



Council of the European Union
General Secretariat

Brussels, 30 June 2021

**Interinstitutional files:
2020/0361 (COD)**

WK 8700/2021 INIT

LIMITE

**COMPET
MI
JAI
TELECOM
CT**

**PI
AUDIO
CONSUM
CODEC
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: NL Delegation
To: Delegations

Subject: Digital Services Act: NL Comments on Compromise Text

WK 8700/2021 INIT

LIMITE

EN

Compromise Text	NL suggested amendments ¹	Justification
GENERAL		
<p><i>In the context of this written comments round, NL would like to discuss our objective to further stimulate hosting services providers in assuming their responsibility vis-à-vis illegal content online that is disseminated through their services.</i></p> <p><i>More concretely, we believe that a duty of care imposed on hosting services providers could be a suitable means to attain this objective. We envisage such a duty of care to be construed as a 'reasonable effort requirement' by providers of hosting services to restrict the dissemination of illegal content online through their services. Evidently, a duty of care should remain within the limits set forth by the rules of the DSA proposal: for instance, it should not amount to the imposition of a general monitoring obligation and conflict with Article 7, or any other DSA provisions. The question as to where this incentive may be best incorporated or introduced, i.e. in which Chapter, is still subject to ongoing internal discussions.</i></p> <p><i>We are currently in the midst of developing concrete text suggestions with respect to the duty of care and would therefore like to request the Presidency the opportunity to revisit our proposals at a later stage in this Council Working Party.</i></p>		
SUBJECT MATTER, SCOPE & DELINEATION		
<p><u>(9) This Regulation fully harmonises the rules applicable to intermediary services in the internal market with the objective to ensure a safe, predictable and trusted online environment, where fundamental rights enshrined in the Charter are effectively protected. Accordingly,</u></p>	<p><i>No changes</i></p>	<p><i>NL fully concurs with the compromise text in Recital 9.</i></p> <p><i>We agree with the Commission's choice of the type of legal instrument, namely a Regulation in light of one of the two-pronged objectives of the DSA proposal: furthering and deepening the internal market for digital services.</i></p> <p><i>National divergence, and consequently, fragmentation, from the fully harmonized rules on intermediary services in the EU's internal market</i></p>

¹ The table below and suggested NL amendments (hereinafter: AMs)D are subject to a (parliamentary) scrutiny reserve, without prejudice to future government's considerations, and may evolve or change over time as the DSA proposal progresses in the legislative deliberation stage in Council. Please note that NL's suggested changes in the text are marked **italicized and in blue, bold font. Deletions are marked in strikethrough format.**

Member States should not adopt or maintain additional national requirements on those matters falling within the scope of this Regulation, unless explicitly provided for in this Regulation, since this would affect the direct and uniform application of the fully harmonised rules applicable to the providers of intermediary services in accordance with the objectives of this Regulation. This does not preclude the possibility to apply other national legislation applicable to providers of intermediary services in accordance with Union law, including Directive 2000/31/EC, in particular its Article 3, which pursue other legitimate public interest objectives. This Regulation should complement, yet not affect the application of rules resulting from other acts of Union law regulating certain aspects of the provision of intermediary services, in particular Directive 2000/31/EC,

should be kept to a minimum so as to achieve this objective.

At the same time, we support Member States in legislating on certain matters of the public interest, namely those relating to public policy, the protection of public health, public security, and the protection of consumers, in line with the so-called Country-of-Origin (hereinafter: CoO) principle, contained in Article 3 of Directive 2000/31/EC (hereinafter e-Commerce Directive (eCD)).

Member States seeking to derogate from the rules in the DSA and eCD to achieve public policy objectives that fall within any of the reasons as enumerated under eCD Article 3.4(a), should do so in accordance with the conditions and requirements as laid down in Article 3.4 – 3.6.

<p>with the exception of those changes introduced by this Regulation, Directive 2010/13/EU of the European Parliament and of the Council as amended,² and Regulation (EU) .../.. of the European Parliament and of the Council³—proposed Terrorist Content Online Regulation. Therefore, this Regulation leaves those other acts, which are to be considered <i>lex specialis</i> in relation to the generally applicable framework set out in this Regulation, unaffected. However, the rules of this Regulation apply in respect of issues that are not or not fully addressed by those other acts as well as issues on which those other acts leave Member States the possibility of adopting certain measures at national level.</p>		
---	--	--

² ~~Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Text with EEA relevance), OJ L 95, 15.4.2010, p. 1.~~

³ ~~Regulation (EU) .../.. of the European Parliament and of the Council—proposed Terrorist Content Online Regulation.~~

<p>(12) In order to achieve the objective of ensuring a safe, predictable and trusted online environment, for the purpose of this Regulation the concept of “illegal content” should <u>underpin the general idea that what is illegal offline should also be illegal online. The concept should be defined broadly to cover</u> be defined broadly and also covers information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that relates to activities that are illegal, such as the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, <u>the sale of products or the provision of services in infringement of consumer protection law,</u> the non-</p>	<p>(12) In order to achieve the objective of ensuring a safe, predictable and trusted online environment, for the purpose of this Regulation the concept of “illegal content” should <u>underpin the general idea that what is illegal offline should also be illegal online. The concept should be defined broadly to cover</u> be defined broadly and also covers information relating to illegal content, products, services <i>and activities</i>, <i>activities and or illegal or unlawful information and activities in and of themselves</i>. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that relates to activities that are illegal, such as the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit</p>	<p><i>NL would like to clarify that the term “illegal content” covers both illegal and unlawful content and activities in and of themselves, such as for instance online fraud or scams. It could be the case that the information that is employed for such activities is not illegal in itself, but the activity is, such as for instance, is the case with phishing emails.</i></p> <p><i>In addition, NL favours the explicit reference to “the illegal offer of accommodation services” as an example of the concept of “illegal content online”.</i></p>
--	--	--

<p>authorised use of copyright protected material, or the illegal offer of accommodation services or activities involving infringements of consumer protection law. In this regard, it is immaterial whether the illegality of the information or activity results from Union law or from national law that is consistent with Union law and what the precise nature or subject matter is of the law in question.</p>	<p>products, <u>the sale of products or the provision of services in infringement of consumer protection law,</u> the non-authorized use of copyright protected material, <u>or the illegal offer of accommodation services</u> or activities involving infringements of consumer protection law. In this regard, it is immaterial whether the illegality of the information or activity results from Union law or from national law that is consistent with Union law and what the precise nature or subject matter is of the law in question.</p>	
<p style="text-align: center;">Article 1</p> <p style="text-align: center;">Subject matter, <u>objectives</u> and scope</p> <p>0. The aims of this Regulation are to: <u>is to</u></p> <p>(a) contribute to the proper functioning of the internal market for intermediary services <u>by</u> ÷</p> <p>(b) <u>setting</u> out uniform harmonised rules for a safe, predictable and trusted</p>	<p><i>No changes</i></p>	<p><i>We favour the introduction of the term "harmonized" under new sub-paragraph 0 in Article 1 so as to underline the and clarify the purpose of the proposal for a Regulation: to achieve a more integrated, single market for digital services, underpinned by harmonized rules that apply across the EU.</i></p> <p><i>We have therefore not made any changes with respect to Article 1.</i></p>

<p>online environment, where fundamental rights enshrined in the Charter are effectively protected.</p> <p>1. This Regulation lays down harmonised rules on the provision of intermediary services in the internal market. In particular, it establishes:</p> <ul style="list-style-type: none">(a) a framework for the conditional exemption from liability of providers of intermediary services;(b) rules on specific due diligence obligations tailored to certain specific categories of providers of intermediary services;(c) rules on the implementation and enforcement of this Regulation, including as regards the cooperation of and coordination between the competent authorities. <p>2. The aims of this Regulation are to: <u>[moved to paragraph 0]</u></p>		
--	--	--

<p>3. This Regulation shall apply to intermediary services providedoffered to recipients of the service that have their place of establishment or are locatedresidence in the Union, irrespective of the place of establishment of the providers of those services.</p> <p>4. This Regulation shall not apply to any service that is not an intermediary service or to any requirements imposed in respect of such a service, irrespective of whether the service is provided through the use of an intermediary service.</p> <p>5. This Regulation is without prejudice to the rules laid down by other specific Union legal acts, in particular, the following:</p> <ul style="list-style-type: none">(a) Directive 2000/31/EC;(b) Directive 2010/13/EU;(c) Union law on copyright and related rights;		
---	--	--

<p>(d) Regulation (EU) .../... on preventing the dissemination of terrorist content online [TCO once adopted];</p> <p>(e) Regulation (EU) .../... on European Production and Preservation Orders for electronic evidence in criminal matters and Directive (EU) .../... laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [e-evidence once adopted]</p> <p>(f) Regulation (EU) 2019/1148;</p> <p>(g) Regulation (EU) 2019/1150;</p> <p>(h) Union law on consumer protection and product safety, including Regulation (EU) 2017/2394;</p> <p>(i) Union law on the protection of personal data, in particular</p>		
---	--	--

<p>Regulation (EU) 2016/679 and Directive 2002/58/EC;</p> <p><u>(j) Union law in the field of judicial cooperation in civil matters, in particular Regulation (EU) 1215/2012;</u></p> <p><u>(k) Union law in the field of judicial cooperation in criminal matters, in particular Regulation (EU)/....on European Production and Preservation Orders for electronic evidence in criminal matters;</u></p> <p><u>(l) Directive (EU)/....laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings</u></p>		
<p>Article 2 Definitions</p>	<p>Article 2 Definitions</p>	<p>NL would like to clarify that the term "illegal content" covers both illegal and unlawful content and activities in and of themselves, such as for instance online fraud or scams. It could be the</p>

<p>For the purpose of this Regulation, the following definitions shall apply:</p> <p>(a) 'information society services' means services within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535;</p> <p>(b) 'recipient of the service' means any natural or legal person who for professional ends or otherwise, uses an intermediary service, in particular for the purposes of seeking information or making it accessiblethe relevant intermediary service;</p> <p>(c) 'consumer' means any natural person who is acting for purposes which are outside his or her trade, business, craft or profession;</p> <p>(d) 'to offer services in the Union' means enabling natural or legal or natural persons in one or more Member States to use the services of the provider of information societyintermediary services which has a substantial connection to the Union;</p>	<p>For the purpose of this Regulation, the following definitions shall apply:</p> <p>(a) 'information society services' means services within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535;</p> <p>(b) 'recipient of the service' means any natural or legal person who for professional ends or otherwise, uses an intermediary service, in particular for the purposes of seeking information or making it accessiblethe relevant intermediary service;</p> <p>(c) 'consumer' means any natural person who is acting for purposes which are outside his or her trade, business, craft or profession;</p> <p>(d) 'to offer services in the Union' means enabling natural or legal or natural persons in one or more Member States to use the services of the provider of information societyintermediary services which has a substantial connection to the Union;</p>	<p><i>case that the information that is employed for such activities is not illegal in and of itself.</i></p>
--	--	---

<p>(da) 'such a substantial connection' means <u>a connection of an provider of intermediary services with the Union resulting either from its</u> is deemed to exist where the provider has an establishment in the Union <u>or from</u>; in the absence of such an establishment, the assessment of a substantial connection is based on specific factual criteria, such as:</p> <ul style="list-style-type: none"> - a significant number of users in one or more Member States <u>in relation to their population</u>; or - the targeting of activities towards one or more Member States. <p>(e) 'trader' means any natural person, or any legal person irrespective of whether privately or publicly owned, who is acting, including through any person acting in his or her name or on his or her behalf, for purposes relating to his or her trade, business, craft or profession;</p>	<p>(da) 'such a substantial connection' <u>means a connection of an provider of intermediary services with the Union resulting either from its</u> is deemed to exist where the provider has an establishment in the Union <u>or from</u>; in the absence of such an establishment, the assessment of a substantial connection is based on specific factual criteria, such as:</p> <ul style="list-style-type: none"> - a significant number of users in one or more Member States <u>in relation to their population</u>; or - the targeting of activities towards one or more Member States. <p>(e) 'trader' means any natural person, or any legal person irrespective of whether privately or publicly owned, who is acting, including through any person acting in his or her name or on his or her behalf, for purposes relating to his or her trade, business, craft or profession;</p>	
---	--	--

<p>(f) 'intermediary service' means one of the following information society services:</p> <ul style="list-style-type: none">- a 'mere conduit' service that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;- a 'caching' service that consists of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;- a 'hosting' service that consists of the storage of information provided	<p>(f) 'intermediary service' means one of the following information society services:</p> <ul style="list-style-type: none">- a 'mere conduit' service that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;- a 'caching' service that consists of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;- a 'hosting' service that consists of the storage of information	
---	--	--

<p>by, and at the request of, a recipient of the service;</p> <p>(g) 'illegal content' means any information, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law;</p> <p>(h) 'online platform' means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation;</p> <p>(i) 'dissemination to the public' means making information available, at the request of the recipient of the service</p>	<p>provided by, and at the request of, a recipient of the service;</p> <p>(g) 'illegal content' means any information <i>or activities</i>, which, <i>in or of themselves</i>, or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law;</p> <p>(h) 'online platform' means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation;</p>	
---	---	--

<p>who provided the information, to a potentially unlimited number of third parties;</p> <p><u>(ia) 'online marketplace' means an online platform which allows consumers to conclude distance contracts with other traders or consumers;</u></p> <p>(j) 'distance contract' means a contract within the meaning of Article 2(7) of Directive 2011/83/EU;</p> <p>(k) 'online interface' means any software, including a website or a part thereof, and applications, including mobile applications;</p> <p>(l) 'Digital Services Coordinator of establishment' means the Digital Services Coordinator of the Member State where the provider of an intermediary service is established or its legal representative resides or is established;</p> <p>(m) 'Digital Services Coordinator of destination' means the Digital Services</p>	<p>(i) 'dissemination to the public' means making information available, at the request of the recipient of the service who provided the information, to a potentially unlimited number of third parties;</p> <p><u>(ia) 'online marketplace' means an online platform which allows consumers to conclude distance contracts with other traders or consumers;</u></p> <p>(j) 'distance contract' means a contract within the meaning of Article 2(7) of Directive 2011/83/EU;</p> <p>(k) 'online interface' means any software, including a website or a part thereof, and applications, including mobile applications;</p> <p>(l) 'Digital Services Coordinator of establishment' means the Digital Services Coordinator of the Member State where the provider of an intermediary service is established or its legal representative resides or is established;</p>	
---	--	--

<p>Coordinator of a Member State where the intermediary service is provided;</p> <p>(n) 'advertisement' means information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes, and displayedserved by an online platform on its online interface against remuneration specifically for promoting that information;</p> <p>(o) 'recommender system' means a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed;</p> <p>(p) 'content moderation' means the activities, automated or not, undertaken by providers of intermediary services aimed, in particular at detecting, identifying</p>	<p>(m) 'Digital Services Coordinator of destination' means the Digital Services Coordinator of a Member State where the intermediary service is provided;</p> <p>(n) 'advertisement' means information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes, and displayedserved by an online platform on its online interface against remuneration specifically for promoting that information;</p> <p>(o) 'recommender system' means a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed;</p> <p>(p) 'content moderation' means the activities, automated or not,</p>	
---	---	--

<p>and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, <u>demonetisation</u>, disabling of access to, or removal thereof, or the recipients' ability to provide that information, such as the termination or suspension of a recipient's account;</p> <p>(q) 'terms and conditions' means all terms and conditions or <u>specifications</u>clauses, irrespective of their name or form, which govern the contractual relationship between the provider of intermediary services and the recipients of the services;</p> <p><u>(r) 'turnover' means the amount derived by an undertaking as defined in Article 5(1) of Regulation (EU) No 139/2004.</u></p>	<p>undertaken by providers of intermediary services aimed, <u>in particular</u> at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, <u>demonetisation</u>, disabling of access to, or removal thereof, or the recipients' ability to provide that information, such as the termination or suspension of a recipient's account;</p> <p>(q) 'terms and conditions' means all terms and conditions or specifications<u>clauses</u>, irrespective of their name or form, which govern the contractual relationship between the provider of intermediary services and the recipients of the services;</p> <p><u>(r) 'turnover' means the amount derived by an undertaking as</u></p>	
---	---	--

defined in Article 5(1) of Regulation (EU) No 139/2004.		
GENERAL MONITORING – SPECIFIC MONITORING DELINEATION		
<p>(28) Providers of intermediary services should not be subject to a monitoring obligation with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation, in accordance with the conditions established in this Regulation. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or a general active fact-finding obligation, or as a general obligation for providers to take proactive measures to relation to illegal content.</p>	<p>(28) Providers of intermediary services should not be subject to a monitoring obligation with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not This does not affect orders by national authorities in accordance with national legislation, in accordance with the conditions established in this Regulation. The ban on a general monitoring obligation on intermediary services should not prevent Member States from imposing monitoring obligations of a specific nature, provided, they meet the principles of proportionality and necessity, are in conformity with the conditions as set out by any relevant Union law, including CJEU case-law, and the illegal content in question is specified, well-defined and delineated. A monitoring obligation that requires intermediary services to perform a search of potentially</p>	<p><i>NL is open to discussing ways in discerning more clearly the boundary between specific and general monitoring obligations, as this lack of clarity has resulted in legal uncertainty for the Member States and companies alike. To address this particular issue, we have drawn inspiration from the CJEU judgement Glawischnig-Piesczek v Facebook Ireland Limited. We are seeking ways to provide for more clarity without undermining – both in a de jure and de facto manner – the ban on a general monitoring obligation as contained in Article 7 of the DSA proposal.</i></p> <p><i>We welcome any input and the views of other Member States to effectively tackle this issue. We would advocate for making such changes in the accompanying Recital 28 to Article 7, rather than modifying the actual provision itself.</i></p>

illegal content without any specification, or a specific monitoring obligation that puts excessive burdens or requires unreasonable or excessive resources and measures by intermediary services beyond the use of readily-available automated tools and technologies, would not be considered to fall within the definition of a specific monitoring obligation definition. It follows from relevant CJEU case-law that specific monitoring obligations may be accompanied by a corollary obligation on intermediary services to remove (access to), or block content identical to, or essentially equivalent, information which it stores, that has previously been declared to be illegal or unlawful, as specified in the specific monitoring obligation, insofar this does not compel intermediary to carry out an independent assessment of that specific content.

Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or **a general** active fact-finding obligation, or as a general obligation for

	providers to take proactive measures to relation to illegal content.	
<p style="text-align: center;"><i>Article 7</i></p> <p style="text-align: center;"><i>No general monitoring or active fact-finding obligations</i></p> <p>No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers.</p>	<p style="text-align: center;"><i>Article 7</i></p> <p style="text-align: center;"><i>No general monitoring or active fact-finding obligations</i></p> <p>No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers.</p>	<p><i>As stated above, we prefer to clarify the line between specific and general monitoring in the accompanying Recital 28, rather than the actual provision.</i></p>
ORDERS		
<p style="text-align: center;"><i>Article 8</i></p> <p style="text-align: center;"><i>Orders to act against illegal content</i></p> <p>1. Providers of intermediary services shall, upon the receipt of an order to act against one or more specific items of illegal content, issued by the relevant national judicial or administrative authorities, on the basis of the applicable Union or national law, in conformity with Union law, inform the authority issuing the order of the</p>	<p><i>Subject to ongoing analysis</i></p>	<p><i>Paragraph 3 of both Articles 8 and 9 seem to imply that Digital Services Coordinators (DSCs) have to inform other DSCs about all orders that are issued against intermediary services. Is this meant to also include situations whereby orders are based on national law, have an exclusive national character, and concern intermediary services that are located in the Member State where the order was issued?</i></p> <p><i>Concerning <u>sub-paragraphs 3a and 4 of Articles 8 & 9</u>, there seems to be a lack of clarity and inconsistency: Sub-paragraph 4 stipulates that <u>the conditions and requirements</u> of Articles 8 and 9 are without prejudice to <u>requirements</u> under <u>national criminal procedural law</u>, whereas sub-paragraph 3a states more broadly without</i></p>

<p>effect given to the orders, without undue delay, specifying the action taken and the moment when the order action was <u>executed</u>taken.</p> <p>2. Member States shall ensure that the orders referred to in paragraph 1 meet <u>at least</u> the following conditions, <u>when transmitted to the provider:</u></p> <p>(a) the orders contains the following elements:</p> <p>(i)– a statement of reasons explaining why the information is illegal content, by reference to the specific provision of Union or national law infringed;</p> <p>(ii)– one or more exact uniform resource locators and, where necessary, additional information enabling the <u>provider of intermediary services to identify and locate</u> identification of the illegal content concerned, <u>such as one or more exact</u></p>		<p><i>prejudice to <u>national criminal procedural law</u>, without singling out an aspect under national criminal procedural law.</i></p> <p><i>This raises the question as to the correct way of construing its meaning: Are we to read these paragraphs as stating that Articles 8 and 9 do not have any bearing on national criminal procedural law?</i></p> <p><i>We believe the sub-paragraphs should state clearly and unambiguously that Articles 8 and 9 are without prejudice to national procedural criminal law. If this is not the case, however, we will put forward concrete text suggestions to this effect.</i></p>
--	--	--

<p><u>uniform resource locators (URL);</u></p> <p>(iii)– information about redress available to the provider of the service and to the recipient of the service who provided the content;</p> <p>(b) the territorial scope of the order, on the basis of the applicable rules of Union and national law, including the Charter, and, where relevant, general principles of international law, does not exceed what is strictly necessary to achieve its objective;</p> <p>(c) the order is drafted <u>transmitted</u> in the language declared by the provider <u>pursuant to Article 10(3) or in another official language of the Union, bilaterally agreed by the authority issuing the order and the provider,</u> and is sent to the</p>		
--	--	--

<p>appointed electronic point of contact, established by the provider, in accordance with Article 10.</p> <p>3. <u>After receiving the order from the competent authority, t</u>The Digital Services Coordinator from the Member State of the judicial or administrative authority issuing the order shall, without undue delay, transmit a copy of the orders referred to in paragraph 1 to all other Digital Services Coordinators through the system established in accordance with Article 67.</p> <p><u>3a. Without prejudice to national criminal procedural law in conformity with Union law, providers of intermediary services shall inform the recipient of the service who provided the content, at the latest at the time of the removal or disabling of access, of the order received and the effect given to it. Such information to the recipient of the service shall, at</u></p>		
--	--	--

<p><u>least, include the statement of reasons and the redress possibilities, as included in the order pursuant to point a of paragraph 2, and the territorial scope of the order.</u></p> <p>4. The conditions and requirements laid down in this article shall be without prejudice to requirements under national criminal procedural law in conformity with Union law.</p>		
<p style="text-align: center;"><i>Article 9</i></p> <p style="text-align: center;"><i>Orders to provide information</i></p> <p>1. Providers of intermediary services shall, upon receipt of an order to provide a specific item of information about one or more specific individual recipients of the service, issued by the relevant national judicial or administrative authorities on the basis of the applicable Union or national law, in conformity with Union law, inform without undue delay the authority of</p>	<p><i>Currently subject to analysis</i></p>	<p><i>Ibid; see Justification with respect to Article 8</i></p>

<p>issuing the order of its receipt, and of the effect given to the order <u>and the moment when the order was executed.</u></p> <p>2. Member States shall ensure that orders referred to in paragraph 1 meet the following conditions, <u>when transmitted to the provider:</u></p> <p>(a) the order contains the following elements:</p> <p>(i) a statement of reasons explaining the objective for which the information is required and why the requirement to provide the information is necessary and proportionate to determine compliance by the recipients of the intermediary services with applicable Union or national rules, unless such a statement cannot be provided for reasons related to the prevention, investigation,</p>		
---	--	--

<p>detection and prosecution of criminal offences;</p> <p>(ii)– information about redress available to the provider and to the recipients of the service concerned;</p> <p>(b) the order only requires the provider to provide information already collected for the purposes of providing the service and which lies within its control;</p> <p>(c) the order is drafted transmitted in the language declared by the provider pursuant to Article 10(3) or in another official language of the Union, bilaterally agreed by the authority issuing the order and the provider, and is sent to the electronic point of contact establishedappointed by that provider, in accordance with Article 10;</p> <p>3. <u>After receiving the order from the competent authority,</u> tThe Digital</p>		
---	--	--

<p>Services Coordinator from the Member State of the national judicial or administrative authority issuing the order shall, without undue delay, transmit a copy of the order referred to in paragraph 1 to all Digital Services Coordinators through the system established in accordance with Article 67.</p> <p><u>3a. Without prejudice to national criminal procedural law in conformity with Union law, providers of intermediary services shall inform the recipient of the service concerned, at the latest at the time when the order is executed, of the order received and the effect given to it. Such information to the recipient of the service shall, at least, include the statement of reasons and the redress possibilities included in the order.</u></p> <p>4. The conditions and requirements laid down in this article shall be without prejudice to requirements under</p>		
---	--	--

national criminal procedural law in conformity with Union law.		
DUE DILIGENCE		
<p style="text-align: center;"><i>Article 14</i></p> <p style="text-align: center;"><i>Notice and action mechanisms</i></p> <p>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.</p> <p>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</p>	<p style="text-align: center;"><i>Article 14</i></p> <p style="text-align: center;"><i>Notice and action mechanisms</i></p> <p>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.</p> <p>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</p>	<p><i>NL believes that requiring individuals to list their name jeopardizes users' anonymity on the Internet, which, in turn, could undermine the fundamental right to privacy, freedom of expression and freedom of information online.</i></p> <p><i>Additionally, fear of retaliation may create a barrier for victims and other notifiers from flagging the illegal content in question.</i></p> <p><i>Anonymous notices should therefore be the norm unless there is a justified exception and should have the same legal effect as non-anonymous notices, i.e. give rise to actual knowledge pursuant to Article 14(3) of the DSA proposal.</i></p>

<p>containing all of the following elements:</p> <p>(a) an sufficiently substantiated explanation of the reasons why the individual or entity considers the information in question to be illegal content;</p> <p>(b) a clear indication of the electronic location of that information, in particular <u>such as</u> the exact URL or URLs, and, where necessary, additional information enabling the identification of the illegal content;</p> <p>(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;</p> <p>(d) a statement confirming the good faith belief of the individual or entity submitting the notice that</p>	<p>enable and facilitate the submission of notices containing all of the following elements:</p> <p>(a) an sufficiently substantiated explanation of the reasons why the individual or entity considers the information in question to be illegal content;</p> <p>(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;</p> <p>(c) the name and an electronic mail address of the individual or entity submitting the notice, except where the name of the individual or entity submitting the notice is a prerequisite for the evaluation of the permissibility of the content</p>	
--	---	--

<p>the information and allegations contained therein are accurate and complete.</p> <p>3. Notices that include the elements referred to in paragraph 2 <u>on the basis of which a diligent provider of hosting services can identify the illegality of the content in question</u> 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.</p> <p>4. Where the notice contains the name and an electronic <u>contact information</u> mail address of the individual or entity that submitted it, the provider of hosting services shall, promptly <u>without undue delay</u>, send a confirmation of receipt of the notice to that individual or entity.</p> <p>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,</p>	<p><i>in question, as identified in 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;</i></p> <p>(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.</p> <p>3. Notices that include the elements referred to in paragraph 2 <u>on the basis of which a diligent provider of hosting services can identify the illegality of the content in question</u> 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.</p>	
--	--	--

<p>providing information on the redress possibilities in respect of that decision.</p> <p>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 54.</p>	<p>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.</p> <p>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.</p> <p>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</p>	
---	---	--

	in the notification referred to in paragraph 54 .	
<p style="text-align: center;"><i>Article 15</i> <i>Statement of reasons</i></p> <p>1. Where a provider of hosting services decides to remove or disable access to <u>or otherwise restrict the visibility of</u> specific items of information provided by the recipients of the service, <u>or to suspend or terminate monetary payments related to those items,</u> irrespective of the means used for detecting, identifying or removing or disabling access to <u>or for restricting the visibility or monetisation of</u> that information and of the reason for its decision, it shall inform the recipient <u>where the electronic contact details are known to the provider, prior to or at the latest</u> at the time of the removal or disabling of access <u>or the restriction of visibility or monetisation taking effect,</u> of the decision and provide with a clear and</p>	<p style="text-align: center;"><i>Article 15</i> <i>Statement of reasons</i></p> <p>1. Where a provider of hosting services decides to <i>maintain or</i> remove or disable access to <u>or otherwise restrict the visibility of</u> specific items of information provided by the recipients of the service, <u>or to suspend or terminate monetary payments related to those items,</u> irrespective of the means used for detecting, identifying or removing or disabling access to <u>or for restricting the visibility or monetisation of</u> that information and of the reason for its decision, it shall inform the recipient <u>where the electronic contact details are known to the provider, prior to or at the latest</u> at the time of the removal or disabling of access <u>or the restriction of visibility or monetisation taking effect,</u> of the decision and</p>	<p><i>NL believes that Article 15's scope should be extended both decisions by hosting services providers to keep the content in question up on their services (so-called "must-carry" decisions).</i></p> <p><i>Extending the scope of Article 15 in this respect provides for more accountability and transparency of the content moderation decisions made by hosting providers vis-à-vis its users.</i></p>

<p>specific statement of reasons for that decision.</p> <p>2. The statement of reasons referred to in paragraph 1 shall at least contain the following information:</p> <p>(a) whether the decision entails either the removal of, or the disabling of access to, <u>the restriction of the visibility of,</u> the information <u>or the suspension or termination of monetary payments related to that information</u>and, where relevant, the territorial scope of the disabling of access;</p> <p>(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;</p> <p>(c) where applicable, information on the use made of automated means in taking the decision, including where the decision was</p>	<p>providewith a clear and specific statement of reasons for that decision.</p> <p>2. The statement of reasons referred to in paragraph 1 shall at least contain the following information:</p> <p>(a) whether the decision entails either the removal of, or the disabling of access to, <u>the restriction of the visibility of,</u> the information <u>or the suspension or termination of monetary payments related to that information</u>and, where relevant, the territorial scope of the disabling of access;</p> <p>(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;</p> <p>(c) where applicable, information on the use made of automated</p>	
---	--	--

<p>taken in respect of content detected or identified using automated means;</p> <p>(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;</p> <p>(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;</p> <p>(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-</p>	<p>means in taking the decision, including where the decision was taken in respect of content detected or identified using automated means;</p> <p>(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;</p> <p>(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;</p> <p>(f) information on the redress possibilities available to the recipient of the service in respect of the decision, in</p>	
---	---	--

<p style="text-align: center;">court dispute settlement and judicial redress</p> <p>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.</p> <p>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.</p>	<p style="text-align: center;">particular through internal complaint-handling mechanisms, out-of-court dispute settlement and judicial redress</p> <p>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.</p> <p>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.</p>	
---	---	--

<p style="text-align: center;"><i>Article 15a²¹</i></p> <p style="text-align: center;"><i>Notification of suspicions of criminal offences</i></p> <p>1. Where an 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.</p> <p>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</p>	<p style="text-align: center;"><i>No changes</i></p>	<p><i>NL appreciates the explicit recognition and inclusion in the text in the new Article 15a of threats to the life or safety involving one or more individuals.</i></p> <p><i>NL further welcomes the fact that Article 21 has been moved to Article 15a, thereby extending the scope of the obligations relating to the notification of suspicions of criminal offences to hosting services.</i></p> <p><i>More generally speaking, we welcome the fact that the term "online platforms" has been replaced by "hosting services" relating to several of the due diligence obligations in Chapter III, as providers of hosting services that are not necessarily platforms are often abused for crime-related purposes.</i></p>

<p>established or has its legal representative or inform Europol.</p> <p>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.</p>		
<p style="text-align: center;"><i>Article 16</i></p> <p style="text-align: center;"><i>Exclusion for micro and small enterprises</i></p> <p>This Section and Section 3a shall not apply to <u>providers of</u> online platforms that qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC <u>and which are not very large online platforms in accordance with Article 25.</u></p>	<p style="text-align: center;"><i>Subject to ongoing analysis</i></p>	<p><i>NL recognizes excluding micro- and small companies from the obligations for online platforms serves to limit disproportionate administrative burdens on the business community, and avoids making entry barriers too high. This can be conducive to innovation in Europe.</i></p> <p><i>However, such an exemption should not result in illegal content and activities migrating to smaller online platforms, which, despite their limited size, turnover and number of employees, still have significant reach. This would undermine the objective of the proposal to create a safer online environment.</i></p> <p><i>Reach, defined in the form of the number of users of an online platform, may be a better-suited</i></p>

		<p><i>alternative in determining whether certain companies would qualify for the exemption in Article 16.</i></p> <p><i>Unfortunately, we note that such a concept is still lacking in the text and would therefore like to reiterate our readiness to work with other Member States to develop this in further detail.</i></p>
<p style="text-align: center;"><i>Article 17</i></p> <p style="text-align: center;"><i>Internal complaint-handling system</i></p> <p>1. <u>Providers of</u> online platforms shall provide recipients of the service <u>and individuals or entities that have submitted a notice</u>, 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 <u>decision taken by the provider of the online platform not to act upon the receipt of a notice or against the</u> following decisions taken by the <u>provider of the</u> online platform on the ground that the information provided by the recipients is illegal content or</p>	<p><i>No changes</i></p>	<p><i>We support the changes with respect to Article 17, concerning the internal complaint handling system, whereby recipients may challenge both removal decisions <u>and</u> must-carry decisions (where a platform has not removed/disabled access to information).</i></p>

<p>incompatible with its terms and conditions:</p> <ul style="list-style-type: none">(a) decisions <u>whether or not</u> to remove or disable access to <u>or restrict visibility of</u> the information;(b) decisions <u>whether or not</u> to suspend or terminate the provision of the service, in whole or in part, to the recipients;(c) decisions <u>whether or not</u> to suspend or terminate the recipients' account;<u>(d) decision whether or not to restrict the ability to monetize content provided by the recipients.</u> <p>2. <u>Providers of online</u> 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.</p>		
--	--	--

<p>3. Providers of Online 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 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, it shall reverse its decision referred to in paragraph 1 without undue delay.</p>		
<p>4. Providers of Online 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</p>		

<p>for in Article 18 and other available redress possibilities.</p> <p>5. Providers of oOnline platforms shall ensure that the decisions, referred to in paragraph 4, are not solely taken on the basis of automated means.</p>		
<p style="text-align: center;"><i>Article 19 Trusted flaggers</i></p> <p>1. Providers of oOnline 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.</p> <p>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</p>	<p style="text-align: center;"><i>Article 19 Trusted flaggers</i></p> <p>1. Providers of oOnline 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 diligently, with priority and without delay.</p> <p>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</p>	<p><i>To maintain consistency, online platforms should equally be under the obligation to process noticed by trusted flaggers diligently, as applicants are under the obligation submit notices in a diligent manner.</i></p>

<p>demonstrated to meet all of the following conditions:</p> <ul style="list-style-type: none">(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;(c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner. <p>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 <u>or revoked it in accordance with paragraph 6.</u></p> <p>4. The Commission shall publish the information referred to in paragraph 3 in a publicly available <u>and easily</u></p>	<p>is established, where the applicant has demonstrated to meet all of the following conditions:</p> <ul style="list-style-type: none">(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;(c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner. <p>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 <u>or revoked it in accordance with paragraph 6.</u></p> <p>4. The Commission shall publish the information referred to in paragraph 3</p>	
--	---	--

<p>5. <u>accessible</u> database and keep the database updated.</p> <p>Where <u>a provider of</u> 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.</p> <p>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</p>	<p>in a publicly available <u>and easily accessible</u> database and keep the database updated.</p> <p>5. Where <u>a provider of</u> 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.</p> <p>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</p>	
--	--	--

<p>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.</p> <p>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.</p>	<p>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.</p> <p>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.</p>	
<p style="text-align: center;"><i>Article 20</i> <i>Measures and protection against misuse</i></p> <p>1. Providers of online platforms shall suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services</p>	<p style="text-align: center;"><i>Article 15b Article 20</i> <i>Measures and protection against misuse</i></p> <p>1. Providers of <i>online platforms</i> shall suspend, for a reasonable period of time and after having issued a prior warning, the</p>	<p><i>NL believes this Article, like Article 21 which has been converted to Article 15a, should be applicable to hosting services and online platforms alike.</i></p> <p><i>Given the fact that hosting services, like platforms, are subject to the Notice and Action (N&A) mechanism, they should have the possibility to resort to measures to protect themselves against misuse of their services.</i></p>

<p>to recipients of the service that frequently provide manifestly illegal content.</p> <p>2. Providers of Online platforms shall 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.</p> <p>3. <u>When deciding on the suspension, providers of</u> Online 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</p>	<p>provision of their services to recipients of the service that frequently provide manifestly illegal content.</p> <p>2. Providers of Online platforms hosting services shall 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.</p> <p>3. <u>When deciding on the suspension, providers of eOnline platforms</u> <i>hosting services</i> 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</p>	
---	--	--

<p>of the online platform. Those circumstances shall include at least the following:</p> <p>(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;</p> <p>(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;</p> <p>(c) the gravity of the misuses, including the nature of illegal content, and of its consequences;</p> <p>(d) where it is possible to infer it, the intention of the recipient, individual, entity or complainant.</p> <p>4. Providers of online 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</p>	<p>and circumstances apparent from the information available to the provider of the online platform hosting service. Those circumstances shall include at least the following:</p> <p>(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;</p> <p>(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;</p> <p>(c) the gravity of the misuses, including the nature of illegal content, and of its consequences;</p> <p>(d) where it is possible to infer it, the intention of the recipient, individual, entity or complainant.</p>	
---	---	--

<p>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.</p>	<p>4. Providers of eOnline platforms hosting services 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.</p>	
<p style="text-align: center;"><u>SECTION 3A</u> <u>PROVISIONS APPLICABLE TO PROVIDERS OF ONLINE MARKETPLACES</u></p> <p style="text-align: center;"><i>Article 224a</i> <i>Traceability of traders</i></p> <p>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</p>	<p style="text-align: center;"><i>Subject to ongoing analysis</i></p>	<p><i>As a general remark, NL has noticed how Article 22 in Chapter III, section 3, has given rise to confusion and calls from both inside the Council and externally, from industry, to differentiate more clearly between speech-related content services (i.e. social media platforms) and product/services-related content services (i.e. online marketplaces) obligations.</i></p> <p><i>We recognise the Commission’s rationale to avoid making too much of a clear-cut distinction between these two types of content category-based obligations to ensure the future-proof character of the provision, especially against the backdrop of an increasing blending of services, for instance influencers selling products on social media platforms.</i></p>

<p>offer products or services to consumers located in the Union if, prior to the use of its <u>their</u> services, the providers of online platform marketplaces <u>marketplaces</u> have obtained the following information, where applicable:</p> <ul style="list-style-type: none">(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 Council⁴;(c) the bank payment 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		<p><i>At the same time, however, we are open to differentiate more clearly between the services provided by online platforms and the corresponding responsibilities.</i></p> <p><i>We therefore welcome the new Section 3a, in conjunction with the inclusion of an "online marketplace" definition in Article 2 of the text. However, several open-ended issues remain which we would like to highlight here:</i></p> <p><i>First, how are "traders" to be construed within the new Article 24a? How is a distinction made between a third party being a trader or merely a consumer? Can this be based on the rules under the so-called 'Omnibus Directive' whereby third parties are required to fill out a declaration form, indicating whether they are a professional trader or merely a consumer? As mentioned before, we believe C2C relations should stay excluded from the scope of this provision.</i></p> <p><i>Second, and this is linked to the first issue, the fact that we wish to maintain the scope limited to professional traders only, should not exonerate online marketplaces from taking action in the event the declaration of a third party declaring to be a "consumer" is erroneous and turns out to be a "trader" instead.</i></p> <p><i>Third, why are advertisers not included in this provision? Problems including scams and deceptions of consumers can also occur through online advertising.</i></p>
--	--	---

⁴ 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.

<p>Article 3(13) and Article 4 of Regulation (EU) 2019/1020 of the European Parliament and the Council⁵ or any relevant act of Union law;</p> <p>(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;</p> <p>(f) a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law.</p> <p>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 points (a), (d) and (e) of paragraph 1 is reliable</p>		<p><i>Fourth, we still have concerns about individual traders who operate from their homes (and do not have a physical office address). Such traders would, pursuant to this article, need to provide sensitive information such as a copy of their ID. We would like to include minimum safeguards in case of data disclosure and retention.</i></p> <p><i>Fifth, more generally from a personal data perspective, especially in the case of individual traders operating from home, and in the context of increasingly frequent data leaks, we are concerned about the protection of such sensitive data gathered for the purposes of the KYBC obligation:</i></p> <p><i>Are there any safeguards as to the safe and correct storage of the data provided pursuant to sub-paragraph 1, some of which – as explained above – is personal data?</i></p> <p><i>on data retention, we take note of a 6 months period during which online marketplaces need to store the information obtained pursuant to Article 24a. Can the Presidency further explain its choice for this specific time period, and has it considered relevant CJEU case-law on data retention in this regard?</i></p> <p><i>Related to the issue of data leaks, is the hacking by malicious actors of online platforms to collect and sell these data to other parties, which, in turn, use it to commit fraud.</i></p>
---	--	---

⁵ 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).

<p>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.</p> <p>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, 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, without delay or within the time period set by Union and national law.</p> <p>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.</p>		<p><i>What kind of safeguards exist when such data is disclosed to third parties?</i></p> <p><i>In addition, are online platforms allowed to use the information gathered on traders pursuant to the requirements contained in Article 22.1 for other commercial purposes? We believe this flexibility conferred on online marketplaces to be incompatible with the rules in the GDPR.</i></p>
--	--	--

<p>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.</p>		
<p>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.</p>		
<p>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, in a clear,</p>		

<p>easily accessible and comprehensible manner.</p> <p>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. <u>[this provision is moved to Article 24b]</u></p>		
VLOPS		
<p>(59) <u>Providers of</u> Very large online platforms should, where appropriate, conduct their risk assessments and design their risk mitigation measures with the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations. <u>In the assessment on whether a measure is reasonable, proportionate and effective, special</u></p>	<p><i>No changes</i></p>	<p><i>we endorse the Presidency's additional language requiring VLOPs to take into account the right to freedom of expression when considering risk mitigation measures on the basis of proportionality, effectiveness and reasonableness.</i></p>

<p><u>consideration should be given to the right to freedom of expression.</u></p>		
<p style="text-align: center;"><i>Article 27</i> <i>Mitigation of risks</i></p> <p>1. Providers of Very large online platforms shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 26. Such measures may include, where applicable:</p> <ul style="list-style-type: none"> (a) adapting content moderation or recommender systems, their decision-making processes, the features or functioning of their services, or their terms and conditions; (b) targeted measures aimed at limiting the display of advertisements in association with the service they provide; (c) reinforcing the internal processes or supervision of any of their 	<p style="text-align: center;"><i>Article 27</i> <i>Mitigation of risks</i></p> <p>1. Providers of Very large online platforms shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 26.</p> <p><i>Prior to putting in place such measures, very large online platforms shall give special consideration to the impact such measures may have on the right to freedom of expression.</i></p> <p>measures may include, where applicable:</p> <ul style="list-style-type: none"> (a) adapting content moderation or recommender systems, their decision-making processes, the features or functioning of their 	<p><i>We would like to ask why the requirement imposed on VLOPs to evaluate the impact on the freedom of expression online when considering risk mitigation measures in Recital 59 has not been reproduced in Article 27?</i></p>

<p>activities in particular as regards detection of systemic risk;</p> <p>(d) initiating or adjusting cooperation with trusted flaggers in accordance with Article 19;</p> <p>(e) initiating or adjusting cooperation with other <u>providers of</u> online platforms through the codes of conduct and the crisis protocols referred to in Article 35 and 37 respectively.</p> <p><u>(f) taking awareness-raising measures and adapting their online interface for increased user information.</u></p> <p>2. The Board, in cooperation with the Commission, shall publish comprehensive reports, once a year, which shall include the following:</p> <p>(a) identification and assessment of the most prominent and recurrent systemic risks reported by <u>providers of</u> very large online platforms or identified</p>	<p>services, or their terms and conditions;</p> <p>(b) targeted measures aimed at limiting the display of advertisements in association with the service they provide;</p> <p>(c) reinforcing the internal processes or supervision of any of their activities in particular as regards detection of systemic risk;</p> <p>(d) initiating or adjusting cooperation with trusted flaggers in accordance with Article 19;</p> <p>(e) initiating or adjusting cooperation with other <u>providers of</u> online platforms through the codes of conduct and the crisis protocols referred to in Article 35 and 37 respectively.</p> <p><u>(f) taking awareness-raising measures and adapting their</u></p>	
---	--	--

<p>through other information sources, in particular those provided in compliance with Article 31 and 33;</p> <p>(b) best practices for providers of very large online platforms to mitigate the systemic risks identified.</p> <p>3. The Commission, in cooperation with the Digital Services Coordinators, may issue general guidelines on the application of paragraph 1 in relation to specific risks, in particular to present best practices and recommend possible measures, having due regard to the possible consequences of the measures on fundamental rights enshrined in the Charter of all parties involved. When preparing those guidelines the Commission shall organise public consultations.</p>	<p style="text-align: center;"><u>online interface for increased user information.</u></p> <p>2. The Board, in cooperation with the Commission, shall publish comprehensive reports, once a year, which shall include the following:</p> <p>(a) identification and assessment of the most prominent and recurrent systemic risks reported by providers of very large online platforms or identified through other information sources, in particular those provided in compliance with Article 31 and 33;</p> <p>(b) best practices for providers of very large online platforms to mitigate the systemic risks identified.</p> <p>3. The Commission, in cooperation with the Digital Services Coordinators, may issue general guidelines on the application of paragraph 1 in relation to specific risks, in particular to</p>	
--	--	--

	<p>present best practices and recommend possible measures, having due regard to the possible consequences of the measures on fundamental rights enshrined in the Charter of all parties involved. When preparing those guidelines the Commission shall organise public consultations.</p>	
ENFORCEMENT		
<p style="text-align: center;"><i>Article 45</i> <i>Cross-border cooperation among Digital Services Coordinators</i></p> <p>1. Where a Digital Services Coordinator of destination has reasons to suspect that a provider of an intermediary service, not under the jurisdiction of the Member State concerned, infringed this Regulation, it may shall request the Digital Services Coordinator of establishment to assess the matter and take the necessary investigatory and</p>	<p style="text-align: center;"><i>Article 45</i> <i>Cross-border cooperation among Digital Services Coordinators</i></p> <p>1. Where a Digital Services Coordinator of destination has reasons to suspect that a provider of an intermediary service, not under the jurisdiction of the Member State concerned, infringed this Regulation, it shall may shall request require the Digital Services Coordinator of establishment to assess the matter and take the necessary investigatory</p>	<p><i>Generally speaking, we would like to strengthen the cooperation mechanism between the Digital Services Coordinators, the Board, and the Commission.</i></p> <p><i>We would therefore like to shore up some of the language around the cooperation between the Digital Services Coordinators of the Member States (including between establishment and destination), as well as the Board and the Commission, favouring more legally binding terminology that enables DSCs and the Board to act more effectively and efficiently. We would welcome further discussion on the cooperation mechanism and other enforcement-related aspects of the Regulation with all the Member States in future Working Party sessions.</i></p>

<p>enforcement measures to ensure compliance with this Regulation.</p> <p>Where the Board has reasons to suspect that a provider of intermediary services infringed this Regulation in a manner involving at least three Member States, it may recommend the Digital Services Coordinator of establishment to assess the matter and take the necessary investigatory and enforcement measures to ensure compliance with this Regulation.</p> <p>2. A request or recommendation pursuant to paragraph 1 shall at least indicate:</p> <p>(a) the electronic point of contact of the provider of the intermediary services concerned as provided for in Article 10;</p> <p>(b) a description of the relevant facts, the provisions of this Regulation concerned and the reasons why the Digital Services Coordinator that sent the request, or the Board, suspects</p>	<p>and enforcement measures to ensure compliance with this Regulation.</p> <p>Where the Board has reasons to suspect that a provider of intermediary services infringed this Regulation in a manner involving at least three Member States, it shall require may recommend the Digital Services Coordinator of establishment to assess the matter and take the necessary investigatory and enforcement measures to ensure compliance with this Regulation.</p> <p>2. An requirement to act request or recommendation pursuant to paragraph 1 shall at least indicate:</p> <p>(a) the electronic point of contact of the provider of the intermediary services concerned as provided for in Article 10;</p> <p>(b) a description of the relevant facts, the provisions of this Regulation concerned and the reasons why the Digital</p>	
--	---	--

<p>that the provider infringed this Regulation;</p> <p>(c) any other information that the Digital Services Coordinator that sent the request, or the Board, considers relevant, including, where appropriate, information gathered on its own initiative or suggestions for specific investigatory or enforcement measures to be taken, including interim measures.</p> <p>3. The Digital Services Coordinator of establishment shall take into utmost account the request or recommendation pursuant to paragraph 1. Where it considers that it has insufficient information to act upon the request or recommendation and has reasons to consider that the Digital Services Coordinator that sent the request, or the Board, could provide additional information, it may request such information. The time period laid down in paragraph 4 shall be</p>	<p>Services Coordinator that sent the request, or the Board, suspects that the provider infringed this Regulation;</p> <p>(c) any other information that the Digital Services Coordinator that sent the request, or the Board, considers relevant, including, where appropriate, information gathered on its own initiative or suggestions for specific investigatory or enforcement measures to be taken, including interim measures.</p> <p>3. <i>The Digital Services Coordinator of establishment shall take into utmost account the request or recommendation pursuant to paragraph 1.</i> Where <i>The Digital Services Coordinator of establishment</i> <i>it</i> considers that it has insufficient information to act <i>upon the request or recommendation</i> and has reasons to consider that the Digital Services</p>	
---	---	--

<p>suspended until that additional information is provided.</p> <p>4. The Digital Services Coordinator of establishment shall, without undue delay and in any event not later than two months following receipt of the request or recommendation, communicate to the Digital Services Coordinator that sent the request, or the Board, its assessment of the suspected infringement, or that of any other competent authority pursuant to national law where relevant, and an explanation of any investigatory or enforcement measures taken or envisaged in relation thereto to ensure compliance with this Regulation.</p> <p>5. Where the Digital Services Coordinator that sent the request, or, where appropriate, the Board, did not receive a reply within the time period laid down in paragraph 4 or where it does not agree with the assessment of the Digital Services Coordinator of establishment, it may refer the matter to the Commission, providing all</p>	<p>Coordinator that sent the request, or the Board, could provide additional information, it shall may request such information. The time period laid down in paragraph 4 shall be suspended until that additional information is provided.</p> <p>4. The Digital Services Coordinator of establishment shall, without undue delay and in any event not later than two months following receipt of the requirement to act request or recommendation, communicate to the Digital Services Coordinator that sent the request, or the Board, its assessment of the suspected infringement, or that of any other competent authority pursuant to national law where relevant, and an explanation of any investigatory or enforcement measures taken or envisaged in relation thereto to ensure compliance with this Regulation.</p> <p>5. Where the Digital Services Coordinator that sent the</p>	
--	---	--

<p>relevant information. That information shall include at least the request or recommendation sent to the Digital Services Coordinator of establishment, any additional information provided pursuant to paragraph 3 and the communication referred to in paragraph 4.</p> <p>6. The Commission shall assess the matter within three months following the referral of the matter pursuant to paragraph 5, after having consulted the Digital Services Coordinator of establishment and, unless it referred the matter itself, the Board.</p> <p>7. Where, pursuant to paragraph 6, the Commission concludes that the assessment or the investigatory or enforcement measures taken or envisaged pursuant to paragraph 4 are incompatible with this Regulation, it shall request the Digital Service Coordinator of establishment to further assess the matter and take the necessary investigatory or enforcement measures to ensure compliance with</p>	<p><i>requirement to act request</i>, or, where appropriate, the Board, did not receive a reply within the time period laid down in paragraph 4 or where it does not agree with the assessment of the Digital Services Coordinator of establishment, it may refer the matter to the Commission, providing all relevant information. That information shall include at least the request or recommendation sent to the Digital Services Coordinator of establishment, any additional information provided pursuant to paragraph 3 and the communication referred to in paragraph 4.</p> <p>6. The Commission shall assess the matter within three months following the referral of the matter pursuant to paragraph 5, after having consulted the Digital Services Coordinator of establishment and, unless it referred the matter itself, the Board.</p> <p>7. Where, pursuant to paragraph 6, the Commission concludes that the</p>	
---	--	--

<p>this Regulation, and to inform it about those measures taken within two months from that request.</p>	<p>enforcement measures taken or envisaged pursuant to paragraph 4 are incompatible with this Regulation, it shall request the Digital Service Coordinator of establishment to further assess the matter and take the necessary investigatory or enforcement measures to ensure compliance with this Regulation, and to inform it about those measures taken within two months from that request.</p>	
<p style="text-align: center;"><i>Article 50 Enhanced supervision for very large online platforms</i></p> <p>1. Where the Digital Services Coordinator of establishment adopts a decision finding that a provider of very large online platform has infringed any of the provisions of Section 4 of Chapter III, it shall make use of the enhanced supervision system laid down in this Article. It shall take utmost account of any opinion and recommendation of</p>	<p style="text-align: center;"><i>Article 50 Enhanced supervision for very large online platforms</i></p> <p>1. Where the Digital Services Coordinator of establishment adopts a decision finding that a provider of very large online platform has infringed any of the provisions of Section 4 of Chapter III, it shall make use of the enhanced supervision system laid down in this Article. It shall take utmost account of any opinion and recommendation of the</p>	<p><i>With respect to the right to recommend investigations of suspected infringements by VLOPs pursuant to Article 50(1), we believe the Board and DSCs of destination could be further empowered by substituting the terms " may recommend" for a more legally binding term, such as "shall require". We would welcome views from the other Member States on this particular issue.</i></p>

<p>the Commission and the Board pursuant to this Article.</p> <p>The Commission acting on its own initiative, or the Board acting on its own initiative or upon request of at least three Digital Services Coordinators of destination, may, where it has reasons to suspect that a provider of very large online platform infringed any of those provisions, recommend the Digital Services Coordinator of establishment to investigate the suspected infringement with a view to that Digital Services Coordinator adopting such a decision within a reasonable time period <u>within a time period predefined in the recommendation.</u></p> <p><u>Where other competent authorities in that Member State are empowered to establish the existence of an infringement and to ensure the enhanced supervision in respect of a given provider of a very large online platform, the Digital Services</u></p>	<p>Commission and the Board pursuant to this Article.</p> <p>The Commission acting on its own initiative, or the Board acting on its own initiative or upon request of at least three Digital Services Coordinators of destination, <i>may, ,shall,</i> where it has reasons to suspect that a provider of very large online platform infringed any of those provisions, <i>require recommend</i> the Digital Services Coordinator of establishment to investigate the suspected infringement with a view to that Digital Services Coordinator adopting such a decision within a reasonable time period <u>within a time period predefined in the recommendation.</u></p> <p><u>Where other competent authorities in that Member State are empowered to establish the existence of an infringement and to ensure the enhanced supervision in respect of a given provider of a very large online</u></p>	
--	---	--

<p><u>Coordinator of establishment shall involve them in accordance with the applicable national law.</u></p> <p>2. When communicating the decision referred to in the first subparagraph of paragraph 1 to the <u>provider of the</u> very large online platform concerned, the Digital Services Coordinator of establishment shall request it to draw up and communicate to the Digital Services Coordinator of establishment, the Commission and the Board, within one month from that decision, an action plan, specifying how that platform intends to terminate or remedy the infringement. The measures set out in the action plan may include, where appropriate, participation in a code of conduct as provided for in Article 35.</p> <p>3. Within one month following receipt of the action plan, the Board shall communicate its opinion on the action plan to the Digital Services Coordinator of establishment. Within one month following receipt of that opinion, that</p>	<p><u>platform, the Digital Services Coordinator of establishment shall involve them in accordance with the applicable national law.</u></p> <p>2. When communicating the decision referred to in the first subparagraph of paragraph 1 to the <u>provider of the</u> very large online platform concerned, the Digital Services Coordinator of establishment shall request it to draw up and communicate to the Digital Services Coordinator of establishment, the Commission and the Board, within one month from that decision, an action plan, specifying how that platform intends to terminate or remedy the infringement. The measures set out in the action plan may include, where appropriate, participation in a code of conduct as provided for in Article 35.</p> <p>3. Within one month following receipt of the action plan, the Board shall communicate its opinion on the action plan to the Digital Services</p>	
--	--	--

<p>Digital Services Coordinator shall decide whether the action plan is appropriate to terminate or remedy the infringement.</p> <p>Where the Digital Services Coordinator of establishment has concerns on the ability of the measures to terminate or remedy the infringement, it may request the very large online platform concerned to subject itself to an additional, independent audit to assess the effectiveness of those measures in terminating or remedying the infringement. In that case, that platform shall send the audit report to that Digital Services Coordinator, the Commission and the Board within four months from the decision referred to in the first subparagraph. When requesting such an additional audit, the Digital Services Coordinator may specify a particular audit organisation that is to carry out the audit, at the expense of the platform concerned, selected on the basis of criteria set out in Article 28(2).</p>	<p>Coordinator of establishment. Within one month following receipt of that opinion, that Digital Services Coordinator shall decide whether the action plan is appropriate to terminate or remedy the infringement.</p> <p>Where the Digital Services Coordinator of establishment has concerns on the ability of the measures to terminate or remedy the infringement, it may request the very large online platform concerned to subject itself to an additional, independent audit to assess the effectiveness of those measures in terminating or remedying the infringement. In that case, that platform shall send the audit report to that Digital Services Coordinator, the Commission and the Board within four months from the decision referred to in the first subparagraph. When requesting such an additional audit, the Digital Services Coordinator may specify a particular audit organisation</p>	
---	--	--

<p>4. The Digital Services Coordinator of establishment shall communicate to the Commission, the Board and the <u>provider of the</u> very large online platform concerned its views as to whether the <u>provider of</u> very large online platform has terminated or remedied the infringement and the reasons thereof. It shall do so within the following time periods, as applicable:</p> <p>(a) within one month from the receipt of the audit report referred to in the second subparagraph of paragraph 3, where such an audit was performed;</p> <p><u>(a) at the same time as the decision adopted pursuant to paragraph 3, where it does not consider the action plan appropriate to terminate or remedy the infringement;</u></p> <p>(b) within three months from the decision on the action plan</p>	<p>that is to carry out the audit, at the expense of the platform concerned, selected on the basis of criteria set out in Article 28(2).</p> <p>4. The Digital Services Coordinator of establishment shall communicate to the Commission, the Board and the <u>provider of the</u> very large online platform concerned its views as to whether the <u>provider of</u> very large online platform has terminated or remedied the infringement and the reasons thereof. It shall do so within the following time periods, as applicable:</p> <p>(a) within one month from the receipt of the audit report referred to in the second subparagraph of paragraph 3, where such an audit was performed;</p> <p><u>(a) at the same time as the decision adopted pursuant to paragraph 3, where it does not consider the action</u></p>	
---	---	--

<p>referred to in the first subparagraph of paragraph 3, <u>where the action plan was considered appropriate to terminate or remedy the infringement</u>, where no such audit was performed;</p> <p>(c) immediately upon the expiry of the time period set out in paragraph 2, where that platform failed to communicate the action plan within that time period.</p> <p>Pursuant to that communication, the Digital Services Coordinator of establishment shall no longer be entitled to take any investigatory or enforcement measures in respect of the relevant conduct by the very large online platform concerned, without prejudice to Article 66 or any other measures that it may take at the request of the Commission.</p>	<p><u>plan appropriate to terminate or remedy the infringement;</u></p> <p>(b) within three months from the decision on the action plan referred to in the first subparagraph of paragraph 3, <u>where the action plan was considered appropriate to terminate or remedy the infringement</u>, where no such audit was performed;</p> <p>(c) immediately upon the expiry of the time period set out in paragraph 2, where that platform failed to communicate the action plan within that time period.</p> <p>Pursuant to that communication, the Digital Services Coordinator of establishment shall no longer be entitled to take any investigatory or enforcement measures in respect of the relevant conduct by the very large online platform concerned,</p>	
---	--	--

	<p style="text-align: center;">without prejudice to Article 66 or any other measures that it may take at the request of the Commission.</p>	
<p style="text-align: center;"><i>Article 51</i> <i>Intervention by the Commission and opening of proceedings</i></p> <p>1. The Commission, acting either upon the Board’s recommendation or on its own initiative after consulting the Board, may initiate proceedings in view of the possible adoption of decisions pursuant to Articles 58 and 59 in respect of the relevant conduct by the provider of the very large online platform that:</p> <p>(a) is suspected of having infringed any of the provisions of this Regulation and the Digital Services Coordinator of establishment did not take the necessary any investigatory or enforcement measures, pursuant</p>	<p style="text-align: center;"><i>Article 51</i> <i>Intervention by the Commission and opening of proceedings</i></p> <p>1. The Commission, acting either upon the Board’s recommendation or on its own initiative after consulting the Board, shall may initiate proceedings in view of the possible adoption of decisions pursuant to Articles 58 and 59 in respect of the relevant conduct by the provider of the very large online platform that:</p> <p>(a) is suspected of having infringed any of the provisions of this Regulation and the Digital Services Coordinator of establishment did not take the necessary any investigatory or enforcement measures,</p>	<p><i>In line with earlier comments made with respect to Article 45 and enforcement, we would welcome strengthened competences for the DSCs and the Board.</i></p>

<p>to the request of the Commission referred to in Article 45(7), upon the expiry of the time period set in that request;</p> <p>(b) is suspected of having infringed any of the provisions of this Regulation and the Digital Services Coordinator of establishment requested the Commission to intervene in accordance with Article 46(2), upon the reception of that request;</p> <p>(c) has been found to have infringed any of the provisions of Section 4 of Chapter III, upon the expiry of the relevant time periods for the communication referred to in Article 50(4).</p> <p>2. Where the Commission decides to initiate proceedings pursuant to paragraph 1, it shall notify all Digital Services Coordinators, the Board and the provider of the very large online platform concerned.</p>	<p>pursuant to the request of the Commission referred to in Article 45(7), upon the expiry of the time period set in that request;</p> <p>(b) is suspected of having infringed any of the provisions of this Regulation and the Digital Services Coordinator of establishment requested the Commission to intervene in accordance with Article 46(2), upon the reception of that request;</p> <p>(c) has been found to have infringed any of the provisions of Section 4 of Chapter III, upon the expiry of the relevant time periods for the communication referred to in Article 50(4).</p> <p>2. Where the Commission decides to initiate proceedings pursuant to paragraph 1, it shall notify all Digital Services Coordinators, the Board and</p>	
---	---	--

<p>As regards points (a) and (b) of paragraph 1, pPursuant to that notification, the Digital Services Coordinator of establishment concerned shall no longer be entitled to take any investigatory or enforcement measures in respect of the relevant conduct by the provider of the very large online platform concerned, without prejudice to Article 66 or any other measures that it_z may take at the request of the Commission. <u>The Commission shall inform the Digital Services Coordinator of establishment of its preliminary findings pursuant to Article 63(1).</u></p> <p>3. The Digital Services Coordinator referred to in Articles 45(7), 46(2) and 50(1), as applicable, shall, without undue delay upon being informed, transmit to the Commission:</p> <p>(a) any information that that Digital Services Coordinator exchanged relating to the infringement or the suspected infringement, as applicable, with the Board and</p>	<p>the provider of the very large online platform concerned.</p> <p>As regards points (a) and (b) of paragraph 1, pPursuant to that notification, the Digital Services Coordinator of establishment concerned shall no longer be entitled to take any investigatory or enforcement measures in respect of the relevant conduct by the provider of the very large online platform concerned, without prejudice to Article 66 or any other measures that it_z may take at the request of the Commission. <u>The Commission shall inform the Digital Services Coordinator of establishment of its preliminary findings pursuant to Article 63(1).</u></p> <p>3. The Digital Services Coordinator referred to in Articles 45(7), 46(2) and 50(1), as applicable, shall, without undue delay upon being informed, transmit to the Commission:</p>	
--	--	--

<p>with the provider of the very large online platform concerned;</p> <p>(b) the case file of that Digital Services Coordinator relating to the infringement or the suspected infringement, as applicable;</p> <p>(c) any other information in the possession of that Digital Services Coordinator that may be relevant to the proceedings initiated by the Commission.</p> <p>4. The Board, and the Digital Services Coordinators making the request referred to in Article 45(1), shall, without undue delay upon being informed, transmit to the Commission any information in their possession that may be relevant to the proceedings initiated by the Commission.</p>	<p>(a) any information that that Digital Services Coordinator exchanged relating to the infringement or the suspected infringement, as applicable, with the Board and with the provider of the very large online platform concerned;</p> <p>(b) the case file of that Digital Services Coordinator relating to the infringement or the suspected infringement, as applicable;</p> <p>(c) any other information in the possession of that Digital Services Coordinator that may be relevant to the proceedings initiated by the Commission.</p> <p>4. The Board, and the Digital Services Coordinators making the request referred to in Article 45(1), shall, without undue delay upon being informed, transmit to the Commission any information in their possession that may be relevant to the</p>	
--	--	--

	proceedings initiated by the Commission.	
--	---	--