Council of the European Union
General Secretariat

Brussels, 22 September 2021

Interinstitutional files:
2020/0361 (COD)

WK 11167/2021 INIT

LIMITE

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

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

NOTE

From:	DK delegation
To:	Delegations
Subject:	Digital Services Act: DK comments on compromise text, Articles 10-24

Council of the European Union

Brussels, 9 September 2021
(OR. en)

Interinstitutional File: 2020/0361(COD)

11459/1/21 REV 1

LIMITE

MI 639
CODEC 1180
COMPET 614
JAI 948
TELECOM 330
CT 115
PI 75
AUDIO 87
CONSOM 191

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	9288/21
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC - Presidency compromise text on Chapters III, with respective recitals

In view of the upcoming Working Party for Competitiveness and Growth on 16 September 2021, delegations will find in Annex to this note a second Presidency compromise text on Chapter III, Sections 1, 2 and 3, including their respective Recitals (34-52).

Changes compared to the first redraft of the proposal (doc. 9288/21) are marked in **bold, underlined and highlight** for the new text and in ~~strikethrough~~ for the deletions.

ANNEX

2020/0361 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

[Having regard to the opinion of the Committee of the Regions[2],**]**

~~Having regard to the opinion of the European Data Protection Supervisor[3],~~

Acting in accordance with the ordinary legislative procedure,

---

1 OJ C , , p. .
2 OJ C , , p. .
3 ~~OJ C, p.~~

(34) In order to achieve the objectives of this Regulation, and in particular to improve the functioning of the internal market and ensure a safe and transparent online environment, it is necessary to establish a clear and balanced set of harmonised due diligence obligations for providers of intermediary services. Those obligations should aim in particular to guarantee different public policy objectives such as the safety and trust of the recipients of the service, including minors and ~~vulnerable~~ users **at particular risk of being subject to hate speech, sexual harassments or other discriminatory actions**, protect the relevant fundamental rights enshrined in the Charter, to ensure meaningful accountability of those providers and to empower recipients and other affected parties, whilst facilitating the necessary oversight by competent authorities.

(35) In that regard, it is important that the due diligence obligations are adapted to the type**, size** and nature of the intermediary service concerned. This Regulation therefore sets out basic obligations applicable to all providers of intermediary services, as well as additional obligations for providers of hosting services and, more specifically, **providers of** online platforms and **of** very large online platforms. To the extent that providers of intermediary services may fall within those different categories in view of the nature of their services and their size, they should comply with all of the corresponding obligations of this Regulation. Those harmonised due diligence obligations, which should be reasonable and non-arbitrary, are needed to achieve the identified public policy concerns, such as safeguarding the legitimate interests of the recipients of the service, addressing illegal practices and protecting fundamental rights **enshrined in the Charter** online.

(36) In order to facilitate smooth and efficient communications relating to matters covered by this Regulation, providers of intermediary services should be required to ~~establish~~ **designate** a single **electronic** point of contact and to publish relevant information relating to th**at**~~eir~~ point of contact, including the languages to be used in such communications. The **electronic** point of contact can also be used by trusted flaggers and by professional entities which are under a specific relationship with the provider of intermediary services. In contrast to the legal representative, the **electronic** point of contact should serve operational purposes and should not **be required** ~~necessarily have~~ to have a physical location.

(37) Providers of intermediary services that are established in a third country that offer services in the Union should designate a sufficiently mandated legal representative in the Union and provide information relating to their legal representatives**. This should allow for the effective oversight and, where necessary, enforcement of this Regulation by the Board,**

the Commission and the national competent authorities, including ~~the~~ authorities executing the powers ~~coferred to~~ of these competent authorities ~~, so as to allow for the effective oversight and, where necessary, enforcement of this Regulation~~ in relation to those providers. It should be possible for the legal representative to also function as **electronic** point of contact, provided the relevant requirements of this Regulation are complied with.

(38) Whilst the freedom of contract of providers of intermediary services should in principle be respected, it is appropriate to set certain rules on the content, application and enforcement of the terms and conditions of those providers in the interests of transparency, the protection of recipients of the service and the avoidance of unfair or arbitrary outcomes. **When applying and enforcing restrictions imposed in relation to the use of their service, providers of intermediary services should pay regard to international standards for the protection of fundamental rights, such as the UN Guiding Principles on Business and Human Rights, which can provide guidance to observe the applicable fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union**.

(39) To ensure an adequate level of transparency and accountability, providers of intermediary services should annually report, in accordance with the harmonised requirements contained in this Regulation, on the content moderation they engage in, including the measures taken as a result of the application and enforcement of their terms and conditions. However, so as to avoid disproportionate burdens, those transparency reporting obligations should not apply to providers that are micro- or small enterprises as defined in Commission Recommendation 2003/361/EC[4].

(40) Providers of hosting services play a particularly important role in tackling illegal content online, as they store information provided by and at the request of the recipients of the service and typically give other recipients access thereto, sometimes on a large scale. It is important that all providers of hosting services, regardless of their size, put in place user-friendly notice and action mechanisms that facilitate the notification of specific items of information that the notifying party considers to be illegal content to the provider of hosting services concerned ('notice'), pursuant to which that provider can decide whether or not it agrees with that assessment and wishes to remove or disable access to that content ('action'). **Such mechanisms should be at least as easy to find and use as notification mechanisms for content that violates the terms and conditions of the hosting service provider.**

---

[4] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Provided the requirements on notices are met, it should be possible for individuals or entities to notify multiple specific items of allegedly illegal content through a single notice. The obligation to put in place notice and action mechanisms should apply, for instance, to file storage and sharing services, web hosting services, advertising servers and paste bins, in as far as they qualify as providers of hosting services covered by this Regulation.

(41) The rules on such notice and action mechanisms should be harmonised at Union level, so as to provide for the timely, diligent and objective processing of notices on the basis of rules that are uniform, transparent and clear and that provide for robust safeguards to protect the right and legitimate interests of all affected parties, in particular their fundamental rights guaranteed by the Charter, irrespective of the Member State in which those parties are established or reside and of the field of law at issue. The fundamental rights include **but are not limited to**, as the case may be, the right to freedom of expression and information, the right to respect for private and family life, the right to protection of personal data, the right to non-discrimination and the right to an effective remedy of the recipients of the service; the freedom to conduct a business, including the freedom of contract, of service providers; as well as the right to human dignity, the rights of the child, the right to protection of property, including intellectual property, and the right to non-discrimination of parties affected by illegal content. **Providers of hosting services should act upon notices in a timely manner, in particular, by taking into account the type of illegal content being notified and the urgency of taking action. For instance, providers can be expected to act without delay when allegedly illegal content involving an imminent threat to life or safety of persons is being notified. The provider of hosting services should inform the individual or entity notifying the specific content without undue delay after taking a decision whether to act upon the notice.**

Regarding recital 41 we support that this recital now reflects that providers of hosting services should act upon notices in a timely manner, in particular, by taking into account the type of illegal content being notified and the urgency of taking action. However, we still find that we could be even more ambitious. The DSA should entail a clearly defined timeline for acting on notifications of illegal content including a differentiated time limit so that illegal content with a serious detrimental effect, such as terrorism-related content and illegal products, is taken down more quickly than other illegal content. Thus, we have submitted a proposal for amendments to art. 5.

(41a) Those mechanisms should allow for the submission of notices which are sufficiently precise and adequately substantiated to enable the hosting provider concerned to take an informed and diligent decision in respect of the content to which the notice relates, in particular whether or not that content is to be considered illegal content and is to be removed or access thereto is to be disabled. Those mechanisms should be such as to facilitate the provision of notices that contain an explanation of the reasons why the notice provider considers that content to be illegal content and a clear indication of the location of that content. The information provided in the notice should contain sufficient information to enable the provider of intermediary services to identify, without a detailed legal examination, that that content is manifestly illegal and that its removal is compatible with freedom of expression. ~~Where, on the basis of the information provided in the notice, it is not evident to a layperson, without any substantive analysis, that the content is illegal, such content should not be removed nor should access to it be disabled.~~ Except for the submission of notices relating to offences referred to in Articles 3 to 7 of Directive 2011/93/EU, it is necessary to know the identity of the notice provider, for instance to avoid misuses or to identify alleged infringements to personality rights or intellectual property rights.

(42) Where a hosting service provider decides to remove or disable information provided by a recipient of the service **or to otherwise restrict its visibility or monetisation**, for instance following receipt of a notice or acting on its own initiative, including **exclusively by** ~~through the use of~~ automated means, that provider should inform **in a clear and easily comprehensible way** the recipient of its decision, the reasons for its decision and the available redress possibilities to contest the decision, in view of the negative consequences that such decisions may have for the recipient, including as regards the exercise of its fundamental right to freedom of expression. That obligation should apply irrespective of the reasons for the decision, in particular whether the action has been taken because the information notified is considered to be illegal content or incompatible with the applicable terms and conditions. **Restriction of visibility may consist in demotion in ranking or in recommender systems, as well as in limiting accessibility by one or more receipients of the service, including 'shadow banning'. The monetisation via advertising revenue of content provided by the recipient of the service can be restricted by suspending or terminating the monetary payment or revenue associated to that content. Hosting service providers should also publish such decisions and respective statement of**

reasons ~~the same information~~ in a publicly available structured database maintained by the Commission. The database should not include the allegedly illegal content itself or the content infringing the terms and conditions of the service provider, but only the information presented in the statement of reasons for restricting the content, and should exclude~~ing~~ personal data. Available recourses to challenge the decision of the hosting service provider should always include judicial redress **in accordance with the laws of the Member State concerned.**

(42a) ***[previous recital 48]*** A **provider of hosting services** ~~n online platform~~ may in some instances become aware, such as through a notice by a notifying party or through its own voluntary measures, of information relating to certain activity of a recipient of the service, such as the provision of certain types of illegal content, that reasonably justify, having regard to all relevant circumstances of which the ~~online platform~~**provider of hosting services** is aware, the suspicion that the recipient may have committed, may be committing or is likely to commit a ~~serious~~ criminal offence involving a threat to the life or safety of person **or persons**, such as offences specified in **Directive 2011/36/EU of the European Parliament and of the Council**[5]**,** Directive 2011/93/EU of the European Parliament and of the Council[6] **or Directive (EU) 2017/541 of the European Parliament and of the Council**[7]**.** In such instances, the ~~online platform~~**provider of hosting services** should inform without delay the competent law enforcement authorities of such suspicion, providing all relevant information available to it, including where relevant the content in question and an explanation of its suspicion. This Regulation does not provide the legal basis for profiling of recipients of the services with a view to the possible identification of criminal offences by **providers of hosting services**~~online platforms~~. **Providers of hosting services**~~Online platforms~~ should also respect other applicable rules of Union or national law for the

---

5 **Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA (OJ L 101, 15.4.2011, p. 1).**

6 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

7 **Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).**

protection of the rights and freedoms of individuals when informing law enforcement authorities.

(42b) ***[previous recital 48]*** Action against illegal content can be taken more quickly and reliably where **providers of** **hosting services** ~~online platforms~~ take the necessary measures to ensure that notices submitted by trusted flaggers through the notice and action mechanisms required by this Regulation are treated with priority, without prejudice to the requirement to process and decide upon all notices submitted under those mechanisms in a timely, diligent and objective manner. **Such trusted flagger status should be awarded by the Digital Services Coordinator of establishment and should be recognised by all providers of online platforms within the scope of this Regulation.** Such trusted flagger status should only be awarded to entities, and not individuals, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content~~, that they represent collective interests~~ and that they work in a diligent and objective manner. Such entities can be public in nature, such as, for terrorist content, internet referral units of national law enforcement authorities or of the European Union Agency for Law Enforcement Cooperation ('Europol') or they can be non-governmental organisations and **private or** semi-public bodies~~,~~ such as the organisations part of the INHOPE network of hotlines for reporting child sexual abuse material and organisations committed to notifying illegal racist and xenophobic expressions online. ~~For intellectual property rights, organisations of industry and of right-holders could be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions.~~ The rules of this Regulation on trusted flaggers should not be understood to prevent **providers of** online platforms from giving similar treatment to notices submitted by entities or individuals that have not been awarded trusted flagger status under this Regulation, from otherwise cooperating with other entities, in accordance with the applicable law, including this Regulation and Regulation (EU) 2016/794 of the European Parliament and of the Council.[8]

[8] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53.

(43) To avoid disproportionate burdens, the additional obligations imposed on **providers of** online platforms under this Regulation should not apply to micro or small enterprises as defined in Recommendation 2003/361/EC of the Commission,[9] unless their reach and impact is such that they meet the criteria to qualify as very large online platforms under this Regulation. The consolidation rules laid down in that Recommendation help ensure that any circumvention of those additional obligations is prevented. The exemption of micro- and small enterprises from those additional obligations should not be understood as affecting their ability to set up, on a voluntary basis, a system that complies with one or more of those obligations.

(44) Recipients of the service **and individuals and entities that have submitted a notice** should be able to easily and effectively contest certain decisions of **providers of** online platforms that negatively affect them. Therefore, **providers of** online platforms should be required to provide for internal complaint-handling systems, which meet certain conditions aimed at ensuring that the systems are easily accessible and lead to swift and fair outcomes**, and are subject to human review**. **Such systems should enable all recipients of the service ~~users~~ to lodge a complaint and should not set up formal requirements such as referral to specific, relevant legal provisions or elaborate legal explanations. The possibility to lodge a complaint for the reversal of the contested decisions should be available for at least six months, to be calculated from the time of informing the recipient of the service of the decision.** In addition, provision should be made for the possibility of out-of-court dispute settlement of disputes **in good faith**, including those that could not be resolved in satisfactory manner through the internal complaint-handling systems, by ~~certified~~ **authorised** bodies that have the requisite independence, means and expertise to carry out their activities in a fair, swift and cost-effective manner. **Out-of-court dispute settlement bodies should preferably be free of charge. In the event that costs are applied the fees charged by the dispute settlement bodies should be reasonable, accessible, attractive, inexpensive for consumer and proportionate, and assessed on a case-by-case basis. Online platforms should be able to refuse to engage in dispute settlement in the case when the same dispute regarding the same content has already been resolved or is being reviewed by another dispute settlement body provided that they comply with the existing or future outcome of the dispute settlement consistently. Recipients of the**

[9] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

service and individuals and entities that have submitted notices should be able to choose between the internal complaint mechanism, an out-of-court dispute settlement or judicial redress. The possibilities to contest decisions of **providers of** online platforms thus created should complement, yet leave unaffected in all respects, the possibility to seek judicial redress in accordance with the laws of the Member State concerned**, and ultimately exercising their right of access to the judicial system as provided for in Article 47 of the Charter of Fundamental Rights of the European Union**.

(45) For contractual consumer-to-business disputes over the purchase of goods or services, Directive 2013/11/EU of the European Parliament and of the Council[10] ensures that Union consumers and businesses in the Union have access to quality-certified alternative dispute resolution entities. In this regard, it should be clarified that the rules of this Regulation on out-of-court dispute settlement are without prejudice to that Directive, including the right of consumers under that Directive to withdraw from the procedure at any stage if they are dissatisfied with the performance or the operation of the procedure.

~~(46) *[moved to Recital 42b]* Action against illegal content can be taken more quickly and reliably where **providers of** online platforms take the necessary measures to ensure that notices submitted by trusted flaggers through the notice and action mechanisms required by this Regulation are treated with priority, without prejudice to the requirement to process and decide upon all notices submitted under those mechanisms in a timely, diligent and objective manner. **Such trusted flagger status should be awarded by the Digital Services Coordinator of the Member State in which the applicant is established establishment and should be recognised by all providers of online platforms within the scope of this Regulation.** Such trusted flagger status should only be awarded to entities, and not individuals, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content, that they represent collective interests and that they work in a diligent and objective manner. **Industry associations representing their members' interests should apply for the status of trusted flaggers, so as to limit the number of trusted flaggers awarded by the Digital Services Coordinator, without prejudice to the right of private parties to enter into bilateral agreements with online platforms.** Such entities can be public in nature, such as, for terrorist content, internet~~

[10] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (OJ L 165, 18.6.2013, p. 63).

~~referral units of national law enforcement authorities or of the European Union Agency for Law Enforcement Cooperation ('Europol') or they can be non-governmental organisations and **private or** semi-public bodies, such as the organisations part of the INHOPE network of hotlines for reporting child sexual abuse material and organisations committed to notifying illegal racist and xenophobic expressions online. For intellectual property rights, organisations of industry and of right-holders could be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions. The rules of this Regulation on trusted flaggers should not be understood to prevent **providers of** online platforms from giving similar treatment to notices submitted by entities or individuals that have not been awarded trusted flagger status under this Regulation, from otherwise cooperating with other entities, in accordance with the applicable law, including this Regulation and Regulation (EU) 2016/794 of the European Parliament and of the Council.[11]~~

(47) The misuse of ~~services of~~ online platforms by frequently providing manifestly illegal content or by frequently submitting manifestly unfounded notices or complaints under the mechanisms and systems, respectively, established under this Regulation undermines trust and harms the rights and legitimate interests of the parties concerned. Therefore, there is a need to put in place appropriate and proportionate safeguards against such misuse. Information should be considered to be manifestly illegal content and notices or complaints should be considered manifestly unfounded where it is evident to a layperson, without any substantive analysis, that the content is illegal respectively that the notices or complaints are unfounded. Under certain conditions, **providers of** online platforms should temporarily suspend their relevant activities in respect of the person engaged in abusive behaviour. This is without prejudice to the freedom by **providers of** online platforms to determine their terms and conditions and establish stricter measures in the case of manifestly illegal content related to serious crimes**, such as child sexual abuse material**. For reasons of transparency, this possibility should be set out, clearly and in sufficiently detail, in the terms and conditions of the online platforms. Redress should always be open to the decisions taken in this regard by **providers of** online platforms and they should be subject to oversight by the competent Digital Services Coordinator. **Providers of online platforms should send a prior warning before deciding on the suspension, which should include the reasons for**

---

11 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53.

the possible suspension and the means of redress against the decision of the providers of the online platform. The rules of this Regulation on misuse should not prevent **providers of** online platforms from taking other measures to address the provision of illegal content by recipients of their service or other misuse of their services, in accordance with the applicable Union and national law. Those rules are without prejudice to any possibility to hold the persons engaged in misuse liable, including for damages, provided for in Union or national law.

~~(48) An online platform may in some instances become aware, such as through a notice by a notifying party or through its own voluntary measures, of information relating to certain activity of a recipient of the service, such as the provision of certain types of illegal content, that reasonably justify, having regard to all relevant circumstances of which the online platform is aware, the suspicion that the recipient may have committed, may be committing or is likely to commit a serious criminal offence involving a threat to the life or safety of person, such as offences specified in Directive 2011/93/EU of the European Parliament and of the Council[12]. In such instances, the online platform should inform without delay the competent law enforcement authorities of such suspicion, providing all relevant information available to it, including where relevant the content in question and an explanation of its suspicion. This Regulation does not provide the legal basis for profiling of recipients of the services with a view to the possible identification of criminal offences by online platforms. Online platforms should also respect other applicable rules of Union or national law for the protection of the rights and freedoms of individuals when informing law enforcement authorities.~~ ***[moved to Recital 42a]***

~~[12] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).~~

(49) In order to contribute to a safe, trustworthy and transparent online environment for consumers, as well as for other interested parties such as competing traders and holders of intellectual property rights, and to deter traders from selling products or services in violation of the applicable rules, online ~~platforms allowing consumers to conclude distance contracts with traders~~**marketplaces** should ensure that such traders are traceable. The trader should therefore be required to provide certain essential information to the **provider of** online ~~platform~~**marketplace**, including for purposes of promoting messages on or offering products. That requirement should also be applicable to traders that promote messages on products or services on behalf of brands, based on underlying agreements. Th~~os~~e online ~~platforms~~ **marketplaces** should store all information in a secure manner for **the duration of their contractual relationship with the trader and 6 months thereafter. This is necessary**~~a reasonable period of time that does not exceed what is necessary~~, so that ~~it~~ **the information** can be accessed, in accordance with the applicable law, including on the protection of personal data, by public authorities and private parties with a legitimate interest, including through the orders to provide information referred to in this Regulation. **Without prejudice to the definition provided for in this Regulation, any trader, irrespective of whether it is a natural or legal person, identified on the basis of Article 6a, paragraph(1)(b) of Directive 2011/83/EU and Article 7 paragraph (4)(f) of Directive 2005/29/EC should be traceable when offering a product or service through an online platform. Similarly, the traceability of holders of domain names for the purpose of contributing to the security, stability and resilience of domain name systems, which in turn contributes to a high common level of cybersecurity within the Union, is ensured by Directive …/… [proposed Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148], which introduces the obligation for top-level domain registries and the entities providing domain name registration services for the top-level domain, so-called registrars, to collect, maintain in a database and provide lawful access to accurate and complete domain name registration data. Directive 2000/31/EC obliges all information society services providers to render easily, directly and permanently accessible to the recipients of the service and competent authorities certain information allowing the identification of all providers.**

(50) To ensure an efficient and adequate application of that obligation, without imposing any disproportionate burdens, the **providers of the** online ~~platforms covered~~ **marketplaces** should make reasonable efforts to verify the reliability of the information provided by the traders concerned, in particular by using freely available official online databases and online interfaces, such as national trade registers and the VAT Information Exchange System[13], or by requesting the traders concerned to provide trustworthy supporting documents, such as copies of identity documents, certified ~~bank~~ **payment accounts'** statements, company certificates and trade register certificates. They may also use other sources, available for use at a distance, which offer a similar degree of reliability for the purpose of complying with this obligation. However, the **providers of** online ~~platforms covered~~ **marketplaces** should not be required to engage in excessive or costly online fact-finding exercises or to carry out verifications on the spot. Nor should such **providers** ~~online platforms~~, which have made the reasonable efforts required by this Regulation, be understood as guaranteeing the reliability of the information towards consumer or other interested parties. **Providers of** ~~Such~~ online ~~platforms~~ **marketplaces** should also design and organise their online interface in a way that enables traders to comply with their obligations under Union law, in particular the requirements set out in Articles 6 and 8 of Directive 2011/83/EU of the European Parliament and of the Council[14], Article 7 of Directive 2005/29/EC of the European Parliament and of the Council[15] and Article 3 of Directive 98/6/EC of the European Parliament and of the Council[16].[17]. **In order to ensure that the intended effect can be achieved, providers of online marketplaces shall make their best efforts to make sure that the traders provide complete information and ensure that products or services are not offered as long as the information is incomplete. This is not a general monitoring obligation or an**

---

13 https://ec.europa.eu/taxation_customs/vies/vieshome.do?selectedLanguage=en

14 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

15 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').

16 Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers.

17 Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers.

obligation for the provider of online marketplaces to assess whether the content provided is in fact compliant with Union law. The obligation could be seen as a more technical obligation where the provider by design of the online interface ensure that a certain product cannot be uploaded and offered to consumers on their marketplace before certain sections has been completed by the trader. How the provider of an online marketplace will ensure this, is up to the provider to decide. Providers of online marketplaces should store the information received by traders for six months. This obligation leaves unaffected potential obligations to preserve certain content for longer periods of time, on the basis of other Union law or national laws, in compliance with Union law.

The amendment in this Recital is a consequential amendment due to our suggestions to Article 24b, which we refer to.

(51) In view of the particular responsibilities and obligations of **providers of** online platforms, they should be made subject to transparency reporting obligations, which apply in addition to the transparency reporting obligations applicable to all providers of intermediary services under this Regulation. For the purposes of determining whether online platforms may be very large online platforms that are subject to certain additional obligations under this Regulation, the transparency reporting obligations for **providers of** online platforms should include certain obligations relating to the publication and communication of information on the average monthly active recipients of the service in the Union.

(52) Online advertis**ing**~~ement~~ plays an important role in the online environment, including in relation to the provision of ~~the services of~~ online platforms**, when the ~~service provider~~ provider of online platform receives remuneration as economic consideration for the placement of the specific advertisement on the platform's online interface, for example as direct payment or increased sale commission**. However, online advertis**ing** ~~ement~~ can contribute to significant risks, ranging from advertisement**s** that ~~is itself~~**are themselves** illegal content, to contributing to financial incentives for the publication or amplification of illegal or otherwise harmful content and activities online, or the discriminatory **presentation**~~display~~ of advertising with an impact on the equal treatment and opportunities of citizens. In addition to the requirements resulting from Article 6 of Directive 2000/31/EC, **providers of** online platforms should therefore be required to ensure that the recipients of the service have certain individualised information necessary for them to understand when and on whose behalf the advertisement is ~~displayed~~**presented**. **They should ensure that the**

information is salient, including through standardised visual or audio marks, clearly identifiable and unambiguous for the average user, and should be adapted to the nature of the individual service's online interface. In addition, recipients of the service should have information on the main parameters used for determining that specific advertis**ment**~~ing~~ is ~~to be displayed~~ **presented** to them, providing meaningful explanations of the logic used to that end, including when this is based on profiling. **Such explanations should include information on the method used for ~~displaying~~ presenting the advertisement – for example whether it is contextual, behavioural or other type of advertising – and, where applicable, the main profiling criteria used.** The requirements of this Regulation on the provision of information relating to advertisement is without prejudice to the application of the relevant provisions of Regulation (EU) 2016/679, in particular those regarding the right to object, automated individual decision-making, including profiling and specifically the need to obtain consent of the data subject prior to the processing of personal data for targeted advertising. Similarly, it is without prejudice to the provisions laid down in Directive 2002/58/EC in particular those regarding the storage of information in terminal equipment and the access to information stored therein. **Finally, this Regulation complements the application of the Directive 2010/13/EU which imposes measures to enable users to declare audiovisual commercial communications in user-generated videos.**

Chapter III

Due diligence obligations for a transparent and safe online environment

SECTION 1

PROVISIONS APPLICABLE TO ALL PROVIDERS OF INTERMEDIARY SERVICES

Article 10

***Electronic p**~~P~~oints~~s~~ of contact*

1. Providers of intermediary services shall ~~establish~~**designate** a single point of contact allowing for direct communication, by electronic means, with Member States' authorities, the Commission and the Board referred to in Article 47 for the application of this Regulation.

2. Providers of intermediary services shall make public the information necessary to easily identify and communicate with their single **electronic** point~~s~~ of contact. **This information shall be easily accessible.**

3. Providers of intermediary services shall specify in the information referred to in paragraph 2, the official language or languages of the Union **which**, **in addition to a language broadly understood by the largest possible number of Union citizens,** ~~which~~ can be used to communicate with their **electronic** point~~s~~ of contact**,** and which shall include at least one of the official languages of the Member State in which the provider of intermediary services has its main establishment or where its legal representative resides or is established.

Article 11

Legal representatives

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

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

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

4. Providers of intermediary services shall notify the name, address, the electronic mail address and telephone number of their legal representative to the Digital Service Coordinator in the Member State where that legal representative resides or is established. They shall ensure that that information is **accurate and** up to date. **Providers of intermediary services shall ensure that their legal representative meet at least the following conditions;**

   a. **Is registered in a trade register or similar public register with registration number or equivalent means of identification in that register, where possible in the Member State established;**

   b. **has sufficient resources;**

   c. **is not subject to reconstruction proceedings, bankruptcy, personal or corporate insolvency.**

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

We are worried that the requirements in article 11(4) could be circumvented by the use of "shell-companies". In order to prevent this it seems necessary to consider the set up of certain requirements regarding *who* can be notified as legal representative. Especially if the legal responsibility should have any effect in reality.

Article 12

Terms and conditions

1. Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review. It shall be set out in clear**, plain, intelligible** and unambiguous language and shall be publicly available in an easily accessible **and machine-readable** format.

1a. Where an intermediary service is primarily aimed at minors or is pre-dominantly used by them, the provider shall explain conditions and restrictions for the use of the service in a way that minors can understand, including conditions and restrictions imposed to comply with its obligations under this Regulation, where applicable.

2. Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the ~~applicable~~ fundamental rights of the recipients of the service as enshrined in the Charter.

Article 13

Transparency reporting obligations for providers of intermediary services

1. Providers of intermediary services shall ~~publish~~ **make publicly available in a specific section in their online interface**, at least once a year, clear **and**~~,~~ easily comprehensible ~~and detailed~~ reports on any content moderation they engaged in during the relevant period. Those reports shall include, in particular, information on the following, as applicable:

   (a) **for providers of intermediary services,** the number of orders received from Member States' authorities, **including orders issued in accordance with Articles 8 and 9,** categorised by the type of illegal content concerned, ~~including orders issued in accordance with Articles 8 and 9,~~ and the **median** ~~average~~ time needed for taking the action specified in those orders;

   (b) **for providers of hosting services,** the number of notices submitted in accordance with Article 14, categorised by the type of alleged illegal content concerned, any action taken pursuant to the notices by differentiating whether the action was taken on the basis of the law or the terms and conditions of the provider, **the number of notices submitted by trusted flaggers, the number of notices processed exclusively by automated means** and the **median**~~average~~ time needed for taking the action;

(c) **for providers of intermediary services, as applicable,** the content moderation engaged in at the providers' own initiative, including the number ~~and type~~ of **removals or other restrictions of the availability,** ~~measures taken that affect~~**to restrict** ~~the availability~~, visibility and accessibility of information provided by the recipients of the service and the recipients' ability to provide information **through the service, and other related restrictions of the service. The information reported shall be**~~,~~ categorised **by the type of illegal content or violation of the terms and conditions of the service provider, by the detection method and by the type of restriction applied** ~~**method of detection of the infringement, the type of measure taken, and the type of alleged illegal content or infringement of the terms and conditions of the service provider**~~by the type of reason and basis for taking those measures~~;

(d) **for providers of intermediary services, as applicable,** the number of complaints received through the internal complaint-handling system**s in accordance with the provider's terms and conditions and, for providers of online platforms, also in accordance with** ~~referred to in~~ Article 17, the basis for those complaints, decisions taken in respect of those complaints, the **median** ~~average~~ time needed for taking those decisions and the number of instances where those decisions were reversed.

2. Paragraph 1 shall not apply to providers of intermediary services that qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC **and which are not very large online platforms in accordance with Article 25**.

3. The Commission may adopt implementing acts to lay down templates concerning the form, content and other details of reports pursuant to paragraph 1. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 70.

Overall, we can support the provision. However, we find that the number of implementing acts should be limited and such acts should only deal with technical issues.

SECTION 2

ADDITIONAL PROVISIONS APPLICABLE TO PROVIDERS OF HOSTING SERVICES, INCLUDING ONLINE PLATFORMS

Article 14

Notice and action mechanisms

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

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

   (a) a~~n~~ **sufficiently substantiated** explanation of the reasons why the individual or entity considers the information in question to be illegal content;

   (b) a clear indication of the electronic location of that information, ~~in particular~~**such as** the exact URL or URLs, and, where necessary, additional information enabling the identification of the illegal content;

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

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

3. Notices ~~that include the elements~~ referred to in paragraph 2 **on the basis of which a diligent provider of hosting services can identify the illegality of the content in question** shall be considered to give rise to actual knowledge or awareness for the purposes of Article 5 in respect of the specific item of information concerned.

4. Where the notice contains ~~the name and~~ an electronic **contact information** ~~mail address~~ of the individual or entity that submitted it, the provider of hosting services shall**,** ~~promptly~~ **without undue delay,** send a confirmation of receipt of the notice to that individual or entity.

5. The provider shall also, without undue delay, notify that individual or entity of its decision in respect of the information to which the notice relates, providing information on the redress possibilities in respect of that decision.

6. Providers of hosting services shall process any notices that they receive under the mechanisms referred to in paragraph 1, and take their decisions in respect of the information to which the notices relate, in a timely, diligent and objective manner. Where they use automated means for that processing or decision-making, they shall include information on such use in the notification referred to in paragraph **5**~~4~~.

We can support the amendments as we find they provide clarity and impose responsibility on platforms that should improve the take-down of illegal content. Especially the modification regarding referral to the exact URL, as it is not always possible to provide such information.

Regarding recital 41 we support that this recital now reflects that providers of hosting services should act upon notices in a timely manner, in particular, by taking into account the type of illegal content being notified and the urgency of taking action. However, we still find, that we could be even more ambitious. The DSA should entail a clearly defined timeline for acting on notifications of illegal content including a differentiated time limit so that illegal content with a serious detrimental effect, such as terrorism-related content and illegal products, is taken down more quickly than other illegal content.

Furthermore, the largest platforms should be expected to ensure that content that once has been identified as illegal and removed, is quickly detected and removed again if a user uploads it again through a so-called stay-down obligation. This of course without imposing a general monitoring obligation.

According to this, we have submitted amendments to art. 5 and a suggestion for a new art. 24e.

Article 15

Statement of reasons

1. Providers of hosting services shall provide a clear and specific statement of reasons to any affected recipients of the service for any of the following restrictions imposed:

a) any restrictions of the visibility of specific items of information provided by the recipient of the service, including removal of content, or disabling access to content;

b) suspension, termination or other restriction of monetary payments (monetisation);

c) suspension or termination of the provision of the service in whole or in part;

d) suspension or termination of the recipient's accounts.

This paragraph shall only apply where the relevant electronic contact details are known to the provider. It shall apply at the latest when the restriction is imposed, and regardless of why or how it was imposed.

~~1. Where a provider of hosting services decides to remove or disable access to **or otherwise restrict the visibility of** specific items of information provided by the recipients of the service, **or to suspend or terminate monetary payments related to those items,** irrespective of the means used for detecting, identifying or removing or disabling access to **or for restricting the visibility or monetisation of** that information and of the reason for its decision, it shall inform the recipient **where the electronic contact details are known to the provider**, **prior to or**at the latest at the time of the removal or disabling of access **or the restriction of visibility or monetisation taking effect**, of the decision and provide**with** a clear and specific statement of reasons for that decision.~~

2. The statement of reasons referred to in paragraph 1 shall at least contain the following information:

(a) whether the decision entails either the removal of, ~~or~~ the disabling of access to**, the restriction of the visibility of**~~,~~ the information **or the suspension or termination of monetary payments related to that information**~~and, where relevant, the territorial scope of the disabling of access~~;

(b) the facts and circumstances relied on in taking the decision, including where relevant whether the decision was taken pursuant to a notice submitted in accordance with Article 14;

(c) where applicable, information on the use made of automated means in taking the decision, including where the decision was taken in respect of content detected or identified using automated means;

(d) where the decision concerns allegedly illegal content, a reference to the legal ground relied on and explanations as to why the information is considered to be illegal content on that ground;

(e) where the decision is based on the alleged incompatibility of the information with the terms and conditions of the provider, a reference to the contractual ground relied on and explanations as to why the information is considered to be incompatible with that ground;

(f) information on the redress possibilities available to the recipient of the service in respect of the decision, in particular through internal complaint-handling mechanisms, out-of-court dispute settlement and judicial redress**.**

3. The information provided by the providers of hosting services in accordance with this Article shall be clear and easily comprehensible and as precise and specific as reasonably possible under the given circumstances. The information shall, in particular, be such as to reasonably allow the recipient of the service concerned to effectively exercise the redress possibilities referred to in point (f) of paragraph 2.

4. Providers of hosting services shall publish the decisions and the statements of reasons, referred to in paragraph 1 in a publicly accessible database managed by the Commission. That information shall not contain personal data.

*Article **15a**~~21~~*

Notification of suspicions of criminal offences

1. Where a~~n~~ **provider of hosting services** ~~online platform~~ becomes aware of any information giving rise to a suspicion that a ~~serious~~ criminal offence involving a threat to the life or safety of **a person or** persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide all relevant information available.

2. Where the **provider of hosting services**~~online platform~~ cannot identify with reasonable certainty the Member State concerned, it shall inform the law enforcement authorities of the Member State in which it is established or has its legal representative or inform Europol.

   For the purpose of this Article, the Member State concerned shall be the Member State where the offence is suspected to have taken place, be taking place and likely to take place, or the Member State where the suspected offender resides or is located, or the Member State where the victim of the suspected offence resides or is located.

We are very pleased to see that the scope of the provision is now extended to hosting services and that micro and small enterprises are not exempted. Considering the seriousness of the offenses covered by the provision the requirements does not seem unproportionate but more as a part of general social responsibility.

*Article **15b**~~19~~*

Trusted flaggers

1. **Providers of hosting services** ~~Online platforms~~ shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers through the mechanisms referred to in Article 14, are processed and decided upon with priority and without delay.

2. The status of trusted flaggers under this Regulation shall be awarded, upon application by any entities, by the Digital Services Coordinator of the Member State in which the applicant is established, where the applicant has demonstrated to meet all of the following conditions:

(a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content;

(b) ~~it represents collective interests and~~ **it** is independent from any **provider of** online platform**s**;

(c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner.

3. Digital Services Coordinators shall communicate to the Commission and the Board the names, addresses and electronic mail addresses of the entities to which they have awarded the status of the trusted flagger in accordance with paragraph 2 **or revoked it in accordance with paragraph 6**.

4. The Commission shall publish the information referred to in paragraph 3 in a publicly available **and easily accessible** database and keep the database updated.

5. Where **a provider of a hosting service** ~~an online platforms~~ has information indicating that a trusted flagger submitted a significant number of insufficiently precise or inadequately substantiated notices through the mechanisms referred to in Article 14, including information gathered in connection to the processing of complaints through the internal complaint-handling systems referred to in Article 17(3), it shall communicate that information to the Digital Services Coordinator that awarded the status of trusted flagger to the entity concerned, providing the necessary explanations and supporting documents.

6. The Digital Services Coordinator that awarded the status of trusted flagger to an entity shall revoke that status if it determines, following an investigation either on its own initiative or on the basis information received by third parties, including the information provided by **a provider of a hosting service** ~~an online platforms~~ pursuant to paragraph 5, that the entity no longer meets the conditions set out in paragraph 2. Before revoking that status, the Digital Services Coordinator shall afford the entity an opportunity to react to the findings of its investigation and its intention to revoke the entity's status as trusted flagger**.**

7. The Commission, after consulting the Board, may issue guidance to assist **providers of** online platforms and Digital Services Coordinators in the application of paragraphs **2,** 5 and 6.

We find that the scope of the provision should be extended to hosting services and that micro and small enterprises should not be exempted. The reason for this being that we wish to remove as much illegal content as possible and that the obligations in the provision does not seem as an unreasonable requirement or too burdensome – even for a small service, since they already establish notice and action mechanisms.

SECTION 3

ADDITIONAL PROVISIONS APPLICABLE TO PROVIDERS OF ONLINE PLATFORMS

Article 16

Exclusion for micro and small enterprises

This Section **and Section 3a** shall not apply to **providers of** online platforms that qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC **and except when they are~~which are not~~ very large online platforms in accordance with Article 25.**

According to the Annex to Recommendation 2003/361/EC, a small enterprise is defined as an enterprise which employs less than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million. A microenterprise is defined as an enterprise which employs less than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

Overall, we support the Commission's recommendation, but in this case, it would be suitable to deviate from the Recommendation. Intermediary Services which has less than 50 or 10 persons with an annual turnover and/or annual balance sheet total that does not exceed EUR 10 or 2 million can still have a great amount of users, and should therefore not be excluded from due diligence obligations. Therefore, we are positive towards the amendment to this provision. However, we're still concerned that the threshold for VLOP's is too high in this connection. We would suggest an approach similar to the one of the Copyright Directive.

Article 17

Internal complaint-handling system

1. **Providers of o~~O~~**nline platforms shall provide recipients of the service **and individuals or entities that have submitted a notice**, for a period of at least six months following the

decision referred to in this paragraph, the access to an effective internal complaint-handling system, which enables the complaints to be lodged electronically and free of charge, against the **decision taken by the provider of the online platform not to act upon the receipt of a notice or against the** following decisions taken by the **provider of the** online platform on the ground that the information provided by the recipients is illegal content or incompatible with its terms and conditions:

(a) decisions **whether or not** to remove or disable access to **or restrict visibility of** the information;

(b) decisions **whether or not** to suspend or terminate the provision of the service, in whole or in part, to the recipients;

(c) decisions **whether or not** to suspend or terminate the recipients' account**;**

(d) decision whether or not to suspend, terminate or otherwise restrict monetary payments related to ~~restrict the ability to monetize~~ content provided by the recipients.

2. **Providers of o~~O~~**nline platforms shall ensure that their internal complaint-handling systems are easy to access, user-friendly and enable and facilitate the submission of sufficiently precise and adequately substantiated complaints.

3. **Providers of ~~O~~**nline platforms shall handle complaints submitted through their internal complaint-handling system in a timely, diligent and objective manner. Where a complaint contains sufficient grounds for the **provider of the** online platform to consider that **its decision not to act upon the request of a notice is unfounded or that** the information to which the complaint relates is not illegal and is not incompatible with its terms and conditions, or contains information indicating that the complainant's conduct does not warrant the suspension or termination of the service or the account **or the restriction to monetary payments related to content**, it shall reverse its decision referred to in paragraph 1 without undue delay.

4. **Providers of o~~O~~**nline platforms shall inform ~~complainants~~ without undue delay of the decision they have taken in respect of the information to which the complaint relates**, clearly justify their decision** and ~~shall~~ inform ~~complainants~~ of the possibility of out-of-court dispute settlement provided for in Article 18 and other available redress possibilities.

5. **Providers of o**~~O~~nline platforms shall ensure that the decisions, referred to in paragraph 4, are not solely taken on the basis of automated means.

We can support the provision and are especially pleased to see the scope includes decisions not to act upon a notice.

Article 18

Out-of-court dispute settlement

1. Recipients of the service **and individuals or entities that have submitted notices,** addressed by the decisions referred to in Article 17(1), shall be entitled to select any out-of-court dispute **settlement body**

   a. **in the Union Member State where the recipient of the service is established or located;**

   b. in the Union Member State where the provider of intermediary service is established; or

   c. in the Union Member State where the provider of intermediary service which do not have an establishment in the Union but offer services in the Union, have designated a legal representative.

   The out-of-court dispute settlement body that has been ~~certified~~ **authorised** in accordance with paragraph 2 in order to resolve disputes relating to those decisions, including complaints that could not be resolved by means of the internal complaint-handling system referred to in that Article. **Providers of o**~~O~~nline platforms shall engage, in good faith, with the body selected with a view to resolving the dispute and shall be bound by the decision taken by the body.

   The first subparagraph is without prejudice to the right of the recipient **or the individual or entity** concerned**, or the provider of online platforms** to redress against the decision before a court in accordance with the applicable law.

   Online platform may refuse to engage in dispute settlement when the same dispute regarding the same content has already been resolved or is being reviewed by another dispute settlement body.

2. The Digital Services Coordinator of the Member State where the out-of-court dispute settlement body is established **can** ~~shall~~, at the request of that body, ~~certify~~ **authorise** the body, where the body has demonstrated that it meets all of the following conditions:

(a) it is ~~impartial and~~ independent of **providers of** online platforms**, of** ~~and~~ recipients of the service provided by the online platforms **and of individuals or entities that have submitted notices**;

(b) it has the necessary expertise in relation to the issues arising in one or more particular areas of illegal content, or in relation to the application and enforcement of terms and conditions of one or more types of online platforms, allowing the body to contribute effectively to the settlement of a dispute;

(c) the dispute settlement is easily accessible through electronic communication technology;

(d) it is capable of settling dispute in a swift, efficient and cost-effective manner and in at least one official language of the Union;

(e) the dispute settlement takes place in accordance with clear and fair rules of procedure**, in compliance with applicable legislation**.

The Digital Services Coordinator shall, where applicable, specify in the ~~certificate~~ **authorisation** the particular issues to which the body's expertise relates and the official language or languages of the Union in which the body is capable of settling disputes, as referred to in points (b) and (d) of the first subparagraph, respectively.

2a. Where an out-of-court dispute settlement body is authorised by the competent Digital Services Coordinator pursuant to paragraph 2, that authorisation shall be valid in all Member States.

3. If the body decides the dispute in favour of the recipient of the service **or of the individual or entity that have submitted a notice**, the **provider of the** online platform shall reimburse the recipient **or the individual or entity** for any fees and other reasonable expenses that the ~~recipient has~~**they have** paid ~~or are~~**is to pay** in relation to the dispute settlement **or waive any such fees or reasonable expenses that may otherwise be due**. If the body decides the dispute in favour of the online platform, the recipient **or the individual or** ~~body~~ **entity,** shall not be required to reimburse any fees or other expenses that the **provider of the** online platform paid or is to pay in relation to the dispute settlement **unless the recipient or the individual or entity acted in manifestly bad faith.**

The fees charged by the body for the dispute settlement shall be reasonable**, accessible, attractive and inexpensive for consumers** and shall in any event not exceed **a nominal fee or** the costs thereof.

~~Certified~~ **Authorised** out-of-court dispute settlement bodies shall make the fees, or the mechanisms used to determine the fees, known to the recipient of the services **or to the individuals or entities that have submitted a notice** and the **provider of the** online platform concerned before engaging in the dispute settlement.

4. Member States may establish out-of-court dispute settlement bodies for the purposes of paragraph 1 or support the activities of some or all out-of-court dispute settlement bodies that ~~they~~ have **been** ~~certified~~ **authorised** in accordance with paragraph 2.

Member States shall ensure that any of their activities undertaken under the first subparagraph do not affect the ability of their Digital Services Coordinators to ~~certify~~ **authorise** the bodies concerned in accordance with paragraph 2.

4a. The Digital Services Coordinator that awarded the status of out-of-court dispute settlement body to an entity shall revoke that status if it determines, following an investigation either on its own initiative or on the basis of the information received by third parties, that the body no longer meets the conditions set out in paragraph 2. Before revoking that status, the Digital Services Coordinator shall afford the body an opportunity to react to the findings of its investigation and its intention to revoke the body's authorisation.

5. Digital Services Coordinators shall notify to the Commission the out-of-court dispute settlement bodies that they have ~~certified~~ **authorised** in accordance with paragraph 2, including where applicable the specifications referred to in the second subparagraph of that

paragraph**, as well as the out-of-court dispute settlement bodies whose authorisation they have revoked**. The Commission shall publish a list of those bodies, including those specifications, on a dedicated website **that is easily accessible**, and keep it updated.

6. This Article is without prejudice to Directive 2013/11/EU and alternative dispute resolution procedures and entities for consumers established under that Directive.

From the wording of the provision, it appears that the recipient is entitled to select any out-of-court dispute settlement body. As we understand from the discussions during the working parties this would imply, that the user can choose a body in any Member State – regardless of where the user lives or where the platform is established. From the outset, we find this problematic and we have some drafting suggestions to the provision.

It appears from the provision, that the online platform shall be bound by the decisions taken by the body. From our side it is very important that the possibility to seek juridical redress in accordance with the laws of the Member State concerned is not affected. It is our understanding that this has been taken into account in art. 18(1) last paragraph.

As we read article 18(2) the Digital Services Coordinator is obligated to authorize a body, if the body demonstrates, that it meets the five requirements listed in the paragraph. From our side we find it important that it is the Member State/Digital Services Coordinator who decides, whether a body that meets the requirements should be designated according to this article. Thus, it should be pointed out that:

- **A body can only be authorized if it meets the requirements of the article, and**
- **The Digital Services Coordinator decides whether the out-of-court dispute settlement body that meets the requirements shall be authorized.**

The requirement, that the body is impartial and independent should be elaborated for instance with inspiration from article 6 in Directive 2013/11/EU on alternative dispute resolution.

The provision does not provide sufficient guidance regarding what clear and fair rules of procedure are. This should also be elaborated appropriately, i.e. with inspiration from Directive 2013/11/EU on alternative dispute resolution.

Regarding the fees for the dispute settlement (article 18(3)), we find it of utmost importance that these fees are kept at a low level in order to secure access to out-of-court dispute settlement for all users. Thus, we are satisfied that this has now been set out in the article and in the recitals that these fees should be reasonable, proportionate, accessible, attractive and inexpensive. However, we do still worry that the provision will allow the dispute settlement bodies to charge high fees which in fact will make the access to out-of-court dispute settlement illusory. Thus, we suggest that it – in line with directive 2013/11/EU – is stressed in the recitals that out-of-court procedures should preferably be free of charge. In the event that costs are applied, costs should not exceed a nominal fee.

~~Article 19~~

~~Trusted flaggers~~

~~[Moved to new art. 15b]~~

~~1. **Providers of o**Online platforms shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers through the mechanisms referred to in Article 14, are processed and decided upon with priority and without delay.~~

~~2. The status of trusted flaggers under this Regulation shall be awarded, upon application by any entities, by the Digital Services Coordinator of the Member State in which the applicant is established, where the applicant has demonstrated to meet all of the following conditions:~~

~~(a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content;~~

~~(b) it represents collective interests and **it** is independent from any **provider of** online platforms**s**;~~

~~(c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner.~~

~~3. Digital Services Coordinators shall communicate to the Commission and the Board the names, addresses and electronic mail addresses of the entities to which they have awarded the status of the trusted flagger in accordance with paragraph 2 **or revoked it in accordance with paragraph 6**.~~

~~4. The Commission shall publish the information referred to in paragraph 3 in a publicly available **and easily accessible** database and keep the database updated.~~

~~5. Where **a provider of** an online platforms has information indicating that a trusted flagger submitted a significant number of insufficiently precise or inadequately substantiated notices through the mechanisms referred to in Article 14, including information gathered in connection to the processing of complaints through the internal complaint-handling systems referred to in Article 17(3), it shall communicate that information to the Digital Services Coordinator that awarded the status of trusted flagger to the entity concerned, providing the necessary explanations and supporting documents.~~

~~6. The Digital Services Coordinator that awarded the status of trusted flagger to an entity shall revoke that status if it determines, following an investigation either on its own initiative or on the basis information received by third parties, including the information provided by **a provider of** an online platforms pursuant to paragraph 5, that the entity no longer meets the conditions set out in paragraph 2. Before revoking that status, the Digital Services Coordinator shall afford the entity an opportunity to react to the findings of its investigation and its intention to revoke the entity's status as trusted flagger.~~

~~7. The Commission, after consulting the Board, may issue guidance to assist **providers of** online platforms and Digital Services Coordinators in the application of paragraphs **2,** 5 and 6.~~

Article 20

Measures and protection against misuse

1. **Providers of o**~~O~~nline platforms shall suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly illegal content.

2. **Providers of** ~~O~~nline platforms ~~shall~~**may** suspend, for a reasonable period of time and after having issued a prior warning, the processing of notices and complaints submitted through the notice and action mechanisms and internal complaints-handling systems referred to in Articles 14 and 17, respectively, by individuals or entities or by complainants that frequently submit notices or complaints that are manifestly unfounded.

3. **When deciding on the suspension, providers of o**~~O~~nline platforms shall assess, on a case-by-case basis and in a timely, diligent and objective manner, whether a recipient, individual, entity or complainant engages in the misuse referred to in paragraphs 1 and 2, taking into account all relevant facts and circumstances apparent from the information available to the **provider of the** online platform. Those circumstances shall include at least the following:

   (a) the absolute numbers of items of manifestly illegal content or manifestly unfounded notices or complaints, submitted in **a given time frame**~~the past year~~;

   (b) the relative proportion thereof in relation to the total number of items of information provided or notices submitted in ~~the~~ ~~past year~~**a given time frame**;

   (c) the gravity of the misuses**, including the nature of illegal content,** and **of** its consequences;

   (d) **where it is possible to infer it,** the intention of the recipient, individual, entity or complainant.

4. **Providers of o**~~O~~nline platforms shall set out, in a clear and detailed manner, their policy in respect of the misuse referred to in paragraphs 1 and 2 in their terms and conditions, including as regards the facts and circumstances that they take into account when assessing whether certain behaviour constitutes misuse and the duration of the suspension.

~~Article 21~~

~~Notification of suspicions of criminal offences~~

~~1. Where an online platform becomes aware of any information giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide all relevant information available.~~

~~2. Where the online platform cannot identify with reasonable certainty the Member State concerned, it shall inform the law enforcement authorities of the Member State in which it is established or has its legal representative or inform Europol.~~

~~For the purpose of this Article, the Member State concerned shall be the Member State where the offence is suspected to have taken place, be taking place and likely to take place, or the Member State where the suspected offender resides or is located, or the Member State where the victim of the suspected offence resides or is located.~~

[Article 22 moved to Article 24a, into new Section 3a]

~~*Article 22*~~

~~*Traceability of traders*~~

~~1. Where an online platform allows consumers to conclude distance contracts with traders, it shall ensure that traders can only use its services to promote messages on or to offer products or services to consumers located in the Union if, prior to the use of its services, the online platform has obtained the following information:~~

~~(a) the name, address, telephone number and electronic mail address of the trader;~~

~~(b) a copy of the identification document of the trader or any other electronic identification as defined by Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council[18];~~

~~(c) the bank account details of the trader, where the trader is a natural person;~~

~~(d) the name, address, telephone number and electronic mail address of the economic operator, within the meaning of Article 3(13) and Article 4 of Regulation (EU) 2019/1020 of the European Parliament and the Council[19] or any relevant act of Union law;~~

~~[18] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC~~

~~[19] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).~~

(e) where the trader is registered in a trade register or similar public register, the trade register in which the trader is registered and its registration number or equivalent means of identification in that register;

(f) a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law.

2. The online platform shall, upon receiving that information, make reasonable efforts to assess whether the information referred to in points (a), (d) and (e) of paragraph 1 is reliable through the use of any freely accessible official online database or online interface made available by a Member States or the Union or through requests to the trader to provide supporting documents from reliable sources.

3. Where the online platform obtains indications that any item of information referred to in paragraph 1 obtained from the trader concerned is inaccurate or incomplete, that platform shall request the trader to correct the information in so far as necessary to ensure that all information is accurate and complete, without delay or within the time period set by Union and national law.

Where the trader fails to correct or complete that information, the online platform shall suspend the provision of its service to the trader until the request is complied with.

4. The online platform shall store the information obtained pursuant to paragraph 1 and 2 in a secure manner for the duration of their contractual relationship with the trader concerned. They shall subsequently delete the information.

5. Without prejudice to paragraph 2, the platform shall only disclose the information to third parties where so required in accordance with the applicable law, including the orders referred to in Article 9 and any orders issued by Member States' competent authorities or the Commission for the performance of their tasks under this Regulation.

~~6. The online platform shall make the information referred to in points (a), (d), (e) and (f) of paragraph 1 available to the recipients of the service, in a clear, easily accessible and comprehensible manner.~~

~~7. The online platform shall design and organise its online interface in a way that enables traders to comply with their obligations regarding pre-contractual information and product safety information under applicable Union law.~~

Article 23

Transparency reporting obligations for providers of online platforms

1. In addition to the information referred to in Article 13, **providers of** online platforms shall include in the reports referred to in that Article information on the following:

   (a) the number of disputes submitted to the out-of-court dispute settlement bodies referred to in Article 18, the outcomes of the dispute settlement and the **median** ~~average~~ time needed for completing the dispute settlement procedures;

   (b) the number of suspensions imposed pursuant to Article 20, distinguishing between suspensions enacted for the provision of manifestly illegal content, the submission of manifestly unfounded notices and the submission of manifestly unfounded complaints;

   (c) any use made of automatic means for the purpose of content moderation, including a specification of the precise purposes, indicators of the accuracy of the automated means in fulfilling those purposes and any safeguards applied.

2. **Providers of o**~~O~~nline platforms shall publish **in a publicly available section of their online interface**, at least once every six months, information on the average monthly active recipients of the service in each Member State, calculated as an average over the period of the past six months, in accordance with the methodology laid down in the delegated acts adopted pursuant to Article 25(2).

3. **Providers of o**~~O~~nline platforms shall communicate to the Digital Services Coordinator of establishment, upon its request, the information referred to in paragraph 2, updated to the moment of such request. That Digital Services Coordinator may require the **provider of the** online platform to provide additional information as regards the calculation referred to in that paragraph, including explanations and substantiation in respect of the data used. That information shall not include personal data.

4. The Commission may adopt implementing acts to lay down templates concerning the form, content and other details of reports pursuant to paragraph 1. **Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 70.**

Article 24

Online advertising transparency

Providers of o~~O~~nline platforms that **present**~~display~~ advertising on their online interfaces shall ensure that the recipients of the service can identify, for each specific advertisement ~~displayed~~ **presented including user-generated advertisements,** to each individual recipient, in a clear**, salient** and unambiguous manner and in real time:

(a) that the information ~~displayed~~ **presented on the interface or parts thereof** is an advertisement**, including through prominent marking standardized for the individual service**;

(b) the natural or legal person on whose behalf the advertisement is ~~displayed~~**presented**;

(c) **clear and** meaningful information about the ~~main~~ parameters used to determine the recipient to whom the advertisement is ~~displayed~~**presented, ~~presented displayed in an easily accessible manner~~. The information shall be directly and easily accessible from the advertisement.**

Providers of online platforms shall provide recipients of the service with a functionality to declare whether the content they provide is or contains commercial communications within the meaning of Article 2(f) of Directive 2000/31/EC.

When the content provider submits a declaration pursuant to this paragraph, the provider of online platform shall ensure that other recipients of the service can identify in a clear and unambiguous manner and in real time, through prominent marking, that the content provided by the recipients of the service is or contains commercial communications.

2. The visually prominent marking should be adapted to the nature of the individual intermediary interface in the form and degree to which it makes sense for the content. It may vary what elements that makes a visually prominent marking of commercial content dependent on the individual intermediary interface.

3. The Commission shall adopt guidelines regarding the requirements for the marking referred to in paragraph 1(a) of this Article.

Evidence show that a visually prominent and standardised marking of ads across content on the individual intermediary services improves consumers' awareness of the ad. Standardization across content on the individual platforms is essential, but the standardization should be adapted to the individual platform, and should thus not be identical across platforms. The standardized commercial marking should be adapted to the nature of the individual platform and interface in the form and degree to which it makes sense for the content. What is prominent on one intermediary service might not be prominent on another – this will depend on the design and 'look' of the individual intermediary. It should therefore be up to the individual intermediary service to make sure they develop a prominent marking. This could be stressed more clearly in the article or alternatively in the recitals.

Paragraph 3 will allow the Commission to provide guidelines with specifications and suggestions for a visually prominent marking.

We are very positive that it is now clearly stated that the parameters used to determine the recipient should be directly and easily accessible from the ad, so that the consumers can choose to look at why they are being shown the individual ad, rather than having the information appear together with or as a part of the ad. This is important in order to avoid that the information about the meaningful parameters for showing the ad will drown in other information and only present noise to the consumer.

Lastly, we are curious as to the addition of the two last paragraphs of the article, as we fail to see what they add to the provision. Maybe the Precedency could elaborate on the additions?

SECTION 3A

PROVISIONS APPLICABLE TO PROVIDERS OF ONLINE MARKETPLACES

*Article 2~~2~~**4a***

Traceability of traders

1. ~~Where an online platform allows consumers to conclude distance contracts with traders, it~~ **Providers of online marketplaces** shall ensure that traders can only use ~~its~~ **their** services to promote messages on or to offer products or services to consumers located in the Union if, prior to the use of ~~its~~ **their** services, the **providers of** online ~~platform~~ **marketplaces** ha**ve~~s~~** obtained the following information**, where applicable**:

   (a) the name, address, telephone number and electronic mail address of the trader;

   (b) a copy of the identification document of the trader or any other electronic identification as defined by Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council[20];

   (c) the ~~bank~~ **payment** account details of the trader~~, where the trader is a natural person~~;

[20] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

(d) the name, address, telephone number and electronic mail address of the economic operator, within the meaning of Article 3(13) and Article 4 of Regulation (EU) 2019/1020 of the European Parliament and the Council[21] or any relevant act of Union law;

(e) where the trader is registered in a trade register or similar public register, the trade register in which the trader is registered and its registration number or equivalent means of identification in that register;

(f) a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law.

2. The **provider of the** online ~~platform~~ **marketplace** shall, upon receiving that information, make ~~reasonable~~ **best** efforts to assess whether the information referred to in point **(d) of paragraph 1, and** ~~s~~ **prior to the use of their services, points** (a)~~, (d)~~ and (e) of paragraph 1 is reliable through the use of any freely accessible official online database or online interface made available by a Member States or the Union or through requests to the trader to provide supporting documents from reliable sources.

3. Where the **provider of the** online ~~platform~~ **marketplace** obtains **sufficient** indications ~~that~~ any item of information referred to in paragraph 1 obtained from the trader concerned is inaccurate**,** ~~or~~ incomplete **or not up to date**, that **marketplace** ~~platform~~ shall request the trader to correct the information in so far as necessary to ensure that all information is accurate**,** ~~and~~ complete **and up to date**, without delay or within the time period set by Union and national law.

Where the trader fails to correct or complete that information, the online platform shall suspend the provision of its service to the trader until the request is complied with.

---

[21] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).

4. The **provider of the** online **marketplace** ~~platform~~ shall store the information obtained pursuant to paragraph 1 and 2 in a secure manner for the duration of **6 months after the end of the** ~~their~~ contractual relationship with the trader concerned. They shall subsequently delete the information.

5. Without prejudice to paragraph 2, the **providers of online marketplaces** ~~platform~~ shall only disclose the information to third parties where so required in accordance with the applicable law, including the orders referred to in Article 9 and any orders issued by Member States' competent authorities or the Commission for the performance of their tasks under this Regulation.

6. The **provider of** online **marketplace** ~~platform~~ shall make the information referred to in points (a), (d), (e) and (f) of paragraph 1 available to the recipients of the service**, at least on the product listing**, in a clear, easily accessible and comprehensible manner **prior to the purchase**.

~~7. The online platform shall design and organise its online interface in a way that enables traders to comply with their obligations regarding pre-contractual information and product safety information under applicable Union law.~~ ***[this provision is moved to Article 24b]***

We support the requirements in article 24a and the amendments.

Article 24b

Compliance by design

1. **Providers of online marketplaces shall design and organise ~~its~~ their online interface in a way that enables traders to comply with their obligations regarding pre-contractual information and product safety information under applicable Union law.**

2. **The online interface shall allow traders to provide at least the information necessary for the ~~unequivocal~~clear and unambiguous identification of the products or the services offered, and, where applicable, the information concerning the labelling in compliance with rules of applicable Union law on product safety and product compliance.**

3. **The online interface shall be designed in a way that enables the provider of the online marketplace to make their best efforts to make sure that the traders provide complete information referred to in paragraph 1 and 2 and make sure that products or services are not offered as long as the information is incomplete.**

We find that systematic and clear requirements are much needed to help ensure compliance and minimize the spread of illegal content and illegal products. We therefore support the Presidency compromise text on article 24b. However, it seems necessary to specify the required information e.g. in the recitals in order to provide clarity.

The provision seems to lack an obligation for the online marketplace to make an effort to assess whether or not the information provided by the trader is complete, and to make sure that products are not offered as long as the information is incomplete. We find such an obligation to be of great importance in order to ensure that the intended effect can be achieved. Therefore, we suggest inserting paragraph 3 in the Article and a clarification in Recital 50.

Article 24c

Right to information

1. **Where a provider of an online marketplace becomes aware, irrespective of the means used to, of the illegal nature of a product or service offered through its services, it shall inform those recipients of the service that had acquired such product or**

contracted such service during the last six months about the illegality, the identity of the trader and any means of redress.

2. Where the provider of the online marketplace does not have the contact details of the recipients of the service referred to in paragraph 1, the provider shall make publicly available and easily accessible on their online interface the information concerning the illegal products or services removed, the identity of the trader and any means of redress.

We support the Presidency compromise text regarding the right to information.

Article 24d

Use of relevant databases

Where a provider of an online marketplace, who is also considered as a very large online platform, has concrete suspicion, that a specific product or service is not compliant with applicable Union law on product safety and product compliance, that provider shall check relevant databases such as [Safe Gate/Rapex] in order to confirm easily if the product or service is illegal and take the necessary steps to ensure that the product or service is not offered on the online marketplace.

We suggest to add a new Article 24d with an obligation to make use of relevant databases in certain cases. The obligation should only be applied in cases where the provider has concrete suspicion, that a specific product is not compliant with applicable Union legislation on product safety and product compliance. In that case, the provider shall upon specific request check relevant databases for compliance, e.g. Safe Gate/Rapex. If the product is listed, the provider shall not authorize the trader to offer that product on the online marketplace.

Article 24e

Stay-down obligation

Where a provider of an online marketplace, who is also considered as a very large online platform, detects and identifies illegal products or services regardless of how, the provider shall immediately take precautionary steps to prevent this and similarly illegal content from reappearing on the platform. This should as a minimum involve the following:

(a) Checking the infringing trader's remaining products or services for similarly illegal content, and

(b) Monitoring the platform for products or services of the same type that are unequivocally illegal.

We suggest adding a stay-down obligation for very large online marketplaces. Meaning that content that was previously notified and removed as illegal (counterfeit products for an example), should be prevented from being uploaded again on very large online marketplaces. These online marketplaces should have the means and resources to ensure that illegal content does not re-appear and we should as regulators ensure that they take on this responsibility.

The proposed obligation should be applicable for not only online marketplaces, but very large online platforms in general in relation to not only illegal products and services, but illegal content in general. Therefore, the obligation could instead be moved to Section 4 in the proposal.

We find that such an obligation is compliant to the basic principles in the DSA proposal because the online marketplace will have knowledge of specific illegal content and therefore we see the obligation as concrete monitoring and not general. Furthermore, we find the proposal proportionate, since it only applies to very large online platforms.