through several means, including its own investigation.

47. L'article 6 du *Digital Services Act* décorrèle entièrement la possibilité, pour les hébergeurs, de bénéficier d'un régime d'exonération conditionnelle de responsabilité, de l'existence de mesures de diligence prises proactivement par ces services. Sur le principe, la France adhère à cette distinction, qui était d'ailleurs celle posée par la Communication de la Commission « *Tackling illegal content* », mais juge nécessaire d'insérer dans l'article 6 lui-même la précision énoncée au considérant 22, selon laquelle les services intermédiaires peuvent avoir connaissance de la présence de contenus illicites du fait de leurs propres initiatives de détection des contenus. Dans ce cas, pour conserver le bénéfice de leur exemption de responsabilité, ils devront promptement retirer ou bloquer l'accès à ces contenus, comme si ces contenus leur avaient été notifiés. Les autorités françaises souhaitent interroger la Commission sur les raisons pour lesquelles la précision énoncée au considérant 22 (la connaissance effective, par les opérateurs, de la présence de contenus illicites peut résulter de leurs propres initiatives de détection des contenus) ne figure pas au sein même de l'article 6. Elles souhaitent qu'elle figure dans l'article.

The provider of hosting services could obtain the actual knowledge or become aware of the illegal activity or information also by means of its own voluntary measures. The existing case law, recalled in recital 22 of the DSA, provides sufficient legal certainty as regards this question and does not find it necessary to repeat this principle in Article 6 itself.

48. How is it ensured that the supervisory authority of a Member State will not be able to abuse this article to the disadvantage of the platform?

Where the concern relates to supervisory authorities requesting further proactive measures, then this clarification for providers to take action voluntarily and deploy measures without losing the liability exemption should be read in conjunction with Article 7 of the DSA. The latter prohibits obligations to monitor the information they transmit or store. As such, Member States are not allowed to oblige providers to carry out these types of investigations.

Where the concern relates to providers losing their liability exemption regardless of this Article, recital 25 clarifies the conditions under which the providers can benefit from this provision in the context of voluntary own-initiative investigations, by providing that the sole fact of carrying out such measures and activities must not lead to the loss of the exemptions of liability.

49. We would like the Commission to elaborate on why there are no proactive requirements for the platforms to detect illegal content?

The Impact Assessment accompanying the DSA has analysed the content moderation tools used to detect content through automated means in terms of efficacy and in terms of impact on fundamental rights, drawing from the growing body of academic research on the matter.

The DSA is intended as horizontal legislation, applying to all types of illegal content as defined in national and EU laws. As such, this may include content which is highly context-specific and for which automated tools may not be suitable. Such obligations for this horizontal approach were deemed unsuitable as they could incentivise removal without proper diligence. Further, the costs of deploying such tools for smaller platforms in particular, may be prohibitive, especially in a situation where these would be applied to such wide areas of illegality.

Where necessary, sector-specific acts of EU law could contain requirements of this kind.

50. What is the real added value of Article 6? We see the logic behind and the link between the provisions of Art. 3-5. (exception from liability) and Art 7. (no general monitoring obligation). How the provision of Articles 6 precisely fits into this scheme? We want to make sure that Art. 6 does not constitute a loophole for service providers in the application of liability rules?

Article 6 of the DSA does not fundamentally change the conditional liability exemption regime as laid down in articles 3-5 of the DSA. It simply seeks to provide legal certainty for those providers of intermediary services that act responsibly and engage in voluntary (or legally required) measures to detect, identify and remove/disable access to illegal content that may be available on or through their services that they will not lose conditional liability exemption on this ground alone. This is not to say that provider of hosting services could not through such measures obtain actual knowledge, which would trigger necessary action on its side in order to continue to benefit from the conditional liability exemption.

It should be noted that absence of such legal certainty in respect of voluntary measures has often been used by providers of intermediary services as one of the grounds for not implementing them in the first place, since providers erred on side of caution and decided not to implement such voluntary measures to avoid the risk of losing the liability exemption benefit simply because they would engage in voluntary measures.

51. How intermediary service providers will know what constitutes illegal content in different Member States?

With regard to orders to act against illegal content (Article 8), the order needs to include the statement of reasons specifying the provision of the national law or the EU law which provides that the content in question is illegal. In this case, the information will be in the order itself.

As to the notice and action mechanism contained in Article 14, its paragraph 2 sets out the requirements for that mechanism. This includes in particular that the mechanism is such as to facilitate the submission of notices that are sufficiently precise and adequately substantiated, including an explanation by the notice provider of the reasons for the alleged illegality. As such, the provider, acting as a diligent economic operator, must reasonably be able to determine on the basis of the notice, if the content in question is illegal. Where intermediaries carry out voluntary own-initiative investigations, such measures will have to be set out clearly in advance in their terms and conditions as per the obligations in Article 12.

52. Our interpretation is that the provision is concerned with the distinction between active and passive intermediary services (i.e. the general requirements on neutrality of the service). However, since this distinction is not codified in the articles in the Digital Services Act (mentioned in recitals only) we are concerned that the article might be misunderstood in its current setting. Given the exemption set in Article 6, we would appreciate if the Commission could elaborate on which obligations, if any, are imposed on platforms that obtain "actual knowledge of illegal activity or illegal content" as a result of "voluntary own-initiative investigations"? Has the Commission considered to clarify the provision in some regards, to make it clear the good samaritan provision applies to the distinction between active and passive intermediaries? This could for example be done by introducing an article codifying the general requirements for neutral/passive intermediary services in line with case law of the CJEU.

The DSA does not "codify" existing case-law in the enacting terms, but it reflects such case-law in the recitals, making also clear that it is subject to further interpretation by the Court. There are two pending cases where the Court might give further guidance on how to interpret the requirement of "neutrality" in relation to the conditional liability exemption for hosting services. As regards Article 6, recital 25 clarifies that "any such activities and measures that a given provider may have taken should not be taken into account when determining whether the provider can rely on an exemption from liability, **in particular as regards whether the provider provides** its service neutrally and can therefore fall within the scope of the relevant provision, without this rule however implying that the provider can necessarily rely thereon" (emphasis added).

53. Was it considered to allow for art. 6 - the Good Samaritan Clause - to apply only to a specific kind of content, such as marketplaces?

Article 6 of the DSA specifies that all providers of intermediary services can carry out voluntary own-initiative investigations without losing, for that reason alone, the liability exemptions provided for in its Articles 3, 4 and 5. The provision is intended to create legal certainty for all providers of intermediary services and avoid any disincentive to take measures, in good faith, either voluntarily or to comply with the requirements of EU law, including the DSA itself.

54. What are the judicial safeguards regarding the non-valuable information accessed upon conducting the own initiative activities foreseen within art. 6? Can these be used or taken advantage of in a different context and what are the instruments in this Regulation to avoid that?

Article 6 of the DSA is intended to address possible legal disincentives and legal uncertainties for service providers and refers to the exemptions from liability referred to in Articles 3, 4 and 5, which strictly relate to their role as intermediary in the transmission and hosting, respectively, of the information provided by recipients.

Article 6 does not exempt service providers from any obligation set through EU law as regards their own obligations in processing information and in particular in processing personal data or interpersonal communications data for the purpose of carrying out 'voluntary own-initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content'. Rights, obligations and prohibitions under the General Data Protection Regulation (EU) 2016/679 and the ePrivacy Directive 2002/58/EU continue to apply unchanged and the provision in Article 6 does not in itself provide for a legal basis for processing data within the respective meaning of the two legal instruments.

Further, a number of provisions under Chapter III of the DSA provide safeguards against abusive or arbitrary decisions taken by online platforms and other intermediary service providers in the course of their voluntary content moderation actions. For example, Article 12 imposes for all online intermediary service providers information requirements on any restrictions that they impose on their service and obliges them to act in a 'diligent, objective and proportionate manner' in enforcing such restrictions, with due regard to the rights and legitimate interests of all parties involved, including the applicable fundamental rights' of their users. Articles 13, 23, and 33, as well as Article 15(4), set the necessary level of transparency in such decisions, and information obligations (Article 15) and complaint mechanisms (Articles 17 and 18) provide for the necessary safeguards to users who could be subject to restrictions.

With regard to very large online platforms, Articles 26 and 27 impose an obligation to assess and to put in place reasonable, proportionate and effective mitigation measures for risks stemming

from the functioning and use of their service, including with regard to a number of fundamental rights.

Importantly, the regulatory oversight and enforcement provisions in Chapter V of the proposal ensure that all such obligations are diligently followed by service providers.

Article 7

55. Art. 15(1) of the eCommerce Directive has been transferred to Art. 7 of the draft DSA; will Member States be allowed to lay down obligations for providers to inform the competent public authorities of suspected illegal activities, as provided for in Art. 15(2) of the eCommerce Directive?

Article 21 of the DSA specifies the conditions under which online platforms are obliged to notify suspicions of criminal offences. Again, the purpose of the DSA is to harmonise the rules and avoid further fragmentation; hence, Member States would not be allowed to impose similar supplementary obligations, to the extent that they are harmonised by the DSA provisions.

Article 8

56. Does the law of a Member State that requires a provider with an establishment in another Member State to remove illegal content or to provide the sought information restrict the freedom to provide service? If yes, can such law of a Member State be regarded as "measure" that is capable of the derogations in Art. 3 para 4 ECD?

Recital 33 of the DSA refers to the conditions under which a removal order, that is an individual act taken by a national authority on the basis of such national legislation, does not in principle constitute a restriction to provide the relevant services on a cross-border basis within the meaning of Article 3 ECD, as it merely orders the intermediary, in a mandatory manner (hence the difference with the notice) to remove, or block access to, a given, specific piece of illegal content in that Member State or across the Union/worldwide, depending on the specific legal basis at stake and other considerations. Such an individual act is not derogating from Article 3 of the ECD, but it is simply not covered by it insofar as it does not restrict the freedom to provide services.

57. As far as we understood, Art. 8 DSA tends to establish an additional possibility for national authorities to address the provider directly in order to achieve that the provider complies with its decision and takes down illegal content or ensures that the illegal content is not uploaded again. We wonder whether this new system affects existing recognition and enforcement systems of civil law decisions between the Member States and between a Member State and a third country (since according to Art. 1 para 3 DSA the establishment of the provider does not necessarily have to be in the EU). Against this background:

- Does Art. 8 DSA affect the Brussels Ia-Regulation? Do any other provisions of the DSA have implications on the Brussel Ia-Regulation? If not, why is the Brussels Ia-Regulation not mentioned in Art. 1 para 5 DSA, nor is „national civil procedural law" mentioned in Art. 8 para 4 DSA?

- Does Art. 8 para 2 DSA intend to regulate additional requirements and conditions of national decisions, in particular decisions of civil courts in general (as far as these decisions concern the termination or prevention of an infringement)? This could be contrary to national civil procedural law, since a decision of a court does not necessarily contain the exact URL of the illegal content (see, for example, the ruling of the Austrian courts in the Glawischnig-case C-18/18). Also, a default decision could be issued without a statement of reasons if the provider as the defending party has not reacted to the lawsuit. Would such a decision that is not in totally in line with Art. 8 Abs. 2 DSA be not enforceable according to Brussels Ia? This could be contrary to Art. 3 para 3, Art. 4 para 2 and Art. 5 para 4, which leaves the possibility for a court to require termination or prevention of an infringement untouched. Or does Art. 8 cover purposes different from enforcement (which purposes would that be)?

- Does Art. 8 DSA have any implications on national provisions (not based on Union law) according to which a take-down-decision or a decision concerning an injunctive relief of another State can be recognized and enforced due to these national provisions (e.g. bilateral enforcement treaties)?

Article 8 of the DSA does not provide any additional (EU) legal basis to address providers directly with orders; it is not a self-standing empowerment for national authorities to issue such orders. The provision merely provides that an order which falls within its scope triggers a self-standing duty to inform the issuing authority about the follow-up taken without undue delay and imposes certain requirements relating to such removal orders. Furthermore, recital 33 recalls that, in principle, such orders do not represent a restriction to the provision of services and therefore are not subject to the specific requirements potentially applicable to such orders pursuant to Article 3 ECD. The requirements of Article 8(2) of the DSA are not exhaustive, accordingly, any order that falls within the scope of Article 8, may also be subject to additional elements which depend on the national legal basis and are not affected by Article 8 (such as deadlines for compliance with the orders as such, modalities for compliance such as blocking or removal, etc…), to the extent that they do not concern the matters harmonised in Article 8. Of course these modalities need also to comply with other provisions of EU law.

The injunctions issued by a court or administrative authority on the basis of Articles 3(3), 4(2) and 5(4) are not necessarily conditional on Article 8, as the latter covers specifically orders to act against specific items of illegal content.

The requirements for the cross-border recognition and enforcement (i.e. execution) of such an order, including the requirements set pursuant to Brussels I Regulation, remain unaffected by the DSA rules.

58. If the intermediary service fails to inform within a reasonable delay the requesting authority of the effect given to the order to act against illegal content, can the DSC of the Member State of the requesting authority initiate the cross border procedure among Digital Services Coordinators as provided in Article 45 (breach of Article 8 DSA: obligation to inform the authorities without undue delay)?

Yes.

59. Does the intermediary service, upon receiving an order from a national authority to act against illegal content, still have a choice as regards the decision to be taken regarding content moderation (the effect given to the order)? E.g. the service deems the measures included in the order too far-reaching and detrimental to fundamental rights of the users of the service. Or, will the intermediary service have absolutely no choice as regards the decision to be taken, and will have to proceed to remove the content. In that event, can the authorities of the Member State that requested the order be held liable if higher norms (such as the European Charter of Fundamental Rights) have been breached?

The order is mandatory for the addressee (as is any other administrative or judicial decision), so the addressee does not have discretion on whether to comply or not with it. Of course, if the addressee considers that the order is invalid (including due to breach of EU or national law), it can be challenged. The remedies to be triggered by the addressee to establish such invalidity will depend on the remedies applicable to such an order and the reasons for invalidity (e.g. whether they provoke nullity or it is necessary to annul it).

60. Regarding orders under Art. 8 and 9: What is the legal basis for the obligation of the providers to act against illegal content / provide information? Which Member State (country of origin of the provider or country in which the provider provides its services) can enforce orders under Art. 8 and 9 of the draft DSA and how? Should there be cross-border enforcement? If so, must the country of origin enforce an order from another Member State without further examination?

As noted above, Articles 8 and 9 do not provide any self-standing (EU) legal basis to address providers directly with orders. The articles require the existence of a valid national legal basis to issue such the orders. Depending on the applicable law constituting the legal basis for the issuance of the orders, they may well be enforceable against any intermediary when it comes to the obligations to remove/disable access illegal content or to provide information which they contain. The enforcement modalities (i.e. execution) of such an order will depend on the ordinary means of execution applicable to the order at stake.

61. What legal remedies are available to providers in order to defend themselves against orders under Art. 8 and 9 that may be unlawful?

When it comes to the obligation to remove/disable access to illegal content or to provide information, the ordinary remedies applicable to the order pursuant to the legal order in the issuing Member State are available. The order is NOT adopted on the basis of Articles 8 or 9, but on the basis of the corresponding national or EU legal basis. If the order does not comply with the requirements of Articles 8(2) or 9(2) DSA, Member States are obliged to provide effective remedy in accordance with the EU law principle of effective judicial protection.

62. Do the Articles mean that the authorities in the Member State, where the provider of an intermediary service is established, will be able to issue an order to act against illegal content and an order to provide information? Or will the authorities in another Member State issue these orders to providers of intermediary services established in yet another member state?

Both authorities can issue orders, if empowered by the applicable legal basis and both types of orders must comply with the requirements of Articles 8(2) and 9(2). The two articles do not make any distinction (of course the clarification in recital 33 relating to Article 3 of the ECD is only relevant for cross-border orders)

63. Considering the challenges experienced with illegal content being re-uploaded, could the Commission elaborate on why there is no “stay-down”-requirement for the platforms when first they have already been notified about specific illegal content on their platform and this content later reappears?

Article 8 does not specify all the modalities under which the order is to be complied with, it will depend on the specific legal basis underpinning the order. Hence it does not rule out the specification of modalities to avoid that a given and well-identified piece of illegal content may reappear, in accordance of course with the limits established by EU law as clarified in the ECJ case law (e.g. an order “to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content”, Case C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited,).

64. Les autorités françaises regrettent que l'article 8 se contente d'imposer au prestataire d'informer l'autorité des suites données à une injonction, mais n'énonce pas d'obligation directe de déférer à une injonction de retrait ou de blocage d'accès. Il serait préférable d'énoncer explicitement une obligation de se conformer à l'injonction, y compris dans un cadre transfrontalier.

The binding effect of the order occurs directly through the legal basis of the order; it is not necessary (and it could be counterproductive and in contrast to the principle of ne bis in idem) to establish a second binding effect on the basis of the Regulation. Given the diversity of situations potentially covered (criminal law, civil law, administrative law), such an effect would be difficult to reconcile with the objectives and the legal basis of the regulation.

65. Does the order Article 8 have to be addressed to any establishment of the intermediary or the main establishment?

The order shall be addressed to the intermediary responsible for the service at stake. Moreover, Article 10 of the DSA provides that such intermediary shall establish a single point of contact that allows for direct communication, by electronic means, with Member States' authorities.

66. Could the Commission play through an example of the process of a DSA order and articulation with existing legislations, such as a copyright infringement of a movie uploaded to a video-sharing platform that is the object of an order from MS A to MS B where the platform is established? Which provisions of the DSA would apply, and which provisions of the Copyright Directive would apply? Would the platform have to comply with orders/procedure of the DSA, and if so, which are its possibilities for redress and dispute resolution (under DSA or under the Copyright Directive)?

The Copyright in the DSM Directive 2019/790 does not include any rules on court injunctions. Relevant obligations for Member States to provide for injunctions against intermediaries whose services are used by a third party to infringe an intellectual property right can be found in Directive 2001/29/EC and Directive 2004/48/EC. The DSA is without prejudice to Union law on copyright and related rights (Article 1(5)(c)). The redress possibilities against such injunctions will continue to be based on national law transposing such Directives.

67. If articles 8 and 9 only come into play based on national rules, what happens if there are no corresponding rules in national law?

If there are no corresponding rules in national law, or other applicable Union law, the Member State at stake cannot make use of Articles 8 and 9 DSA.

68. What is the Commission's view on the protection of individuals' fundamental rights with respect to the execution of cross-border orders contained in Articles 8 and 9? What happens if an order is retroactively found to constitute an infringement on the Charter?

The orders under Articles 8 and 9 are issued on the basis of applicable Union or national law. In case the intermediary service provider considers that the order is not lawful because it fails to respect the requirements of Articles 8 or 9, in the light of the EU law principle of effective judicial protection, Member States must ensure that there are effective means to challenge the order before national courts. The recipient of the services who is impacted by the order must also have redress possibilities at national level. The DSA does not include rules on the potential liability of the service provider for the removal of content which happened not to be illegal. The DSA only exempts it from liability for the illegality of the content, not for liability resulting from the removal of legal content.

69. If an intermediary service removes content in utmost good faith based upon the explanation of illegality provided by a Member State national administrative authority yet it is subsequently held liable for breach of the material provider's right to freedom of expression and it transpires that the statement of illegality was issued in error what indemnity is available to the intermediary service?

The intermediary services provider is normally obliged to act on an order from national authorities, without assessing its well-founding, unless it has concerns about its legality. In this regard, orders are different from notices (Article 14), which require the provider's assessment on whether to act upon the notice. Therefore, any restriction of the freedom of expression of the recipient of the service resulting from the removal order is attributable to the issuing authority. Relevant means of redress at national level would then apply.

70. How proportionality principle will be ensured in the process of removal of illegal content, given that the Regulation does not impose an obligation to initially use more lenient means?

As explained earlier, the basis for the orders as such is to be found in other national or Union laws. Equally, the possibility to use more lenient means from the authorities' side is to be assessed in the course of application of such laws.

71. Art. 8 of DSA provides that an authority from one Member State will be able to issue an order to act against illegal content also against an intermediary located in another Member State. What if there will be differences in this assessment between MS whether content indicated in the order is illegal? Has the EC considered the potential for disputes between Member State authorities over cross-border removal orders and how such disputes might be resolved?

Since the orders falling within the scope of Article 8(1) concern a specific item of illegal content, they in principle do not set requirement for the intermediary service provider to assess the

content, but rather identify precisely an illegal piece of illegal content carried on/hosted by the intermediary that must be removed/blocked on the basis of a national or EU legal basis. To cater for the exact situation whereby a piece of content is illegal in one Member State but not in another Article 8(2)(b) should be read together with recital 31, which clarifies that this circumstance should be taken into account when determining the territorial scope of the order.

72. How an intermediary will be able to confirm the authenticity of an order received under Article 8 and Article 9, and how to provide for a secure communication channel between the intermediary and the issuing authority to ensure security and integrity of processed data?

Save for the requirements set in Article 8(2), Article 8 does not regulate other formal requirements of orders nor modalities to comply with them. This depends on national law (or other acts of EU law) regulating the order and the terms of the order.

73. Considering that the interpretation that the obligations set out in the articles on orders are limited to procedural aspects and handling of an order from an authority is correct, meaning that the rules risk not being relevant if there is no material support for an order regarding illegal content in another EU-regulation, we wonder on the need for the provision? Procedural rules regarding orders are also found in other legal acts that contain rules on orders. In case they are limited to procedures only, what is the added value of additional rules if they are limited to procedures? We would appreciate the Commission's view on this key issue for understanding of the regulation. If the provision is intended to serve as material support for the Member States to be able to issue orders for illegal content, several other questions arise. One key issue is whether the examination of an order is to be carried out in accordance with national law where the supplier has its registered office or whether the supplier also has to comply with the legislation of the issuing state. I.e. does a Swedish supplier have to act on an order from Poland based on what is illegal under Swedish law? Or should the supplier also comply with Polish legislation? The question arises in the light of the country of origin-principle of the eCommerce Directive, the ECJ's judgment in Glawischnig-Piesczek v. Facebook, Article 8.2 (b) of the proposal and recitals 31 and 33 of the proposal. In this context, how the definition in article 2 (g) should be understood, i.e. “irrespective of the precise subject matter or nature of that law” -does it refer to all forms of (national) legislation or only criminal law?

The added value of Articles 8 and 9 is that they provide legal certainty to both Member States and providers with regard to orders addressed to providers which are not established in the territory of the issuing Member State, and impose certain uniform requirements for removal orders and orders for information. Recital 33 refers to the fact that orders related to specific items of illegal content and information, containing specific elements do not in principle restrict the intermediaries’ freedom to provide services across borders, hence the country of origin principle of Article 3 ECD does not apply. Articles 8 and 9 also set an information obligation for intermediary service providers towards the issuing authorities. The issuing Member State has the right to protect its citizens against content which is illegal in its territory. Hence, in the example used in the question, if an order from Poland is based on Polish law, such order may have effects in Poland.

The country of origin principle is not endangered through this mechanism insofar as such orders are not considered restrictions to the freedom to provide services.

74. What is expected of the provider if it finds that a specific item of content is illegal? Can an individual, an entity, a Member State, a trusted flagger, The Digital Service Coordinator, the Commission or the European Board for Digital Services act in any way if a provider chooses *not to remove/block access to* content that is considered illegal? We note that the provisions related to penalties in articles 42 and 58 respectively, can be used if there is a failure to comply with the regulation. This requires that there are clear obligations in the relevant articles. In our reading, there is no direct obligation to remove or block specific content in the provisions on orders. Hence, can the provider's (lack of) actions have any consequences?

The obligation to comply with the obligations to remove/disable access to illegal content or to provide information contained in such orders is set out in national or Union law, hence the enforcement of such obligations must also be done on the basis of such laws. The obligations provided in the DSA are obligations to inform the authorities about the actions taken and the moment it was taken (Article 8(1)), or to inform the authority of the receipt of the order and the effect given to it (Article 9(1)). The enforcement of these latter obligations will be done on the basis of the system set out in the DSA (Chapter IV).

75. How Art. 8 and Art. 9 might be enforced in relation to the providers of intermediary services established outside the EU (as per Art. 1 (3))?

As noted, the enforcement of the DSA obligations in Article 8(1) and 9(1) takes place in accordance with the rules set out in Chapter IV. If the provider is not established in the EU, it has the obligation to appoint a legal representative (Art. 11(1)). The Digital Services Coordinator of the Member State where the legal representative is established has jurisdiction (Art. 40(2)).

76. Does Article 8 intend to provide an agreed system for the issuing of cross-border removal orders, similar to the TCOR, for the removal of content online, and in which case what is the status of content that is illegal in one Member State but not in another, particularly not in the Member State in which the service provider has its main establishment?

- Or, is Article 8 intended to simply provide a uniform process for a Member State to enforce the disabling of access to illegal content from its own jurisdiction, irrespective of where the service provider has its main establishment?
- Or, is it that the DSA will provide the legal basis?
- Or, is it that the legal basis has to be provided for in either national law of a MS or in Union law such as the TCOR?

Articles 8 and 9 are not empowering provisions. The legal basis for issuing orders should be found in national laws or other applicable Union laws. Hence, Articles 8 and 9 are not similar to the Regulation on terrorist content online, which is providing a legal basis for the issuing and processing of orders against terrorist content.

77. What is the meaning of "undue delay" in art. 8 and in art. 9? Why not a negative deadline ("no later than…" – as in art. 45, 4)? Is the meaning of "undue delay" in art. 8, 1) the same as in art. 8, 3)? Does that apply both to the DSC of establishment and to the DSC of destination?

The DSA is a horizontal instrument. Articles 8 and 9 apply to orders against all types of illegal content and related to the provision of information in diverse sectors. The DSA does not harmonise the time limits for the action that the relevant providers are to take, that is, either to remove/disable access to certain specific items of illegal content or to provide certain specific information. The requirement of 'undue delay' refers to the obligation imposed on intermediary services providers to inform the issuing authorities about the actions taken; it does not refer to the taking of said action itself.

'Undue delay' does not imply a fixed time frame. The meaning of this wording will depend on a case-by-case assessment. It naturally indicates that the providers are to inform the authorities as soon as reasonably possible under the given circumstances of the effects they gave to the orders.

Article 8(3) and 9(3) entail an obligation for the Digital Services Coordinator of the issuing Member State to transmit a copy of the order to all other Digital Services Coordinators.

78. Is it in any way reflected or considered in the procedural structure of art. 8 and art. 9, the procedural qualitatively variations governing different spheres of activities or of content? For instance, the greater the importance of the matter in terms of national security, the greater the means made available by the governments. Is such procedural hierarchical order reflected or accounted for in any way in this Regulation, given its attempt to be neutral, though it covers a wide range of (potentially conflicting or subject to different though EU-wide value standards) issues? Do the means follow the ends, so to speak, or are the means impassive whether the order to act or provide information follows the flagging of the selling of counterfeit goods or a matter of national security? Should not the timelines correspond to the quality at stake?

The substantive requirements for an order under Articles 8 or 9 are not set out in the DSA. Save for the issues harmonised in Articles 8(2) and 9(2), and without prejudice to the requirements resulting from other provisions of EU law, Member States remain competent to adopt national legislation to address illegal content online, taking into consideration considerations such as the gravity of the illegal content. For instance, the requirement for a specific timeframe for giving effect to an order is not set out in the DSA. The national law may provide for such timeframes, which are binding for the intermediary services providers.

Article 8 (2)

79. How Article 8 (2)(b) should be understood, specifically what “territorial scope of the order” means. The same paragraph refers to “the applicable rules of Union and national law” as well as “general principles of international law”. What rules and principles are specifically thought of in this paragraph? A concrete example: If a comment on a social media is illegal in the Member State where the commenting user is living, but not illegal in the Member State where the online platform is established, could the Member State of the user then give direct orders to the online platform - and this without cooperation with the Member State of the online platform’s establishment?

In accordance with Article 8(2) the territorial scope, as defined in the order, must not exceed what is strictly necessary to achieve its objective. In general, this scope may depend on the applicable Union or national law enabling the issuance of the order and on the circumstances of the case. For instance, if the order is issued in relation to an infringement of an EU-wide right, then its scope may potentially be pan-EU.

The illegality pertains to the content, not to the intermediary service at stake. If a MS identifies a specific piece of content illegal and orders its removal in accordance with the conditions of Article 8, the place of establishment of the intermediary service (mere-conduit, hosting, etc…) is irrelevant, insofar as this order does not restrict the freedom to provide services.

80. How to define and practically understand ‘what is strictly necessary to achieve its objective’?

The territorial scope of the order must be proportionate to its objective. The objective is defined by the legal basis, hence the order, to be covered by Article 8, must be limited to what is necessary to achieve the objective pursued by that legal basis. If for instance the legal basis of the order is the violation of a national prohibition for the dissemination certain types of illegal content (e.g. information on the online sale of alcohol hosted by a marketplace prohibited in a given Member States), blocking access to that specific content from that Member State could be sufficient to achieve the objective, while a broader removal could exceed it.

81. Concerning the blocking/removal of illegal content, with the Nordic Resistance Movement banned in Finland, is the Finnish authority empowered to issue an order to a service provider based in another Member State to disable access to NRM content across all Member States, or just in their jurisdiction? Similarly, in relation to provision of services, and where it is illegal to sell alcohol online in Sweden, is it correct to understand that a Swedish authority can disable access to online retailers of alcohol in the Swedish jurisdiction, but that this retailer can continue to operate in other Member States? And what would occur, either relating to the Nordic Resistance Movement or the sale of alcohol online as merely illustrative examples, if the issuing authority requested that access to this content be disabled outside of their respective jurisdictions?

As mentioned above, the authority issuing the order must assess what the necessary territorial scope of the order should be, especially where the scope may extend to other Member States and where, given the objective pursued, the information at issue is not likely to constitute illegal content in other Member States. If the order exceeds this limit, it will not be issued in conformity with Article 8(2). In the specific examples indicated thereto, it would indeed be necessary to carefully assess whether a worldwide removal order would be proportionate.

82. How can the Digital Services Coordinator become involved in the enforcement of non-compliance with Articles 8 and 9 (which are contained in Chapter 2) when Article 40 limits the jurisdiction of the Digital Services Coordinator to the provisions of Chapters 3 and 4.

Article 42 provides for the obligation to provide penalties for infringements of the DSA by intermediary services providers “under their jurisdiction”, hence it envisages the possibility for the DSC of the country of origin to impose penalties also for failure to comply with Art 8(1) and 9(1), that is, failure provide information on follow-up to order by the intermediaries within their jurisdiction.

83. If our understanding of the Commission’s clarification is correct, what options of redress will be provided to the service provider in Member State A, in terms of Article 8 paragraph (2)(a) of the proposed DSA text? Will redress only be allowed to be sought in the country of consumption or also in the country of origin? In the circumstance defined in question 1 above, what is expected of an ISP which is obliged to take action against the content provided from within Member State A in this scenario of a conflict of laws?

The order is subject to the ordinary remedies provided for under the issuing Member State. In the light of the principle of effective judicial protection, each MS must provide for effective judicial remedy against the orders falling within the scope of DSA.

84. What happens in a scenario where the national law of a Member State which is used as the legal basis to determine that content is illegal, is itself in violation of EU law?

The described scenario corresponds to a general situation where an administrative or a judicial decision is issued on the basis of the national law which is found to be incompatible with EU law. The DSA does not change anything in this respect.

85. In Articles 8(2)(c) and 9(2)(c), why should orders be written in the “language declared by the provider”, instead of being acceptable if written in any of the official languages of the EU? In the interest of expeditious action by Member States affected by such illegal content, it would be faster for the MS to simply write to the provider in their national languages. It should be up to the provider to have access to translation services to comply with the Order if they already operate across multiple jurisdictions.

The condition laid down in Articles 8(2)(c) and 9(2)(c) defines certain linguistic requirements to be complied with when transmitting the orders to the point of contact in coherence with the solution set out Article 10(3) and in line with other pieces of EU law.

86. Providing exact URL might prove difficult, since the illegal content in question may be already removed or moved elsewhere and the URL used as an example in the order will become obsolete. Does "additional information" cover, for example, enclosing screenshots of illegal content?

With regard to orders to act against a specific item of illegal content, Article 8(2)(a) second indent requires orders to contain one or more exact uniform resource locations, and where necessary, additional information enabling the identification of the illegal content concerned. In case of non-compliance with this requirement, the order would be in breach of the DSA obligation in Article 8(2)(a).

Article 8 (3)

87. The text does not provide an obligation for the authority issuing the order to inform its own national Digital Service Coordinator (either to put the DSC in copy when sending its order, or to transmit the DSC a copy without undue delay). Does the text impose an "implicit obligation" for national authorities issuing the order to notify ("put in cc") their country's Digital Services Coordinator or is there room for further clarifying this in Article 8(3)?

The modalities under which the DSC should be informed of the order are not regulated by DSA (eg contextual notification; information forwarded afterwards, etc…). However it is indeed necessary that the issuing authority informs its national DSC in an appropriate manner (obligation of result), so that this can transmit the order in the information sharing system.

88. What is the reason for individual notification to all Member State DSCs whenever a notice is issued (Article 8 subpara 3) when an online register of such notices would be far less labor intensive? It is believed that such an approach, by providing a register with limited details of each notice, would address some concerns around disseminating full details of the notice such as:

- Whether it would be necessary to provide for scenarios where the fact of an ongoing criminal investigation would make the dissemination of a content removal order to all DSCs or the publication of such orders inappropriate, and

- Whether it is possible that the uniform resource locators and potential other information required to be contained in content removal could be considered personal data or even sensitive personal data, and whether therefore, there is sufficient legal basis in the DSA for the dissemination of all content removal order to all DSCs or the publication of such orders?

The transmission of the order within the information sharing system is not a public transmission, as this is limited only to information sharing among specific authorities (COM, Board and other DSCs) and Article 67 requires the system to be "secure". Also, Article 8 does not require a "contextual/immediate" information to the DSCs, if investigation needs are to be preserved. Similarly, as the DSA is without prejudice to the GDPR, the safeguards as regards personal data should be maintained.

Article 9

89. With regard to Art. 9 of the draft DSA, how can Member States protect the public interest, especially with regard to the local level?

The orders to which Article 9 DSA refers are orders issued by the competent national authorities (administrative or judicial) on the basis of applicable Union or national law. These orders must in particular contain a statement of reasons explaining why the requested information is necessary and proportionate to determine compliance by the recipients of the intermediary services with national or Union rules. Therefore, on the basis of the information obtained through such orders, Member States can assess the compliance of recipients of intermediary services with local rules.

90. S'agissant de l'article 9, elles estiment que les propositions sur la transmission d'informations par les services intermédiaires aux autorités répressives et administratives sont insuffisantes et devraient être améliorées pour permettre une coopération renforcée entre ces prestataires et les autorités nationales, ce qui permettrait également de clarifier leur articulation avec le futur règlement e-evidence. Les autorités françaises souhaitent interroger la Commission sur l'absence de disposition imposant aux fournisseurs de services intermédiaires de se conformer aux injonctions des autorités des Etats membres portant sur le retrait ou le blocage d'accès aux contenus constituant des infractions pénales. Elles s'interrogent par ailleurs sur l'articulation du mécanisme de transmission d'informations avec le futur règlement e-evidence. À cet égard, elles souhaitent également savoir de quelle manière la Commission entend améliorer la lutte contre les contenus infractionnels. Elles estiment ainsi qu'il est nécessaire, à cette fin, de renforcer les propositions relatives à la transmission d'informations par les prestataires de services intermédiaires à la demande des autorités répressives et administratives tout en clarifiant l'articulation avec le futur règlement « e-evidence », en imposant la transmission des données d'identification lorsqu'elles sont demandées par les autorités dans le cadre d'enquêtes pénales, qui serait assortie des garanties adéquates.

The DSA explicitly clarifies in Article 1 the relationship between the e-evidence proposal and the DSA, noting that the DSA is without prejudice to the rules laid down in the future e-evidence legislative act.

The DSA is conceived as a horizontal instrument. The conditions to remove specific types of illegal content and to provide information about the recipients of intermediary services are necessarily

those set out in national law, in accordance with Union law, taking into consideration the particularities of each sector. If the DSA imposed an obligation to remove notified content, the same obligation would be repeated in both EU and national law, thereby creating problems with the enforcement of such obligation.

However, by clarifying that orders related to specific items of illegal content and information, do not in principle restrict the intermediaries' freedom to provide services across borders, and imposing certain uniform conditions for those orders (Articles 8(2) and 9(2)), the DSA aims to address the proliferation of illegal content online. Additionally, Articles 8 and 9 provide for a system for the cross-border treatment of orders, under certain conditions, which leaves the single market principles unaffected.

91. Can the information gathered under Article 9 be used for purposes in other legislations, such as DMA?

The orders to provide information which fall under the scope of Article 9 relate to information about the recipients of the service provided by the intermediary services provider. Article 9, paragraph 2(a) provides that orders must contain a statement of reasons explaining why the requirement to provide the information is necessary and proportionate to determine compliance by the recipients of the intermediary services with applicable Union or national rules. Therefore, the information collected on the basis of this article does not relate to the provider of intermediary services. Hence, its application for the purposes of DMA does not seem relevant.

92. What if a service provider refuses to disclose the information requested and insists on being it a trade secret - as per information requested - by Art.9?

Article 9 does not regulate the enforcement of the order, including the issue referred to in the question. In general, the situation in question is also unlikely to arise in practice, since Article 9 is not related to information about the intermediary service provider, but about the recipients of the intermediary service. For example, in case recipients of the service are traders, the requested information may relate to information already collected by the online marketplace covered by Article 22 DSA. In any event, the authority issuing the order under Article 9 DSA must explain why the information is necessary and proportionate to determine compliance with national and EU laws. The order must also contain information about redress available to the provider and the recipients of the service concerned.