Position paper

Proposal for a Regulation on a Single Market for Digital Services and amending Directive 2000/31/EC

26 March 2021

Summary

Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) ('eCommerce Directive' – 'eCD') was adopted on 8 June 2000. Since then, the significance of information society services for European societies and economies has increased massively, leading to new policy challenges. Moreover, many instances of the need for accountable information society services have been manifested in the legal, societal and economic spheres in the framework of specific individual cases. On 15 December 2020, the European Commission published a proposal for a Regulation on a Single Market for Digital Services ('Digital Services Act' – 'DSA'), which would amend Directive 2000/31/EC. Building on the key principles set out in the eCD, which remain valid today, this proposal seeks to ensure the best conditions for the provision of innovative digital services in the internal market, to contribute to online safety and the protection of fundamental rights, and to set a robust and durable governance structure for the effective supervision of providers of intermediary services.

Bitkom supports the ambition of the Digital Services Act to strengthen the digital market in the EU. The planned reform is an opportunity to establish a clear, horizontal, uniform and up-to-date, innovation-friendly legislative framework for providers of digital services. We aim for a legal framework that allows service providers to tackle the task of keeping the internet safe and play their parts in creating a healthier online environment. In addition, it is important to ensure the necessary cooperation between the Member States as well as adequate supervision of suppliers of digital services in the EU. Services which are active on the European market must comply with the legal provisions applicable in the EU. To this end, it is of decisive importance that all relevant players work together in order to secure a functioning digital single market and adequate protection for consumers and users: Online intermediaries, rights holders, users, governments and law enforcement all have their role to act responsibly and improve safety and trust in the Internet economy.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Marie Anne Nietan

P +49 30 27576-221
m.nietan@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Bitkom would like to take the opportunity to comment on the framework proposed, highlighting our most urgent open questions and concerns. While this paper summarizes our initial evaluation of the four chapters of the proposal, we would be looking forward to also commenting on further issues and in more depth in the course of the legislative process.

Chapter 1: General Provisions

The **distinction between mere hosting providers and online platforms** according to the proposed **definitions** needs to be further clarified. The draft definition in **Article 2 (h)** proposes 'dissemination of information to the public' as the criterion to distinguish online platforms from mere hosting providers. 'Dissemination to the public', in turn, is defined in Article 2 (i) as 'making information available [...] to a potentially unlimited number of third parties'. In general, Bitkom supports taking the functionalities and technical architecture of services into account when defining their obligations. Using the criterion 'dissemination of information to the public' in order to distinguish between mere hosting providers and online platforms is reasonable, justified, and well-tailored. It is important for the protection of the overwhelming majority of law-abiding users to see their privacy secured when sharing material on a (cloud) service, which is explicitly designed not to be accessible to the public. This right to privacy and data protection must be carefully balanced against the danger of dissemination of illegal content online.

Cloud services which are not effectively designed and intended to be used for the dissemination of content to the public should only be classified as hosting services to avoid the risk of them inadvertently being subject to the due diligence requirements for online platforms. Particularly in case of business-to-business cloud services, it is the customer of the cloud service provider - and not the cloud service provider itself – who not only owns but controls the content stored. The moderation of content in the cloud may be de facto impossible for the service provider due to a lack of technical capabilities to identify and remove individual pieces of content or for privacy and contractual reasons. The primary purpose of cloud services is not to disseminate information to the public, but rather to allow users to store and share personal or professional content stored and shared in closed groups. In addition, many cloud service providers already implement strong safeguards to prevent fraudulent businesses from using their services (e.g., contractual obligations in service contracts, security-based services against fraud).

As a consequence, any obligation to remove or disable access to illegal content should first be put on the customer or end-user who has made available the content. Services deeper in the internet stack acting as online intermediaries should be required to take proportionate actions where the customer or a service provider closer to the customer fails to remove the illegal content, unless implementation of the required action is technically impracticable.

The DSA should take this complexity into account and – as already reflected upon to some extent by recital 26 last sentence and recital 27 first two sentences - not subject cloud services to the strict due diligence requirements that apply to online platforms. Such an approach is in line with the definition in Article 2 (h), which states that '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'. It should, however, be clarified that this also applies to ancillary features of cloud services themselves and not to only 'another service' – otherwise cloud services that don't have as their main feature the dissemination to the public nevertheless risk to be qualified as online platforms. Only if cloud services are effectively designed and intended to be used for the dissemination of content to the public, comparable to an online platform, the additional requirements for online platforms should apply.

To ensure coherence with the Audiovisual Media Services Directive, the definition of 'online platform' should not cover services which aggregate services for which editorial control is present and which are subject to regulatory scrutiny, such as non-linear audiovisual services.

Chapter 2: Liability of providers of intermediary services

Bitkom welcomes that the European Commission acknowledges and reinforces in Article 3, 4, 5 and 7 of its draft proposal the **general principles of the eCommerce Directive** – the **graduated liability framework** as well as the **ban on general monitoring obligations**. Those principles are the fundamental building blocks for the protection of fundamental rights online, including the freedom of expression and information, and have been decisive in enabling the development of the thriving European digital single market.

Open questions remain regarding **Article 5 (3)**, which proposes an exception from the liability protection with regard to consumer protection law. We believe that this provision would benefit from additional language clarifying that it does not amount to a new regulation but rather echoes the status-quo under the existing eCommerce Directive. In addition, it should be clarified that online platforms which forward customers to a third-party website to conclude the contract there are not within the scope of this exception from the liability protection.

We welcome the introduction of the **Good Samaritan principle in Article 6**, which clarifies that voluntary own-initiative investigations do not, in and by themselves, prevent service providers from benefitting from the liability exemptions. Providers of online platforms should be encouraged to take proactive voluntary measures to detect and eventually remove illegal and potentially harmful content from their platforms – and not deterred from doing so, reflecting the current legal framework.

Having said that, any provision on voluntary measures should be very clearly defined as to its scope and limits. Under the proposed wording, the scope of the protection offered to online intermediaries by Article 6 remains unclear. Article 6 would benefit from further clarity by reference to acquiring 'actual knowledge' under Article 5. Further, the catch-all provision under 'requirements of Union law' is vague, unclear and unnecessarily broad. Finally, it should be clarified that such voluntary activities and actions can be pursued by automated or non-automated means.

We welcome the steps taken in **Article 8 and 9** of the proposal to clarify how **authorities** can indicate illegal content to and request information from platforms. However, further clarifications are needed. Firstly, the relationship between such orders and notice and action requests according to Article 14 should be further elaborated upon. In our view it would not be acceptable that by choosing between those two measures authorities can de facto decide whether legal safeguards apply, e.g. whether platforms will have instruments at their disposal to challenge the notice/order or not. Procedural rules should be inserted to clarify how providers can challenge orders that lack a proper legal basis, have been issued neglecting procedural safeguards, are unsubstantiated, unsuited, unjustified or disproportionate. Providers need clear and effective means to do so without having recourse to lengthy and costly court proceedings.

Secondly, it is important that any future legal and regulatory regime in this area does not undermine the country of origin principle - which remains a key pillar to the functioning of the EU internal market - or lead to fragmented enforcement with competing and contradictory outcomes. Article 8 and 9 (and 14) should therefore be aligned with Article 3 of the eCommerce Directive, according to which 'Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State' and, if they wish to do so, first need to consult with the Member State of establishment as well as the Commission. The same procedure needs to apply with regard to orders under the DSA. Due to prevailing cultural differences and different legal approaches among Member States when it comes to defining certain kinds of illegal content, such as hate speech, orders in some instances must be regarded as problematic.

Thirdly, it should be clarified whether orders under Article 8 refer to such requests as mentioned in Article 5 (4) by courts or administrative authorities to service providers instructing the latter to terminate or prevent an infringement.

If the DSA foresees cross-border information provision orders, Article 9 should be aligned with the e-Evidence Regulation. There should be a single decision on orders to provide information by the lead authority of the service providers' Member State of main establishment.

Chapter 3: Due diligence obligations

The DSA addresses a broad range of service providers from different sectors as well as different types of content. We welcome the idea of a **horizontal regulatory approach** covering all information society services and the preservation of the fundamental principles of the eCommerce Directive for all of these services. However, a differentiated approach in the structuring of service providers' obligations is needed which takes into account the specific platform and content types. There needs to be more flexibility with regard to measures service providers can use in order to comply with the new legislation. Many of the obligations in this proposal are very detailed, and non-observance is punishable by fines. Due to the broad variety of business models and types of content disseminated we suggest, generally speaking, to reduce the degree of detail within the individual obligations and take the differences between platforms and content into account when it comes to enforcement of these rules.

Provisions applicable to hosting service providers:

We welcome the introduction of EU-wide standards for **notice and action mechanisms in Article 14**. For all legal remedies and anti-abuse mechanisms, information is decisive for identification, although any standard must be technologically neutral and future proof. The more specific the conditions for a communication, the better, more seamless and rapid the processing operation and reaction. For the sake of legal clarity, the provisions on how to deal with (repeated) abusive communications that can be found in Article 20 (2) and (3) of the draft should be placed under Article 14.

The current wording of Article 14 (3) suggests that a platform will be deemed to have actual knowledge or awareness with regard to Article 5 once the elements mentioned in Article 14 (2) are fulfilled. Here, it should be clarified that notices only give rise to awareness but not necessarily to knowledge of the illegality of the content. Article 5 ensures there is no instant liability - however, awareness means the platform must process and take a

decision in respect to the information to which the notice relates, as pointed out in Article 14 (6). In some instances, the illegality of an information is obvious, or the platform obtains additional certainty due to the notice coming from a trusted partner. In other instances, however, depending on the nature of the intermediary and of the illegal content, it may be difficult for the intermediary to determine whether content is illegal and, therefore, the provider cannot be understood to have actual knowledge of an illegality simply as the result of the notice. This needs to be taken into account and a balance struck between ensuring clearly illegal content is dealt with responsibly and swiftly whilst platforms continue to receive the benefits of the liability protection (Art. 5) in respect to content which is not so easy to assess for illegality. Accordingly, the wording of Article 14 (3) should be clarified to reflect this. In unclear cases, the platform should nonetheless be authorized to take action to prevent the incriminated content to continue to be accessible until further clarification.

Article 14 (2) (b) requires a notice to give a 'clear indication of the electronic location of the information', but then specifies that this requires 'in particular the exact URL or URLs'. This requirement is technologically too specific, as it is oriented towards websites only and thus not future proof, as we already see illegal content or products being offered in other technical ways, such as apps, where locations are not defined by URLs. Instead, Art. 14 should use the same terminology as in Art. 8, which requires notices (in this case by authorities) to provide 'one or more exact uniform resource locators'. Alternatively, 'in particular the exact URL or URLs' could be replaced by 'such as the exact URL or URLs'.

After taking down illegal products, some E-Commerce platforms already voluntarily notify customers of unsafe products sold to them by third party sellers based on information from manufacturers, market surveillance authorities or public recall websites. While such practices do not necessarily work in all circumstances and across all platforms, they could be seen as a way forward with respect to the online sale of unsafe illicit products.

The obligation in **Article 15** to disclose 'the facts and circumstances relied on in taking the decision' within a provider's **statements of reasons** in certain instances raises concerns with regard to the protection of users. In the context of decisions on taking down content such as hate speech, terrorist content or child sexual abuse material (CSAM) it would be problematic to let the uploader of such content know exactly which facts and circumstances were relied on when taking the decision, such as notices received by other users/organizations. Giving too detailed statements of reasons could lead to these bad actors gaming the services' content moderation systems or getting to know who reported their content.

bitkom

Additional provisions applicable to online platforms

While we believe that functioning appeal systems are important, the DSA should help ensure that services are able to devise and implement such systems responsibly and with all equities in mind. **Article 17** on the **internal complaint-handling system** needs to contain additional safeguards to ensure that notifiers' information is protected during the complaint handling process, so identities are not revealed to users who upload, for example, terrorist or CSAM content. Inflexible requirements around complaint handling could also imperil investigations in case a user is notified about removal, for example, if law enforcement has sought removal of CSAM content.

The scope of the **Out-of-Court dispute settlement** proposed in **Article 18** is too broad. It should be reviewed in light of the proportionality principle, limited to decisions taken with regard to illegal content and aligned with the Platform to Business and Consumer Redress Regulation as well as the Audiovisual Media Services and Copyright Directive. In its current form, Article 18 could be abused by bad actors to arbitrate every content removal across EU Member States at a company's expense. Platforms remove billions of pieces of content from bad actors trying to spam, trick, or defraud users. Enabling bad actors to access out-of-court dispute settlement processes could slow down the process for legitimate seekers of redress. Therefore, Article 18 should offer exceptions for content like spam. In addition, we propose adopting the language of the platform to business regulation, which requires platforms to consider any request for mediation in good faith. This scheme would allow platforms to reject out-of-court dispute settlement in obviously abusive cases while in case of doubt they would need to explain why they did so.

The system proposed in Article 18 further does not strike a fair balance between online platforms and recipients of the service. The former shall be bound by the decision of the dispute settlement body while the latter can still seek judicial redress against the decision. The same option should be available for online platforms – therefore, the decision cannot be ultimately binding on either party. It should further be clarified that in case of decisions taken following orders from authorities or courts no dispute settlement involving the online platform is available. Finally, it should be clarified that recipients of the service first need to exhaust the platform's internal complaint handling system.

Because **trusted flaggers** are envisaged in **Article 19** to receive preferential treatment over notices from other users, it is vital to ensure that trusted flaggers are indeed entities whose notices are especially helpful for the platform concerned, in line with current practices. Granting Digital Services Coordinators the power to solely appoint trusted flaggers is not appropriate - the platform should also be involved in awarding that status. Moreover, the obligation to grant preferential treatment to notices of trusted flaggers should not be absolute – there might be situations in which the platform needs to give priority to other, very urgent notices. In order to ensure that any abuse of the trusted flaggers system can

be swiftly addressed, Article 19 (6) should specify that Digital Services Coordinators deal with complaints on trusted flaggers in a timely manner.

Cooperation with trusted flaggers, which should include 'trusted corporates', e.g. brand owners that have legal departments in place responsible for checking for, and taking actions with respect to, intellectual property infringements should be encouraged. The existing voluntary cooperation mechanisms between platforms and rights holder work well in many instances and should not be compromised by the new system under the DSA. Platforms should continue to be able to appoint individual companies as trusted corporates under their cooperation mechanisms in order to eliminate infringements of intellectual property.

The proposed **measures against misuse** in **Article 20** are too detailed and should leave more scope for flexibility for providers of online platforms. They should be allowed to take proportionate but effective measures to prevent repeated upload of illegal content depending on the type of content and severity of the infringement. Providers might warrant a permanent suspension (e.g. after a judicial decision), a temporary suspension until the recipient commits to stop uploading illegal content or dispense from the requirement of a prior warning.

It should be clarified that providers of online platforms cannot be held liable for any failure to act on a notice submitted during suspension of the submitter. Whether online platforms suspend the processing of notices and complaints should rest within their discretion and not be made obligatory. The platform should also be free to remove identical or equivalent content and close other accounts the seller might manage as well as prevent him/her from opening new accounts. Coherence should be ensured with the obligations of the Platform to Business Regulation with regard to restriction, suspension and termination of intermediation services to business users. Moreover, measures to disincentivize unfounded and abusive notices should be integrated.

We recognize the desire for greater transparency and **traceability of traders** on platforms and support the Commission's approach. Traceability of traders is an important tool for platforms to prevent misuse of their services, to dis-incentivise bad actors online and to provide a safe and trusted environment for their customers. To make the proposed regulation in **Article 22** more specific, we would recommend to refer to the specifications on the 'Know Your Business Customer' principle in the own-initiative report of the committee on the internal market and consumer protection preceding the publication of the Commission's proposal on the Digital Services Act. It specifies that this obligation should be 'limited to the direct commercial relationships' of the platform. The traceability of traders system in the DSA should furthermore be coherent with similar systems in other areas in which such (legal) obligations already exist, such as money laundering, in order to prevent double regulation.

The requirement in Article 22 (1) (d) for the platform to obtain information on the economic operator, which relates to the individual product and not to the trader, may be unrealistic. At the moment of account creation by the trader, not all economic operators will be known as these can differ for every product in a trader's catalogue which itself will change over time. In addition, we would like to receive clarification on the intended purpose behind the requirement in Article 22 (1) (f) for the platform to obtain a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law.

With regard to the requirement in Article 22 (2) to make reasonable efforts to assess the reliability of the information provided by traders, it should be defined what 'reasonable efforts' amount to and coherence ensured with the obligations in the Consumer Omnibus Directive. Over time, it should be the traders' obligation to update their information as it changes. Online platforms should remain free to remove products or suspend sellers as soon as it becomes evident that the information given are false. Doing so will give the necessary leverage to ensure compliance by sellers, while ensuring that no inaccurate or incomplete information remains online.

In order to ensure effective removal of illegal content, we suggest an amendment to Article 22(5) to clarify that the contact details and the identity of the trader should also be provided to law enforcement authorities and rights holders to allow them to pursue legal action. Where the online platform has been notified of action against a trader, they shall be obliged to maintain the information obtained pursuant to Art 22(4) until resolution of the action, and should not delete the information on expiry of their contractual relationship with the trader.

Under the **transparency reporting obligations for providers of online platforms** in **Article 23**, we would recommend that dispute-settlement bodies publish information on their procedures according to Article 23 (1) (a) rather than platforms since they have this information available anyways and are best placed to present them. In addition, it is not comprehensible why platforms should be obliged to publish information on the average monthly active recipients of the service in each Member State according to Article 23 (2). Such information can be detrimental to competition in the single market and is not helpful for the average user to obtain. Instead, such information should only be made available to competent authorities/ the Digital Services coordinator responsible on request. Moreover, any transparency obligation should comprise protective measures against passing on business secrets. The templates concerning form, content and other details of reports the Commission may lay down according to Article 23 (4) would most likely be too rigid to take into account the different business models of online platforms. Providers should be granted flexibility in portraying their efforts in tackling illegal content.

The proposed rules on **online advertising transparency** in **Article 24** should not be applicable to marketplaces as we don't see the benefit for consumers to receive such information for standard advertisement displayed there. The rules also seem to lead to an unequal playing field with offline advertising for which the provision of such information is not required. It would be more appropriate to require online platforms to include general information on advertising practices in their terms and conditions instead of requiring the information for each piece of advertisement.

Additional obligations for very large online platforms

Linking regulation to **threshold values** such as user volume, as suggested by the proposal for very large online platforms (VLOPs) in **Article 25**, broadly reflects a notion of proportionality – the idea that services with a high user volume and reach have a greater societal and economic relevance and thereby responsibility. Even if this notion of proportionality is correct and reach remains the decisive factor, it may be inappropriate or ineffective to link regulation only to specific threshold values.

When it comes to determining which platforms should take additional measures to prevent the dissemination of illegal content, additional qualitative risk-based factors should also be considered. The provider with most monthly users might not necessarily be the one most likely to disseminate illegal content. Therefore, we propose a mechanism which allows platforms exceeding the threshold to be qualified as a very large online platform to appeal to the award of that status by laying out why - despite their reach - the assumed risks with regard to dissemination of illegal content are not present.

In the threshold set by the Commission proposal it is furthermore unclear how 'active recipients' can be defined.

The obligations around **risk assessment and mitigation** as they are formulated now in **Article 26 and 27** as well as powers granted to the Commission with regard to **codes of conduct** in **Article 35** of the proposal could lead to a regulation of legal content through the back-door. According to recital 68, 'possible negative impacts of systemic risks on society and democracy, such as disinformation or manipulative and abusive activities' is an area in which codes of conduct should be considered. The recital further states that 'adherence to and compliance with a given code of conduct by a very large online platform may be considered as an appropriate risk mitigating measure. The refusal without proper explanations by an online platform of the Commission's invitation to participate in the application of such a code of conduct could be taken into account, where relevant, when determining whether the online platform has infringed the obligations laid down by this Regulation'. This could render codes of conduct on harmful but legal content effectively binding on very large online platforms, which runs counter the Commission's stated intent to protect

lawful content and limit the DSA obligations to illegal content. In the explanatory memorandum to the DSA, the Commission states that lawful but harmful content 'should not be subject to removal obligations, as this is a delicate area with severe implications for the protection of freedom of expression'. The provisions mentioned, however, risk doing just that. While we do see the importance of tackling harmful but legal content such as disinformation and welcome the Commission's activities in this area, also within codes of conduct, we do think these issues should be treated separately and not introduced to the DSA through the back-door of quasi-binding codes of conduct rather than through democratic processes.

According to **Article 28**, very large online platforms should be subject to regular **independent audits**. We recognize the importance of reviewing the risk assessments and risk mitigation measures of very large online platforms by independent experts to provide regulators with meaningful insights into how VLOPs are attempting to meet DSA obligations. However, we would propose to conduct regular audits only every second year in order to have meaningful time frames for audit activities. In addition, platforms should be given reasonable time to create an audit implementation report - the deadline of one month is too short, as some recommendations may require significant technical changes that need time for adequate planning.

Chapter 4: Implementation, cooperation, sanctions and enforcement

Improving **legal enforcement** is a central concern. We welcome that the Commission aims to strengthen cooperation between national supervisory authorities to ensure consistent enforcement of rules across the EU. However, there remains some uncertainty with regard to the appointment and powers of the **Digital Services Coordinator**/national competent authorities versus the **European Commission**'s role and the role of the **Board**. More clarity in this area would be welcomed. Given the fundamental role to be played by the Digital Services Coordinators in ensuring the consistent application of the DSA, it is essential that they have sufficient knowledge of the range of platform services covered by the Regulation. We have some concern with regard to the oversight and enforcement role granted to the European Commission. The powers seem disproportionate and there is a lack of safeguards to better frame this power. We would therefore recommend focussing more on the due process and other safeguards around competent authorities exercising their powers.

Bitkom welcomes that the Commission maintains the attribution of **Jurisdiction** according to the **country of origin principle** in **Article 40**. This principle constitutes a basic condition for providers' free choice of place of establishment and the free movement of digital services in the EU digital single market. For this reason, coherence needs to be ensured with the provisions on jurisdiction in the eCommerce Directive and possibly also the

Audiovisual Media Services Directive. In order to strengthen the country of origin principle, the DSA should clarify that any derogations from the country of origin principle within the coordinated area must be exceptional, on a case-by-case basis only, clearly aligned with EU legal frameworks and that there must be a clear process for notifying the Commission and respective Member States of establishment. Additionally, we would propose introducing an enforcement process in order to deal with impermissible derogations by Member States.

Due to prevailing differences between Member States' understanding and therefore continued lack of a common definition of what constitutes illegal content, full harmonization of actions against such content will mostly likely not be achieved by the DSA. This, however, makes the country of origin principle even more important in order to limit fragmentation to a minimum. In the new cooperation mechanism proposed by the Commission it is of utmost importance that competencies and responsibilities are clearly assigned between authorities, making it easier for the service providers to know their 'go-to' points – here, the Digital Services Coordinator can play an important role to clarify and simplify the competencies of national authorities.

Concerning **penalties** as laid down in **Article 42**, the DSA should clarify that these are intended to apply only to systematic failure to comply with the obligations of the DSA. Furthermore, it should be clarified how the maximum fines will be calculated exactly.