April 2021

A Single Market for Digital Services: Summary of DOT Europe Recommendations

With the Digital Services Act (DSA), the European Commission aims to create a real Single Market for digital services. DOT Europe – the voice of leading digital, online and tech companies in Europe – welcomes this approach.

The DSA provides a real opportunity to establish a horizontal framework for all digital services, providing legal certainty and the necessary assurances for stakeholders. As part of this new framework, the proposal introduces several measures for online service providers, which are collectively referred to as due diligence obligations. These measures are not necessarily new, and several online service providers currently make use of similar measures on a voluntary basis to tackle different issues on their services. Given this experience and the diversity of services on offer, DOT Europe members have much to contribute to the discussion on the practicality and feasibility of the proposals in the DSA.

Below, we have put forward several recommendations on Chapters I to III of the DSA proposal**,** building on the questions we raise in a complementary paper "DOT Europe Questions and Recommendations on the DSA". With this feedback, we aim to contribute to the creation of an effective and proportionate framework which addresses stakeholders' concerns, while supporting innovation in the EU Single Market.

The scope and definitions in the DSA should be clear and precise

The DSA has the potential to establish a new approach to tackling illegalities online – one which takes account of the **diversity of services in the online ecosystem** and proposes **asymmetric, proportionate, and tech-neutral responsibilities** to address the challenges in the online space.

To do so, **the scope and definitions of the DSA must be correct and precise**. Concepts such as **"dissemination to the public", "illegal content" and "minor and purely ancillary feature" in Article 2 will need to be clarified**. Similarly, it is not clear what an "active recipient" means in practice when considering which services meet the very large online platforms threshold in Article 26.

Continuing with Article 2, given the importance of the subsidiarity of obligations under the DSA framework, it will also be important to specify that IT infrastructure services deeper in the internet stack (i.e., cloud infrastructure services, content distribution services, DNS services) are not considered "hosts" and B2C cloud services are not considered "online platforms".

These clarifications will be necessary to ensure that the DSA does not lead to unintended consequences or give rise to situations in which certain service providers cannot comply with elements of the proposal due to the structural nature of the service on offer.

The liability regime in the DSA should echo the horizontal nature of the proposal

The DSA can establish a new horizontal baseline for the rules and responsibilities for all stakeholders in the online ecosystem. Consequently, DOT Europe is encouraged to see that **the core principles of the e-Commerce Directive** (Articles 12-15) - namely the limited liability regime and the ban of general

monitoring obligations - **are preserved** in the DSA proposal (Articles 3-7). These provisions **provide legal certainty and ensure the protection of fundamental rights in the online space**.

However, **Article 5(3) conflicts with this goal**, introducing a specific parallel liability regime for certain services in relation to liability under consumer protection law, without making it clear how it will work within the DSA's horizontal framework. It is also not clear how this deviation will benefit consumers, as they cannot determine in advance whether a court will find that they even have a claim against a service provider. This Article should be removed, and the specific issues relating to consumer protection be addressed in separate legislation, to avoid fragmenting the DSA from the outset.

Orders to act and provide information need to be clarified

The country-of-origin principle (COO) allows online service providers to develop working relationships with the authorities in their Member State of establishment, drastically increasing the effectiveness of all measures. **The COO principle should not be weakened through the orders proposed under Articles 8 and 9**.

Specifically on Article 9, any requests for information should remain limited to information that the service provider collects in order to provide the service, and which lies within its control.

Information about content moderation

Regarding Articles 12 and 29, **the granularity of the information required by both Articles will need to be carefully considered** by policy-makers, as well as the target audience of this information - too much insight can allow bad actors to game the system. **Service providers should also not be required to disclose information relating to trade secrets**.

During this discussion, it is also important to keep in mind that "recommender systems" can take many forms (listing in chronological order can also qualify as a "recommender system"), and that **many online service providers already offer users different options as to how they would like to view content on a service.** Moreover, it will never be possible for users to completely opt-out of how a service provider presents content, given that the content must be organized in some way or another.

Notice and Action provisions should be carefully drafted

Article 14(3) needs to be clarified so that a notice which fulfils all the requirements of a substantiated notice should not in itself give rise to actual knowledge. As it is currently drafted, Article 14(3) could mean that notified content would have to be immediately removed or disabled by a service provider in order to avoid liability, without allowing the service provider to carry out their own assessment to determine the legality of notified content and stripping the service provider of the discretion to keep lawful content online.

In fact, it is recommended that **"action" under Article 14 should constitute any service provider response on a notice**, be it via action taken on the content, the decision not to act against the content, or via updates provided to the notice issuer following the service provider's assessment of the notice

A notice and stay-down obligation should also be avoided in Article 14, and indeed in any part of the DSA. Such **obligations are akin to a general monitoring obligation**, as it will still require an online service provider to scan all uploads for specific notified infringements. Introducing such measures would thereby conflict with Article 7 of the DSA and prove **detrimental for the freedom of speech and users' right to privacy** – which the prohibition on general monitoring is designed to protect. Instead,

safeguards such as those currently envisaged under Article 6 should be put in place for service providers to proactively come up with solutions to address previously identified infringing content.

Transparency reporting should be designed with the intended audience in mind

With regards to transparency reporting obligations under Articles 13, 23, 24, 30 and 33, it is important to keep the intended audience in mind. **Those intended for the public eye should not be so granular** as to allow bad-faith actors to circumvent service providers' content moderation measures, while **those addressed at authorities for enforcement purposes can be more detailed**. In considering the required content of these reports, it is also important to take account of the variety of digital services which must comply with these obligations. **Introducing a one-size-fits-all approach**, e.g. in terms of reporting formats or outputs, **will certainly not be optimal for all service providers, nor present an accurate picture** as to the proportion of illegalities notified and removed.

This discussion on transparency reporting also offers the opportunity to **expand the scope of the obligations to other parties which are involved in the notice and action process**, such as rightsholders, trusted flaggers, competent authorities, etc. Requiring these parties to also submit transparency reports would provide valuable information on how notices are filed and treated in the online ecosystem, and provide a better picture of the systems in place for tackling illegalities for policy-makers. This broadened scope would also go a long way towards enhancing cooperation among stakeholders, and optimising notice and action procedures.

With regards to the Digital Services Coordinators (DSCs) and their role in the transparency regime, **it is recommended that their tasks and objectives are clearly defined**. This could include objectives around market observation and the assimilation of information and learnings based on the transparency reports submitted by online service providers.

More clarity is needed on complaint handling and dispute resolution

Regarding Articles 17 and 18, **users should use internal complaint handling mechanisms first, rather than turning directly to an out-of-court dispute settlement body**. These systems can then be overseen by the regulatory framework proposed in the DSA in order to avoid any unintended consequences.

Moreover, a dispute resulting from a notice or order from an authority should be exclusively resolved between the notifier or the authority and the affected recipient, as the service provider does not necessarily have all the facts that led to the notice/order and is acting on the notifier's request.

Finally, to maintain full access to justice, more clarity is needed regarding the possibilities for parties to **challenge the conclusion of a dispute settlement body** in case a party disagrees with the outcome.

Ensure the use of trusted flaggers does not do more harm than good

Article 19 currently states that the notices from trusted flaggers should be given priority over other notices. However, **service providers should be able to process notices flexibly, depending on the nature of the notifier and the nature of the alleged illegality notified**. Certain types of illegalities can require a more urgent response (e.g. CSAM, or activity that might give rise to material and bodily harm), and these will have to be prioritised above notices from trusted flaggers.

More details on the appointment of trusted flaggers are also needed, given the role they will play under the DSA**. Objective vetting criteria for trusted flaggers are also advisable.** As there is no limit to the number of trusted flaggers appointed by Member States, there is a risk of imbalance in numbers

and in expertise between Member States e.g. should trusted flaggers specialised in certain issues be more numerous in a specific country. This could lead to a situation in which e.g. many trusted flaggers from the same country flood a service's inbox with notices regarding content that might be illegal in their Member State but is perfectly legal in the service provider's country of origin. Additionally, the trusted flagger status should not be a means for law enforcement authorities to bypass the notification system they have already in place.

Online service providers should have the final say on their repeat offender policy

Article 20 should provide the **flexibility** for online service providers **to assess whether or not to adopt measures against the misuse of their services**. If an online service provider wishes to process and consider all the notices for illegal content it receives, it should be able to continue doing so – assuming the risk that this may entail in terms of liability.

Furthermore, **in some very severe cases** (e.g., sharing of child pornography, attempted sale of illegal drugs) **one violation must be enough** to justify the suspension of an account.

Article 20(3)(d) should be deleted, as it requires online service providers to **evaluate the "intention" of the alleged abuser**. This form of subjective assessment should not be up to service providers to investigate or judge, but rather should remain in the remit of the courts.

The scope of "suspicious criminal activity" should be defined

The obligations under Article 21 are **potentially very far-reaching**. Policy-makers should clarify what constitutes a "threat to life", and how a service provider is to determine when a threat is "likely to take place", as well as what "reasonable certainty" will mean in practice.

It should also be made clear that there is **no resulting constructive liability** for situations that are not notified to law enforcement by a service provider – reasonableness and proportionality should always be considered.

The Traceability of traders should take into account existing legislation

The **definition of "trader"** in Article 2(e) of the DSA is based on the same definition in the Consumer Rights Directive and **should not be altered** during the legislative process. It should also be made clear that it does not apply to B2B services, as some services allow anyone to open a business account, making it impossible for the service provider to check the credentials of every "business" user.

On the Know Your Trader (KYT) obligations under Article 22, alignment with existing and forthcoming legislation (e.g. Anti-Money Laundering Directive and DAC 7) **should be prioritised**. This includes the method of verification, which should be flexible enough to allow for automated processes to facilitate a system based on users' self-declaration, and to enable service providers to adopt a risk-based approach to define a timeline for re-screening. Furthermore, the "kick-out mechanism" should be adaptable enough for the company to decide when to block a user, in line with the DAC 7 Directive.

The final rules on KYT the DSA should also be supported by the right infrastructure. When it comes to reporting, **authorities should provide simple and secure ways for service providers to report data,** and for their data to be treated following the submission of a report.

Finally, the **notion of economic operator should not be confused** with the obligations in the DSA and should remain in the corpus of law related to goods, to avoid contradicting existing legislation concerning the display of the economic operators' information.

Risk Management must take into account the diversity of services

Flexibility is very important to the overall success of the approach to risk management under Article 26 of the DSA. It must also be **complemented by the safeguard in Article 6**, to ensure that the VLOPs taking steps **to mitigate any identified risks can do so with the necessary assurances and legal certainty**. Furthermore, **the scope of risk mitigation under Article 26 should focus on illegal content** – as it is currently drafted, service providers will be required to assess systemic risks based on content that is harmful but not necessarily illegal.

Policy-makers should also consider **who could fulfil the role of auditors** for the purposes of Article 28 and reflect on whether a sufficient number of experienced independent auditors actually exist. Adopting a **risk-based approach to audit findings** is also recommended to support the development of action plans and remediation.

Finally, Codes of Conduct are included in the risk management provisions of the DSA. As they are voluntary by nature, it is recommended that these frameworks should be **excluded from the scope of audits** under Article 28(1), and that reporting and verification processes be tailored to each of the Codes of Conduct instead.

Data-sharing should always be balanced with privacy and security

Given the sensitivity of the data that must be provided to the DSC and the Commission under Article 31, the **technical conditions for the provision of this data should not be defined under delegated acts**. Furthermore, precision is needed in this Article, notably regarding the definition of "reasoned request". We would recommend **allowing service providers to take more measures to protect the privacy of data subjects** and setting limits on what can be done with the data and how, with respect to security standards.

The compliance framework should be future-proof and proportionate

All service providers should have the opportunity to engage in the Commission's process for the development of the Codes of Conduct under Article 35. Article 35 should also set out the broad boundaries within which the Codes will be developed.

For the purposes of Article 57, **explanations of databases and algorithms** ought to be provided **in response to information requests by the Commission**. This Article relates to highly commercially sensitive information, and this approach would be more proportionate than granting direct access.

Other considerations

Should a situation arise in which there is a need for **fines or penalties**, these **should be used by the DSCs to tackle systemic breaches** of the due diligence obligations, not individual infringements, and should only be pursued in the event of a breakdown of dialogue between the parties.

More clarity on the tasks and objectives of the Commission and DSCs would be welcome, particularly on the operation of COO under the envisaged cooperation framework between DSCs in different Member States under Articles 45-46.

Finally, **the implementation period for this Regulation ought to be extended under Article 74**. The DSA proposes a new framework for all stakeholders, and its success will depend on the ability of all the parties in the chain to effectively play their role.