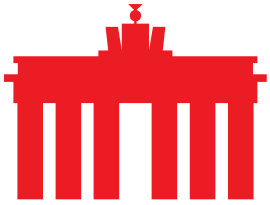

WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

POSITION PAPER

on the proposal for a Regulation on a Single Market for Digital Services (Digital Services Act) – COM(2020) 825 final

Brussels/Berlin, 25 March 2021

With its proposal for a Digital Services Act (DSA)[1], the European Commission on 15 December 2020 published the long-awaited update to the Directive on electronic commerce, known as the E-Commerce Directive (ECD)[2], adopted in 2000. The latter has been – with its limited liability regime for mere conduit (including Internet access), caching and hosting providers – the foundation for the development of the Internet as we know it today and the services offered through or based on it.

eco welcomes the opportunity to share its initial view on the proposed regulation, and we look forward to further specifying the initial, subsequent remarks in the near future.

eco acknowledges the ambitious proposal and welcomes the Commission's approach with regard to the continuation of the existing liability exemptions, which have been carried over from the ECD into the DSA. As we have previously remarked in our guidelines on the liability of Internet service providers[3], it is, among other things, paramount to have uniform rules for the Single Market, to maintain fair and reasonable liability exemptions, clarify some aspects of the notice and take-down framework, and to have legal certainty and clear definitions. Therefore, we support the Commission's approach, specifically the targeted scope, requiring different rules for different services.

The term 'digital services' encompasses a large number of companies, business models, or services; many of whom play technically or practically little to no role in the proliferation of illegal content online. For example, the business model of some business-to-business (B2B) services providers result in completely different access to the services offered and to the content received than with some platforms operating in the consumer space (B2C).

Therefore, applying the same enhanced obligations to which hosting services or even online platforms are subject to mere conduit, caching or 'pure' hosting

---

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0825

[2] **Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17.7.2000, p. 1.**

[3] **Guidelines on the liability of Internet service providers with regard to the Directive on electronic commerce (2000/31/EC), 21 October 2019, https://go.eco.de/qOQRBax.**

services would inappropriately add unnecessary burdens on them with regard to enhanced obligations. An example of such services are some cloud services, which are far removed from content and do not or, more likely, cannot technically interact with it. Not only that, it would also put such services at a disadvantage on an international market without making any significant contribution to the fight against illegal content.

Finally, eco sees multiple provisions that raise a concern and run the risk, e.g., of breaking the established trusted flagger process, of weakening the country-of-origin principle (and conditions for exceptions as established by the ECD today), of over-burdening transparency obligations and of introducing an overly extensive fines regiment.

1. On the individual Articles

1.1. Definitions (Article 2 DSA)

1.1.1. Illegal content (Article 2 (g) DSA) and harmful content

eco supports the Commission's approach, and we believe that regulatory efforts should focus on illegal content and address harmful content separately, such as through voluntary or co-regulatory approaches. Then again, it needs to be ensured that legal restrictions on blocking for Internet service providers and voluntary or co-regulatory approaches do not contradict each other.[4]

While the DSA focuses on illegal content, a definition of illegal content is not actually included in the DSA. According to the EU Commission, this was a deliberate decision. As a consequence, the laws of EU Member States are likely to result in different definitions of illegal content, giving rise to obligations to delete content that is defined as illegal in only one Member State.

Nonetheless, with the definition of illegal content as "any information—which in itself or by its reference to an activity […] is not in compliance with Union law or the law of a Member State", the DSA might lead to unintended consequences. As it stands, any reference to illegal activity from another Member State with different laws shall be deemed illegal content on the basis of the DSA.

eco urges to reconsider the choice of such a vague expression as 'any reference' in this context.

However, eco welcomes that the DSA does not include harmful content in its definition of illegal content because, while the legality of content is defined by law, harmful content is defined by a subjective impression. We would further appreciate

[4] cf. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, OJ L 310, 26.11.2015, p. 1–18

the legislator including confirmation of the exclusion of harmful but legal content from the DSA in the text.

1.1.2. Online platforms (Article 2 (h) DSA)

In its paper on the ECD, eco called for an introduction of a subcategory of hosting providers to address different sets of obligations depending on an intermediary service provider's possible reach and potential amplification. We, therefore, appreciate the Commission's proposal to create a separate category of 'online platforms' and we support maintaining a differentiation in the scope of the DSA: a one-size-fits-all approach that would impose the same rules on all intermediaries would create a disproportionate burden for many businesses, particularly among cloud services and in the B2B sector. Such an approach would limit the uptake of cloud and emerging technologies across businesses, particularly SMEs, and among consumers. This could lead to a chilling effect on innovation in the EU and damage the broader data economy, as well as Europe's technological sovereignty.

Therefore, eco considers the chosen definition to be too wide. Without adaptations, even classic hosting providers or cloud (infrastructure) services, which for technical and legal reasons in many cases do not have access to allegedly illegal content of users or customers, could be inadvertently covered by the scope of the DSA's extended obligations.

Further clarification on the definitions, along the lines of Recital 13, such as the meaning of dissemination to the public or ancillary features, could be beneficial to avoid unintentionally capturing non-platform services. As an example, it should be clarified that services whose primary purpose is not the dissemination of information to the public and who are not obviously used for such purposes but who may nevertheless provide users with some basic or limited sharing functionalities are not classified as online platforms.

1.1.3. Actual knowledge

One of the points of general criticism towards the ECD was its partial lack of clarity regarding definitions. This was the case, for example, on the point of actual knowledge. Up to now, it has not been clearly established as to when the criteria of actual knowledge are fulfilled or when they are actually not.

The proposed text does not satisfy the expectations in this regard since it, again, does not elaborate on the issue. Only in Article 14.3 does the DSA offer one example of notices giving rise to "actual knowledge or awareness". Further, the text refers to Article 5 DSA while neglecting to mention actual knowledge regarding caching providers (Article 4.1(e) DSA).

eco would encourage the legislator to improve the clarity of the definition and give intermediary service providers the necessary legal certainty. This is the case , e.g., with regard to Article 14.3 DSA which lacks clarity on the requirements in conjunction with Paragraph 2.

1.2. Mere conduit, caching and hosting providers (Articles 3, 4 and 5 DSA) and no general monitoring or active fact-finding obligations (Article 7 DSA)

The DSA proposal transfers Articles 12, 13, 14 and 15 ECD into Articles 3, 4, 5 and 7 DSA with only one change worth mentioning: the exemption from limited liability of hosting providers in the case of online trading platforms in regard to consumer protection laws. In that regard, eco would ask the legislator to clarify that the exemption from Article 5.1 DSA shall only be applicable to the specific part of the trader's platform on which users conclude distance contracts and not be applicable to cases of intermediaries that forward users to a third-party trader's website where the contract is concluded (one example would be price comparison websites).

eco welcomes the Commission's approach to further harmonise these rules by carrying them over into the new regulation. Especially positive is the reference in Recital 27, naming fundamental services contributing to the technical infrastructure of the Internet, like DNS, CDN or Registries and confirming that these services can benefit from liability protection under the DSA. However, eco would like to highlight that the framework's clarity would benefit from including these references into the regulatory part of the proposal, specifying into which category of intermediaries the services fall.

We fully support the prohibition of a general monitoring obligation[5]. Such an obligation, when put on intermediary services, would raise significant privacy issues: it could require hosting services to monitor inter alia personal, financial and medical data of potentially millions of data subjects in addition to the content of corporations and governments.

Regarding the monitoring obligations, it is worth highlighting an additional issue it would pose for B2B or B2C services, which have no contractual rights and no technical access to content that business customers or consumers store or process on their services. Only the customers have absolute control and responsibility for the content and the services they operate.

We want to emphasise that the numerous interpretations by the Court of Justice of the European Union should be preserved, as suggested in Recital 16. Moreover, the liability exemption has proven to be a reasonable approach to allow intermediary service providers to offer services without introducing an ex-ante assessment of content.

The DSA should harmonise the legal framework for all intermediary service providers by stipulating basic conditions for mandated actions (e.g. injunctions). Most importantly, only after addressing the recipient of the service first, the provider best placed to remedy the illegal situation should be addressed, and

[5] **In the light of the decision on specific obligations in the Judgement of the Court of Justice of 3 October 2019, *Eva Glawischnig-Piesczek* v *Facebook* Ireland Limited, C-18/18, ECLI:EU:C:2019:821.**

recourse to other intermediaries lower down the Internet stack should only take place where interventions are or would likely be unsuccessful.[6] The service provider requested to take action must be exempt from liability for taking the ordered measures.

In this regard, eco would also like to underline the recognition by the Commission of the role of mere conduit and caching services within the Internet infrastructure, in particular (see Recitals 26, 27 and 35).

In cases where measures are requested although the conditions for exemptions from liability are met, basic costs of action should be reimbursed on the basis that there is neither liability nor responsibility of the service provider for the illegal action or content. Finally, where recourse to judicial review against an injunction should not be admissible (e.g., in case of alleged "overriding reasons of urgency"), judicial review of the measure requested must still be secured.

1.3. Voluntary own-initiative investigations and legal compliance (Article 6 DSA)

eco welcomes the introduction of specific wording on the subject of voluntary own initiative investigations by intermediary service providers. This confirms that intermediaries are able to take proactive measures to address illegal content without, for this reason alone, falling outside the liability exemptions.

However, since the proposal only refers to illegal content, the process would benefit from a clarification that Article 6 DSA also applies to (automated and non-automated) voluntary measures that are not solely directed at illegal content but also at content in violation of an intermediary's terms and conditions (T&C).

1.4. Orders to act against illegal content and orders to provide information (Articles 8 and 9 DSA)

Contrary to the stated intention to foster the Digital Single Market also by preserving the general principles underlying the ECD, the country-of-origin principle is being put at risk by the DSA proposal. This is to the extent that the latter lacks conditions and safeguards in the case of one or several Member States intervening against an intermediary service falling under the jurisdiction of another Member State.

Since the respective ECD's provisions on the competence of the Member State of establishment as well as the provisions on an exceptional competence of another Member State remain in force, accompanied by specific procedural rules and safeguards in the interest of the functioning of the Internal Market, Articles 8 and 9 DSA as proposed are formulated in an unclear manner. In particular, Article 9 DSA does not contain the necessary safeguards for authorities to access user data. We

[6] **Notwithstanding current regulation like Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10-19, Recital 59.**

believe it should match the standards and principles of the e-Evidence Regulation, including the need for harmonized legal frameworks for cross-border law enforcement requests within the EU, and strong procedural and substantive safeguards.

Furthermore, the DSA proposal should clarify the relationship between injunctions, which were already foreseen in the ECD, and the additional measures it introduces, such as orders, notice and action requests, etc.

1.5. Points of contact and legal representatives (Articles 10 and 11 DSA)

The DSA proposal introduces the obligation for intermediary service providers to establish a single point of contact (SPOC) or, if there is no establishment in the European Union, the obligation to designate a legal representative in one of the Member States.

Recital 36 refers to the possibility of trusted flaggers or other 'professional entities' using the SPOC, aside from authorities, the EU Commission and the DSC Board.

eco would like to underline that, while publishing contact information might allow for 'easy' communication, it is challenging and inefficient for companies to have to address a wide variety of unrelated communications through a single, publicly disclosed and available point of contact. This approach is more likely to result in important messages being overlooked, like a needle in a haystack.

eco recommends that the decision should be left to the intermediaries if they want to have one SPOC for all requests or one point of contact for requests from authorities, another one for exchanges with trusted flaggers, and a third one for any other inquiry.

1.6. Terms and conditions (Article 12 DSA)

In its attempt for more transparency, the Commission's DSA proposal introduces obligatory information to be provided in the intermediary service provider's T&C. While transparency to a certain degree is a welcomed approach, it can also conflict with intellectual property rights or trade secrets. In addition, transparency is only useful when it is adequate and proportionate.

If intermediary service providers are obliged to share detailed information on, e.g., measures, tools and algorithms, used to address illegal behaviour or content, it might prevent the above from working efficiently, offering ways of circumvention by malicious users. In addition, while general rules on content moderation have a permanent character, some more granular parts might change according to worldwide developments without an intermediary's immediate influence. As a consequence, an obligation for an exaggerated level of detail could lead to the T&C becoming an unreliably fluid document. eco, therefore, suggests that intermediaries should be able to refer to a publicly available online-source for details on content moderation in an easily accessible format.

The DSA proposal requires intermediary service providers to act with due regard to the 'applicable fundamental rights of the recipients'. eco believes it is important to discuss the Commission's expectations for the scope of this assessment of fundamental rights, including freedom of expression. If interpreted too broadly, this could make it difficult for platforms to limit the scope of the services for business reasons, such as limiting the content allowed on a cooking platform to content about cooking and not allowing political discussions.

1.7. Transparency reporting obligations for intermediary service providers (Article 13 DSA)

The DSA foresees the introduction of new and extensive transparency reporting responsibilities. The draft requests, with a lack of specificity, "clear, easily comprehensible and detailed reports on any content moderation", and only micro and small enterprises are exempt from this obligation.

eco sees no benefit to anyone if exaggerated reporting obligations lead to increased costs for companies but only produce reams of paper. Therefore, eco advocates for reasonable reporting obligations. Moreover, the types of reporting expected for transparency reports should reflect the practices and requirements of different types of intermediaries. For example, mere conduit and caching services cannot be expected to report on content moderation practices as that is not an activity they engage in.

1.8. Notice and action mechanisms (Article 14 DSA)

The DSA introduces a relatively detailed notice and action procedure for hosting providers. It requests an easily accessible, user-friendly electronic mechanism to submit "sufficiently precise and adequately substantiated notices, on the basis of which a diligent economic operator can identify the illegality of the content in question".

It stays, however, unclear if the elements in Paragraph 2 (a)-(d) have a mandatory character for the notifier or if they are just options that the intermediary service provider is obliged to offer. It also remains unclear if, regarding Paragraph 3, notices that include only some of the elements in Paragraph 2 are sufficient to trigger actual knowledge or awareness for the purposes of Article 5 DSA.

The reference to 'actual knowledge' in Paragraph 3 is, in fact, the closest the DSA gets to a definition. This is despite the fact that the lack of clarity already in the ECD has been one of the main points of criticism of the Directive and one of the most asked for clarifications in an updated regulation.

In addition, eco would welcome a mechanism to allow hosting providers some leeway to reject requests referring to content that is not obviously illegal, but merely questionable, and to prevent over-blocking by not giving rise to actual knowledge automatically in any possible case – especially in regard to Article 14.3 DSA.

Finally, eco is concerned that the legislator is putting private companies in the position of a judicial actor. The legal interpretation of content cannot, and most definitely should not, lie with an intermediary service provider. Especially considering that the Internet is a global market and even smaller intermediary service providers often operate internationally, a legal interpretation of the respective national law in any possible market constitutes an unsolvable challenge.

1.9. Statement of reasons (Article 15 DSA)

Article 15 DSA says that "where a provider of hosting services decides to remove or disable access to specific items of information provided by the recipient of the service", it shall inform the recipient about the details of the removal or blocking. The legislator also introduces the obligation to document the decisions in a publicly accessible database. These obligations target every hosting provider, irrespective of its size.

The DSA draft proposal does not include any technical details on the database, e.g., how access would be granted and data submitted: by API or manually through an online form. Also, the scope of Article 15 DSA explicitly addresses (even pure) hosting providers and excludes neither micro nor small or medium-sized enterprises.

eco believes the referred article to be too vague and disproportionate, leading to an exaggerated burden, not only, but especially on MSMEs. Detailed publicly available documentation would further enable users in bad faith to find loopholes and potentially circumvent the removal or blocking of illegal content.

1.10. Internal complaint-handling system and out-of-court dispute settlement (Articles 17 and 18 DSA)

Aside from a notice-and-action mechanism, the DSA also foresees a responsibility for intermediary service providers which are considered online platforms to provide the recipient of their service with an internal complaint-handling system as well as an obligation to engage in an out-of-court dispute settlement.

Article 17.1 DSA clarifies that the online platform has to provide the recipient with the complaint-handling system for six months following any decision to remove or block content as well as to suspend or terminate the provision of the service or the recipient's account.

Recipients of the service are further entitled to use a certified out-of-court dispute settlement body in the above-mentioned cases. "Online platforms shall engage, in good faith, with the body selected with a view to resolving the dispute and shall be bound by the decision taken by the body."

In accordance with Article 18.3 DSA and depending on the outcome of a decision, the online platform either has to burden all the costs of the settlement procedure, in the case of a decision in favour of the recipient of the service, or their costs, in the case of a decision in the online platform's favour.

eco would like to highlight that, regarding Article 17.1 DSA, a six-month period is unrealistic and a disproportionate burden. The Internet is a short-lived medium. If a recipient of a service does not challenge the decision of an online platform within days, it has to be expected that they either do not feel treated wrongly, that the relevance of the action is minor, or that the account is not in active use. For an online platform, on the other side, this long period would increase the number of cases to be brought forward despite a lack of gravity, that data has to be kept on a decision or that the reasoning in the meantime could face changed realities. eco urges, therefore, that the period be decreased to ten weeks, following the approach of the German Network Enforcement Act (NetzDG).

We also urge the legislators to consider defining exceptional circumstances in which intermediaries are not obliged to offer redress options, including out-of-court dispute settlement, e.g., when the content in question is spam, child sexual abuse material or terrorist content. This further applies to removals based on national authorities' removal orders (under Article 8 DSA), including where these orders may be confidential and appear as the online platforms' own decision.

Further, eco would like to underline, concerning Article 18.3 DSA, that platforms are always obliged to bear their costs for an out-of-court dispute settlement, while the recipients of the service only face the risk of having to bear their expenses – or nothing at best. In addition, the process of arbitration does not include any protective measures against abuse and, as a consequence, actors in bad faith could flood an intermediary with out-of-court dispute settlement procedures, generating costs and slowing down the process for other, legitimate recipients of the service. This approach seems to be unfairly imbalanced.

Finally, we believe that out-of-court dispute settlement processes should foster transparency and clarity. To that effect, we suggest that there should be one certified out-of-court dispute settlement body per Member State and that such bodies should work towards harmonized approaches and decisions to avoid fragmentation. One potentially helpful measure in this regard could be that settlement bodies take on the responsibility of publishing transparency reports on out-of-court dispute settlements (as foreseen in Article 23 DSA). Finally, we believe that out-of-court dispute bodies should be distinct from regulatory oversight bodies and that the text should clarify this.

1.11. Trusted flaggers (Articles 19 and 20 DSA)

Trusted flaggers have been used by online platforms for a reasonably long time to support their work of finding and evaluating content on their platforms. The choice of partners so far was theirs to make and depends on their criteria and their requirements.

With the DSA, the legislator takes away the choice from the online platform and centralises it on a national level by leaving it up to the DSC to define a minimum group of appointed trusted flaggers.

Applicants need to represent collective interests and need to be “independent from any online platform”. Recital 46 points out that “for intellectual property rights, organisations of industry and right-holders could be awarded trusted flagger status”.

eco does not see any indication being given as to why a well-established system, developed between trusted flaggers and online platforms, is forced into centralisation on a national level and strongly advises against the introduction of the latter. Online platforms generally work in an international market and have developed their network of entrusted entities. These entities know the online platform and the staff as well as the individual systems, interfaces and workflows many of the platforms offer to increase efficiency and allow them to quickly assess flagged content.

The system proposed in the DSA compels online platforms to work with any awarded trusted flaggers and to arrange certain procedures with them. For this, it would not matter if a trusted flagger interacts with the platform multiple times a day or maybe only once a year. In combination with the SPOC in Article 10, it would even be possible to use a generally published contact, probably via email, to flag content. This can by no means result in an efficient procedure.

The reference to right-holders is a worrying example of how complicated the system could become very quickly. While it is without a doubt that right-holders are affected by illegal content they are also numerous. To keep a system effective it is, however, necessary to limit the number of trusted flaggers nationally awarded by a DSC. This being said, it is still up to individual platforms to intensify the exchange with any other associations or individuals where they see fit and award them an individual trusted flagger status.

With respect to Art. 20.2 DSA, the proposal defines that online platforms “shall suspend the processing of notices and complaints submitted” by trusted flaggers “that frequently submit notices or complaints that are manifestly unfounded”. eco would welcome a further specification to include the phrasing from Article 19.5 DSA specifying “insufficiently precise or inadequately substantiated notices” to trigger a suspension. Finally, liability and compensation obligations for the resulting damage need to be introduced for abusive blocking requests.

1.12. Notification of suspicions of criminal offences (Article 21 DSA)

The DSA introduces the obligation that “where an online platform becomes aware of any information giving rise to a suspicion that a serious criminal offence […] has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities”.

eco criticises that platforms are put into the role of law enforcement. Aside from this, we consider the chosen wording to be too extensive. To avoid any risk of wrong-doing, a VLOP would likely have to be oversensitive. As a result, law enforcement would receive a high number of false reports. eco encourages the

legislator to amend the language and the safeguards, taking into account existing legislation.

1.13. Traceability of traders (Article 22 DSA)

With the DSA, the legislator introduces a so-called know-your-business-customer (KYBC) obligation for online platforms offering traders an online market place directed at consumers. According to Recital 49, these new rules should contribute to a safe, trustworthy and transparent online environment.

Online market places will have to gather and check detailed information on traders allowed on their platform. The proposal also foresees that the online market place has to obtain information on the economic operator.

The idea of a KYBC approach in the DSA seems reasonable. However, the obligation to gather information on the economic operator, aside from a wide range of details on the trader, appears excessive. For an average online market place, this duty likely results in having to check and maintain dozens to hundreds of references per trader. eco would, therefore, welcome the removal of Paragraph 1 (d).

We further suggest clarifying that these provisions, which are aiming at online marketplaces, should not apply to online platforms that do not allow the consumer to conclude a distance contract but act as intermediaries between the user and the third-party trader.

1.14. Very large online platforms, risk assessment, mitigation of risks, independent audit (Articles 25ff DSA)

For the DSA proposal, the legislator introduces a distinction of hosting providers that are not only online platforms, but ‘very large online platforms’ (VLOP). The threshold to qualify as a VLOP is set to 45 million average monthly active recipients. VLOPs are to be subject to stricter rules and extended obligations.

At least once a year, VLOPs “shall identify, analyse and assess […] any significant systemic risks stemming from the functioning and use made of their services in the Union.” Art. 26.1 DSA offers examples of systemic risks. Aside from the dissemination of illegal content, it stays very vague, though, mentioning ‘any negative effects’ on fundamental rights as well as the manipulation of a platform’s service with an at least foreseeable negative effect on different sensitive areas.

While it is in a platform provider’s own interest to mitigate risks of misuse of its platforms, eco criticises the lack of clarity in the set-out obligations using an unspecific ‘any’ as well with ‘significant systemic risks’ and with ‘negative effects’, and also ‘foreseeable negative effect’.

We also see that Article 26 and Article 35 will regulate harmful, but legal, content through the backdoor. Contrary to the European Commission’s intention with the DSA to focus on illegal content, the new powers for regulators to define risks and suggest risk mitigation measures may result in lawful content being taken down excessively.

On the basis of the yearly risk assessment, the DSA obliges a VLOP also to conduct an independent audit at least once a year at their own expense. Following the audit, a VLOP shall implement possible recommendations within a month.

eco worries that VLOPs will spend a lot of time and a considerable amount of money on writing reports for the sake of evaluating, mitigating and auditing risks and behaviours instead of focusing on actual work to improve their systems. We suggest decreasing the frequency of independent audits to at least every two years and increasing the time for the implementation report.

Finally, the reference in Article 28.1(a) DSA on including the whole Chapter III seems excessive. eco would consider a carveout of at least Articles 34ff DSA appropriate, not only but also assuming that these will fall under separate monitoring.

1.15. Data access and scrutiny (Article 31 DSA)

With the DSA, the legislator not only wants to ensure that VLOPs do more, but also wants to get more insight for DSCs and researchers. With mandatory access to data for researchers via databases or application programming interfaces (APIs), another layer shall be added to control VLOPs and to monitor their compliance with the regulations.

Putting aside that adding a third layer of supervision gives the impression that VLOPs need to be scrutinised more intensively than financial institutions: Granting access to databases upon ‘reasoned request’ puts trade secrets at risk, and sharing data externally via databases or APIs introduces unnecessary security risks by having to offer access that can be misused by third parties. While Paragraph 6 considers the risk of vulnerabilities for the security or the protection of confidential information, it only does so in the case of ‘significant’ ones and puts VLOPs in the position of having to ‘request’ an adapted request from the DSC. However, the final decision lies again with the DSC or the Commission.

By means of delegated acts, the Commission shall further be able to lay down the purposes for which the data may be used. By doing so, the Commission would be able to change the purpose of Article 31 DSA without any checks and balances.

eco calls the legislator to remove the ultimate obligation to give access to researchers by means of data(base) copies or APIs as well as the right for the Commission to amend the use of data by delegated acts. Finally, a definition of reasons for requests and limitations on what data can be used for (in line with the purpose-limitation principle of the GDPR) would increase legal certainty and should be oriented on what is necessary.

1.16. Competent authorities and Digital Services Coordinators (Articles 38ff DSA)

The Commission’s draft introduces the new function of a Digital Services Coordinator (DSC). While Member States shall be able to designate more than one competent authority, it is being made clear that only one competent authority has

to be declared as the DSC. The jurisdiction further falls to the Member State in which the main establishment of the intermediary service provider is located. However, the DSC "shall act with complete independence. They shall remain free from any external influence, whether direct or indirect and shall neither seek nor take instructions from any other public authority or any private party."

eco welcomes the clear structure and the centralisation of points of contact to a maximum of one per Member State as well as the independence of DSCs. The cooperation of DSC on the board further supports the harmonisation approach.

1.17. Penalties and fines (Articles 42 and 59ff DSA)

Regarding penalties and fines, the DSA was clearly modelled on the General Data Protection Regulation with its maximum of 4% of the worldwide annual turnover. However, while the motivation for drastic fines is obvious, a further significant elevation to 6% of the worldwide annual turnover of an intermediary in the DSA can be considered exaggerated.

Leaving the precise adjustment of penalties to the Member States further will not support the harmonisation of the Single Market but lead to different approaches in the Member States and likely to significantly different ranges of penalties.

eco urges to clarify the interplay of Article 42 and Articles 59ff DSA and strongly supports a unified list of fines and penalties instead of potentially 27 different approaches in the Member States plus one for the Commission. We would also welcome a clarification that the fining powers of the Commission may apply only to systematic violations of specific due diligence obligations.

1.18. Entry into force and application (Article 74 DSA)

The DSA poses a variety of significant changes and new challenges to intermediary service providers, but also to national authorities. This is why eco considers the application within three months after the DSA enters into force as unrealistic. For proper planning, implementation and coordination with other involved parties, a time frame of at least 18 months will be necessary.

2. Conclusion

The Commission's proposal for the DSA to update the ECD is ambitious and is the result of solid work and detailed preparation.

However, in some detailed aspects, eco sees room for improvement to make sure that especially the liability exemptions for classic hosting providers and the country-of-origin principle are clearly defined and maintained, effectively contained by legal guarantees and safeguards through procedural provision.

A clear definition is also, what – despite the modernisation – eco is still missing in particular with regard to 'actual knowledge' (also in light of Article 14.3 DSA), 'dissemination to the public' or with the newly introduced definitions of 'illegal content' or 'online platforms'.

With the introduction of a notice-and-action procedure defined by law, the DSA tries to set a standard for the handling of illegal content. This also includes the centrally awarded trusted flagger status, publicity beyond transparency for processes, actions and technology due to the new transparency obligations, the unbalanced complaint handling and out-of-court procedures, and the continued privatisation of jurisdiction supported by the notification obligations for suspicions of criminal offences.

As mentioned in the introductory remarks, eco supports the newly introduced differentiation of (very large) online platforms from classic hosting providers. However, we also think that some burdens the DSA puts on VLOPs are unclear or extensive without showing a benefit that is worth the workload created for platforms.

The controlling rights for DSCs and the Commission should be further specified and limitations introduced by the legislator.

Finally, the application of the DSA should not begin earlier than 18 months after it entered into force.

About eco

With more than 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995, eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. The focal points of the association are the reliability and strengthening of digital infrastructure, IT security, trust, and ethically-oriented digitalisation. That is why eco advocates for a free, technology-neutral, and high-performance Internet.