# DSA proposed Amendments
# On Art. 2, 17, 18, 21 and Recital 13

| Articles | Related Recitals | Suggested amendment language |
|---|---|---|
| **Chapter I – General provisions** | | |
| *Article 2 - Definitions* | (12) (13) (14) | Article 2(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~~ ***by virtue of its presence on an intermediary service*** is not in compliance with Union law or the law of a Member State ***that is consistent with Union law***, irrespective of the precise subject matter or nature of that law; |
| | | Recital 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 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~~ ***by virtue of its presence on an intermediary service*** is ~~either itself~~ illegal ***under applicable Union law or national law that is consistent with Union law***, 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, the non-authorised use of copyright protected material 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.~~ |
| | | *Justification: the Commission has explicitly stated that the DSA does not purport to define what illegal content is. This remains a matter for applicable national and EU law. Accordingly, there is a need to tighten the definition of illegal content by removing the "reference to an [illegal] activity," which could lead to excessive takedowns (e.g. would a video showing a car breaking the speed limit in Munich also qualify as illegal content?).* |
| | | Article 2(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~~ ***or*** purely ancillary feature ***or functionality*** of ***the principal*** ~~another~~ service ***offered*** and, for objective and technical reasons cannot be used without that ~~other~~ ***principal*** service, and the integration of the feature ***or*** |

| | | |
|---|---|---|
| | | ***functionality*** into the other service is not a means to circumvent the applicability of this Regulation. |
| | | Recital 13: … However, in order to avoid imposing overly broad obligations, providers of hosting services should not be considered as online platforms***, for the entirety or part of their service, on account of a feature or functionality that may allow*** ~~where the~~ dissemination to the public***, but*** is merely a minor ~~and~~ ***or*** purely ancillary feature ***or functionality*** of ***the principal*** ~~another~~ service ***offered,*** and that feature ***or functionality*** cannot, for objective technical reasons, be used without that ~~other,~~ principal service, and the integration of that feature ***or functionality*** is not a means to circumvent the applicability of the rules of this Regulation applicable to online platforms. For example, the comments section in an online newspaper ***or video-sharing service*** could constitute such a feature, where it is clear that it is ancillary to the main ***purpose*** ~~service~~ represented by the publication of news ***or the sharing of videos*** ~~under the editorial responsibility of the publisher~~. ***Similarly, a link-sharing option in a consumer cloud storage service may constitute such a functionality, where it is minor compared to the main purpose of the service to allow users to store personal content and share it within closed circles.*** |
| | | *Justification: the DSA provides that, where storing and publicly disseminating information is "a minor and purely ancillary feature", it may be exempted from the application of online platforms' due diligence obligations (but will still be subject to hosting services' due diligence obligations). Given the multifaceted and constantly evolving nature of online platforms and associated features and functionalities, some clarification that different features or functionalities within the same service may be subject to different sections of the DSA is needed.*<br>*Cloud services should be explicitly classified as "basic hosting" services, to avoid the risk that they may be inadvertently subject to the due diligence obligations for "online platforms." The main purpose of cloud services is not to disseminate information to the public, but rather to allow users to store personal content and share it within closed circles. For B2B services, customers of cloud service providers - and not cloud service providers themselves - have ownership and control over the content they put on the cloud.* |
| | | Recital (14): The concept of 'dissemination to the public', as used in this Regulation, should entail the making available of information to a potentially unlimited number of persons, that is, making the information easily ***discoverable by and*** accessible to users in general without further action by the recipient of the service providing the information being required, irrespective of whether those persons actually ***discover and*** access the information in question. The mere possibility to create groups of users of a given service should not, in itself, be understood to mean that the information disseminated in that manner is not disseminated to the public. However, the concept should exclude dissemination of information within closed groups consisting of a finite number of pre-determined persons. Interpersonal communication services, as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council, such as emails or private messaging services, fall outside the scope of this Regulation***, but may benefit from the exemptions from liability under Chapter II, to the extent that they qualify as 'mere conduit', 'caching' or 'hosting' services***. Information should be considered disseminated to the public within the meaning of this Regulation only where that occurs upon the direct request by the recipient of the service that provided the information. |

| | | |
|---|---|---|
| | | *Justification: clarifying the combined reading of Recitals 14 and 27, as regards the applicability of the DSA to interpersonal communication services.* |
| | | Article 2(p): 'content moderation' means the activities undertaken by providers of intermediary services aimed at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken ***to remove or disable access to*** ~~that affect the availability, visibility and accessibility of~~ that illegal content or that information~~, such as demotion, disabling of access to, or removal thereof~~, or ***to affect*** the recipients' ability to provide that information, such as the termination or suspension of a recipient's account; |
| | | Article 2(l): 'Digital Services Coordinator of establishment' means the Digital Services Coordinator of the Member State where the provider of an intermediary service ***has its main establishment*** ~~is established~~ or its legal representative resides or is established; |
| | | *Justification: the preservation of cornerstone principles of the Digital Single Market, including the prohibition on general monitoring or active fact-finding, will help protect freedom of expression and allow innovation to flourish.* |
| *Article 9 - Orders to provide information* | (30) (31) (32) (33) | Recital 30: Orders to act against illegal content or to provide information should be issued in compliance with Union law, in particular Regulation (EU) 2016/679 and the prohibition of general obligations to monitor information or to actively seek facts or circumstances indicating illegal activity laid down in this Regulation. The conditions and requirements laid down in this Regulation ~~which apply to orders to act against illegal content~~ are without prejudice to other Union acts providing for similar systems for acting against specific types of illegal content ***or providing information,*** such as ~~Regulation (EU) …/…. [proposed~~ Regulation ***2021/784 of the European Parliament and of the Council of 29 April 2021 on*** addressing the dissemination of terrorist content online~~],~~ ***Regulation (EU)[E-Evidence Regulation],*** or Regulation (EU) 2017/2394 ~~that confers specific powers to order the provision of information on Member State consumer law enforcement authorities, whilst the conditions and requirements that apply to orders to provide information are without prejudice to other Union acts providing for similar relevant rules for specific sectors~~. Those conditions and requirements should be without prejudice to retention and preservation rules under applicable national law, in conformity with Union law and confidentiality requests by law enforcement authorities related to the non-disclosure of information.<br><br>Recital 31: The territorial scope of such orders to act against illegal content should be clearly set out on the basis of the applicable Union or national law enabling the issuance of the order and should not exceed what is strictly necessary to achieve its objectives. In that regard, the national judicial or administrative authority issuing the order should balance the objective that the order seeks to achieve, in accordance with the legal basis enabling its issuance, with the rights and legitimate interests of all third parties that may be affected by the order, in particular their fundamental rights under the Charter. In addition, where the order referring to the specific information may have effects beyond the territory of the Member State of the authority concerned, the authority should assess whether the information at issue is likely to constitute illegal content |

| | | |
|---|---|---|
| | | in other Member States concerned and, where relevant, take account of the relevant rules of Union law or international law and the interests of international comity. ***Since intermediaries should not be required to remove information which is legal in their country of origin, Union authorities should be able to order the blocking of content legally published outside the Union only for the territory of the Union where Union law is infringed and for the territory of the issuing Member State where national law is infringed.***<br><br>Recital 32: The orders to provide information regulated by this Regulation concern the production of specific information about individual recipients of the intermediary service concerned who are identified in those orders for the purposes of determining compliance by the recipients of the services with applicable Union or national rules. Therefore, orders about ***data not deemed to be personal data as defined by Regulation EU 2016/679*** ~~information~~ ***related to*** ~~on~~ a group of recipients of the service who are not specifically identified, including orders to provide aggregate information required for statistical purposes or evidence-based policy-making, should remain unaffected by the rules of this Regulation on the provision of information.<br><br>Recital 33: Orders to act against illegal content and to provide information are subject to the rules safeguarding the competence of the Member State where the service provider addressed is established and laying down possible derogations from that competence in certain cases, set out in Article 3 of Directive 2000/31/EC, only if the conditions of that Article are met. Given that the orders ***to provide information*** ~~in question~~ relate to specific items of ~~illegal content and~~ information~~, respectively,~~ where they are addressed to providers of intermediary services established in another Member State, they ***may*** ~~do~~ not in principle restrict those providers' freedom to provide their services across borders. ***However*** ~~Therefore~~, the rules set out in Article 3 of Directive 2000/31/EC, including those regarding the need to justify measures derogating from the competence of the Member State where the service provider is established on certain specified grounds and regarding the notification of such measures, ***continue to*** ~~do not~~ apply in respect of those orders.<br><br>Article 9<br>1. Providers of intermediary services shall, upon receipt ***of an order served via a secure communications channel*** to provide a specific item of information about one or more specific individual recipients of the service, issued by ***a*** ~~the relevant~~ national judicial ~~or administrative authorities~~ ***authority*** on the basis of the applicable Union or national law, in conformity with Union law, ***for the purpose of preventing serious threats to public security,*** inform without undue delay the authority of issuing the order of ~~its receipt and~~ the effect given to the order ***via a secure communications channel***.<br><br>***1a. Paragraph 1 shall not apply to an order or request related to a criminal offence which should be made in accordance with Regulation (EU) [E-Evidence], or a judicial order related to civil or commercial matters which should be made in accordance with Regulations 1215/2012 and 1393/2007.***<br><br>2. Member States shall ensure that orders referred to in paragraph 1 meet the following conditions:<br>***(a) the order is issued for the purpose of preventing serious threats to public security;*** |

| | | |
|---|---|---|
| | | ***(aa) the order seeks information on a suspect or suspects of a serious threat to public security;***<br>***(aaa)*** the order contains the following elements:<br>- 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 taking due account of the impact of the measure on the fundamental rights of the specific recipient of the service whose data is sought and the seriousness of the offence, unless such a statement cannot be provided for reasons related to the prevention, investigation, detection and prosecution of criminal offences*** ~~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, detection and prosecution of criminal offences~~;<br>- information about redress available to the provider and to the recipients of the service concerned;<br>- ***the applicable provisions of the law of the issuing Member State;***<br>- ***the exact purpose(s) for which the information is sought;***<br>- ***a unique identifier to allow the service provider to identify the user whose data is sought, such as email address, phone number, IMEI;***<br>- ***the data category sought (subscriber data, traffic data or content data) and an explanation as to why the data is necessary and proportionate for the purpose for which it is sought;***<br>- ***the time and/or data range within which the data requested was created, tailored as narrowly as possible.***<br>(b) the order ***may*** only require~~s~~ the provider to provide information already ***legally*** collected for the purposes of providing the service and which lies within its control ***and can be reasonably identified and obtained by the provider;***<br>(c) the order ***must be*** ~~is~~ drafted in the language declared by the provider and ***should be*** ~~is~~ sent to the point of contact appointed by that provider ***for the purpose of receiving requests made pursuant to Article 9***~~, in accordance with Article 10~~.<br><br>3. The Digital 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.<br><br>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.~~<br><br>***4. The provider may inform, without undue delay, the recipient whose data is being sought. As long as this is necessary and proportionate and is in order to protect the fundamental rights of another person, the issuing judicial authority, taking due account of the impact of the measure on the fundamental rights of the person whose data is sought, may request the provider to delay informing the recipient. Such a request shall be duly justified, specify the duration of the obligation of confidentiality and be subject to periodic review.*** |

| | | |
|---|---|---|
| | | ***5. Providers of intermediary services shall transfer personal data on recipients of their service requested by public authorities only where the conditions set out in this Article are met.***<br><br>***6. The conditions and requirements laid down in this article shall be without prejudice to requirements under Union law, including but not limited to Regulation (EU) [E-Evidence] which sets out the requirements for cross border requests for information in criminal proceedings and Regulations 1215/2012 and 1393/2007 which set out the requirements for judicial orders related to civil or commercial matters.***<br><br>***7. The Commission shall adopt implementing acts pursuant to Article 291 of the Treaty on the Functioning of the European Union (TFEU), establishing a common European information exchange system with secure channels for the handling of authorised cross-border communications, authentication and transmission of the orders referred to in paragraph 1 and, where applicable, of the requested data between the competent judicial authority and the provider. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 70, and in consultation and agreement with the providers of intermediary services.***<br><br>***8. In cases where the information sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, the order or request should only be addressed to the provider of the intermediary services when other investigative measures directly addressed to the company or entity are not appropriate.*** |
| | | |

| ***Section 3 - Additional provisions applicable to online platforms*** | | |
|---|---|---|
| *Article 17 - Internal complaint-handling system* | (44) (45) | Article 17(1): Online platforms shall provide recipients of the service, for a period of at least ~~six months~~ ***one month*** 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 following decisions taken by the online platform on the ground that the information provided by the recipients is illegal content or incompatible with its terms and conditions:<br>(a) decisions to remove or disable access to the information;<br>(b) decisions to suspend or terminate the provision of the service, in whole or in part, to the recipients;<br>(c) decisions to suspend or terminate the recipients' account. |
| | | *Justification: providing an internal complaint-handling system for 6 months following the content moderation decision is disproportionate and undermines legal certainty and fundamental rights. For example, a rightsholder would have to wait for 6 months in uncertainty to confirm whether a decision to remove IP infringing content is final or may be appealed by the uploader.* |

| | | |
|---|---|---|
| | | Article 17(5): ~~Online platforms shall ensure that the decisions, referred to in paragraph 4, are not solely taken on the basis of automated means.~~<br><br>*Justification: the text is too rigid in requiring that no decision on appeal should be taken solely on the basis of automated means.*<br>*This is not reasonable given the scale at which content moderation takes place. Automation is routinely used to handle the billions of spam or bad ads content, we need to ensure that the DSA does not risk our ability to handle scaled abuse.*<br>*A more appropriate outcome would be a risk-based approach to appeals, using a combination of human review and automation: for more egregious and nuanced cases online platforms may indeed need to more heavily rely on expert human review.* |
| *Article 18 - Out-of-court dispute settlement* | | ***1. Providers of online platform services shall identify in their terms and conditions two or more out-of-court dispute settlement bodies that have been certified in accordance with paragraph 2 and with which they are willing to engage to attempt to reach an agreement with recipients of the service on the settlement, out-of-court, of any disputes between the provider and the recipient of the service arising in relation to decisions to terminate the provision of the service to that recipient or terminate that recipient's account, with the exception of such decisions made on spam grounds, provided that the recipients of the service affected by those decisions:***<br><br>***(a) are not traders within the meaning of Article 2(e) of this Regulation;***<br>***(b) prior to having recourse to the out-of court dispute settlement body, have exhausted the appeal possibilities offered to them by the internal complaint-handling system referred to in Article 17 and provided evidence that they have done so;***<br>***(c) submit a request for recourse to out-of-court dispute settlement within two weeks from the decision reached through the internal complaint-handling system.***<br><br>***Providers of online platform services may only identify out-of-court dispute settlement bodies providing their services from a location outside the Union where it is ensured that the recipients of the service concerned are not effectively deprived of the benefit of any legal safeguards laid down in Union law or the law of the Member States as a consequence of the out-of-court dispute settlement bodies providing those services from outside the Union.***<br><br>***2. The Digital Services Coordinator of the Member State where the out-of-court dispute settlement body is established shall, at the request of that body, certify the body, where the body has demonstrated that it meets all of the following conditions:***<br><br>***(a) it is impartial and independent;*** |

| | | |
|---|---|---|
| | | ***(b) it has the necessary expertise in relation to the issues arising in one or more particular areas of illegal content, or in relation to the application and enforcement of terms and conditions of one or more types of online platforms, allowing it to contribute effectively to the attempt to settle the disputes;***<br>***(c) it offers dispute settlement that is easily accessible through electronic communication technology;***<br>***(d) it is capable of settling disputes in a swift, efficient and cost-effective manner and in at least one official language of the Union;***<br>***(e) it has in place clear and fair rules of procedure, including strict confidentiality safeguards.***<br><br>***3. Notwithstanding the voluntary nature of this out-of-court dispute settlement provision, providers of online platform services and recipients of the service concerned shall engage in good faith throughout any out-of-court dispute settlement attempts conducted pursuant to, and in accordance with, this Article.***<br><br>***4. Providers of online platform services and recipients of the service concerned shall each bear a reasonable proportion of the total costs of out-of-court dispute settlement in each individual case. A reasonable proportion of those total costs shall be determined, on the basis of a suggestion by the out-of-court dispute settlement body, by taking into account all relevant elements of the case at hand, in particular the relative merits of the claims of the parties to the dispute, the conduct of the parties, as well as the size and financial strength of the parties relative to one another.***<br><br>***5. Any attempt to reach an out-of-court agreement on the settlement of a dispute in accordance with this Article shall not affect the rights of the providers of online platform services and of the recipients of the service concerned to initiate judicial proceedings at any time before, during or after the out-of-court dispute settlement process.*** |
| | | *Justification: in order to avoid several potential unintended consequences, it is more appropriate for the regulator to oversee, at a systemic level, internal complaints processes, and for enough flexibility to be allowed as to how online platforms ensure users have recourse to meaningful redress options. A more balanced approach to Article 18 should be pursued, in line with the approach adopted in the Platform-to-Business Regulation.* |
| *Article 21 - Notification of suspicions of criminal offences* | (48) | Article 21(1): Where an online platform becomes aware of ~~any information giving rise to a suspicion that a serious criminal offence involving a~~ ***content involving an imminent*** threat to ~~the~~ life ~~or safety of persons has taken place, is taking place or is likely to take place~~, it shall ~~promptly~~ inform ***authorities competent for the investigation and prosecution in criminal offences in the concerned Member State(s).***~~the law enforcement or judicial authorities of the Member State or Member States concerned. of its suspicion and provide all relevant information available~~. |
| | | Article 21(2): Where the online platform cannot identify with reasonable certainty the Member State concerned, it shall inform the law enforcement authorities of the Member State in which it ***has its main establishment*** ~~is established~~ or has its legal representative ~~or~~ ***and also transmit this information to Europol for appropriate follow up***~~inform Europol~~. |

| | | |
|---|---|---|
| | | For the purpose of this Article, the Member State concerned shall be the Member State where ***the threat to life is imminent.*** ~~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.'~~ |
| | | Recital (48): An online platform may in some instances become aware, such as through a notice by a notifying party or through its own voluntary measures, of ***content involving an imminent threat to life*** ~~information relating to certain activity of a recipient of the service, such as the provision of certain types of illegal content, that reasonably justify, having regard to all relevant circumstances of which the online platform is aware, the suspicion that the recipient may have committed, may be committing or is likely to commit a serious criminal offence involving a threat to the life or safety of person, such as offences specified in Directive 2011/93/EU of the European Parliament and of the Council~~. In such instances, the online platform should inform without delay the ~~competent law enforcement~~ ***relevant competent*** authorities ~~of such suspicion~~, providing all relevant information available to it~~; including where relevant the content in question and an explanation of its suspicion~~. This Regulation does not provide the legal basis for profiling of recipients of the services with a view to the possible identification of criminal offences by online platforms. Online platforms should also respect other applicable rules of Union or national law for the protection of the rights and freedoms of individuals when informing ~~law enforcement~~ authorities. |
| | | *Justification: the requirement for a service to notify authorities where it "becomes aware of any information giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place" would improperly shift the function of law enforcement investigation from government to private actors.*<br>*This Article should be aligned with the language used and safeguards included in the Terrorist Content Online Regulation. This would ensure the DSA reflects Europe's strong tradition of protecting privacy as a fundamental right.* |