BUSINESSEUROPE

POSITION PAPER

21/05/21

The Digital Services Act (DSA)

KEY MESSAGES

1. **We support the goals of the DSA to ensure a safer, more predictable and trusted online environment.**
2. **The DSA should focus on intermediaries disseminating public information to ensure a safer and more transparent online environment.**
3. **While codes of conduct could curtail "systemic risks" that are harmful but not necessarily illegal, we agree that the DSA should focus on the removal of illegal goods & content online.**
4. **Upholding the "country of origin" principle throughout the application of the DSA is of paramount importance.**
5. **We agree that the current limited liability scheme of the eCommerce Directive should continue to be upheld and that authority orders should be harmonised to efficiently remove illegal content rapidly. We support harmonisation of the notice and action and trusted flagger mechanisms to ensure efficient removal of illegal goods and content online.**
6. **We support no general obligation to monitor and the ability for platforms to be encouraged to carry out their own investigations to actively remove illegal content online.**
7. **We support the Know Your Business Customer (KYBC) provision to apply to online platforms that allow consumers to conclude distance contracts with 3rd party traders for the sale of goods or content.**

BUSINESSEUROPE a.i.s.b.l.
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL main@businesseurope.eu
WWW.BUSINESSEUROPE.EU – Follow us on Twitter @BUSINESSEUROPE
EU Transparency register 3978240953-79

CONTEXT

Digital services have continued to thrive throughout the application of the eCommerce Directive. However, since its inception in 2000, the state of the internet and the business models it supports have changed rapidly. Online intermediaries now play a prominent role in offering goods and services to EU citizens in what is now a highly varied and complex environment.

In 2002, only 7% of EU citizens shopped online at all, this now stands at over 70%. Online commerce has become more popular due to its consumer benefits of: choice, ease and comparability. This has also offered businesses greater opportunities to scale up and reach new markets. In 2015, the Commission estimated the online sales of goods at 7% of the total retail sales in the EU. The upward trend in e-commerce continues with the annual value of e-commerce in Europe expected to be €621 billion by the end of 2019, up from €547 billion in 2018, a 13.6% growth rate, compared to an annual growth rate of between 2 and 3% for retail overall. E-commerce across all digital channels therefore represents about half of the growth in retail in absolute value. In 2017 about 68% of EU internet users shopped online at least once.

However, there is an ongoing concern about measures to control unsafe and counterfeit goods brought through these online channels. IP infringing goods continue to be imported from 3rd countries for distribution across various channels. In 2019 EU customs detained 40m[1] articles with a potential retail value of €759m. Unfortunately, a large amount of these goods were found to be counterfeit. Around 80% of actions by customs related to small packages. There is no data about the sales channels through which these were ordered, although DG TAXUD reports that the goods seized in postal traffic are mainly consumer articles ordered via ecommerce – which could therefore relate to purchases directly from websites, via social media advertisements, sales through online marketplaces or other distance selling. Separately, the EUIPO estimates that the value of all domestic imports of IP infringing items across all channels could be as large as €121bn in 2016.

A 2018 Eurobarometer found that 60% of respondents thought they had seen some sort of illegal content online when using digital services. This included scams, frauds, illegal practices and hate speech. The EU network of hotlines for exploited children, INHOPE, estimated that online child sexual abuse material processed between 2017 and 2019 had doubled.

The ongoing COVID-19 pandemic and pursuant local lockdowns have increased the use of digital services, which have provided an important means of keeping consumers supplied and many businesses able to continue to trade in difficult times. With that growth comes further opportunities for illegal goods and content to circulate. At the same time, we remind policy makers that other legislation impacting the online economy does currently exist in other policy areas: the GDPR, the Geo-blocking Regulation, the Copyright Directive, the Terrorist Content Regulation and the Platform to Business Regulation. More recently, the Commission has launched both an IP Action Plan and a Customs Action Plan. We therefore remind policy makers that digital services already make conscious efforts to curtail the number of illegal activities that are online.

[1] The largest volumes seized were matches (22.9%), cigarettes (21.3%), packaging materials (13.6%), toys (9.6%) and clothing (3.9%).

Cooperation with authorities also to address these issues also takes place. This is not only to be compliant with the law, but to enable a safer and therefore more profitable online space. Businesses thrive on customer trust, and trust is earned by services that focus on protecting their customers and ensuring the integrity of their services. However, national notification and action procedures born from Art 14(3) of the eCommerce Directive remain highly fragmented in practice. We recognise the issue of the growing amount of illegal goods & content online and the need to complement the eCommerce Directive to the realities of the current online landscape. We also recognise the need to add more novel due diligence requirements of platforms with the largest reach in the public space.

We share the Commission's ambition to ensure a safer, more predictable and trusted online environment. As a key societal stakeholder, BusinessEurope outlines its reaction to the Commission's proposal for the DSA, below:

SCOPE

The online economy offers various services to natural and legal persons. From intermediary or hosting services offering network and cloud infrastructure to online platforms offering public marketplaces or social media, the digital single market has complex supply chains, different actors responsible for offering individual services that when taken together, offer a seamless consumer and business user experience.

For these services to remain beneficial for business users and consumers alike, each actor involved in offering these services should be responsible for ensuring that they are free from illegal goods or content. However, intermediaries providing merely technical services may not technically or even legally be able to see and remove potential illegal content on their service.

While we agree with the definition and coverage of "online platforms" (Art 2(h)) being those that only disseminate public information and should adhere to the graded obligations to ensure a transparent and safe online environment as listed in Chapter III and any potential order under Art 8 to act against illegal content, we remain concerned with the definition of a "hosting" service under Art 2(f) which when read with Art 2(b) creates concern for service providers that do not disseminate public information as they do not have legal access or control over client or user generated data. Some use cases of cloud infrastructure could also mistakenly be covered.

It is necessary to consider that Art 2(f) includes "hosting" services in the scope of the DSA that store information at the request of "legal persons" (Art 2(b)). However, some B2B services do not aim to disclose information to the public, particularly industry platforms or cloud services. Content moderation in these circumstances can therefore be nearly impossible. Such service providers cannot always see and remove individual pieces of content. The DSA should take this complexity into account. Therefore, these services should not be penalised if they cannot fulfil Art 8, 14 or 19 obligations because it is otherwise technically or legally impossible. However, if such a situation arises where an Art 8, 14 or 19 notice of illegal goods or content can be linked to such B2B services and they are not technically or legally restricted from acting, then they should act without delay. We agree that in other cases, B2B services, could implement some graded

obligations assigned to them in Chapter III where relevant to ensure a transparent and safe online environment.[2]

Inclusion of "reference" to an illegal activity in Art 2(g) should avoid a broad application that considers content illegal that is simply being demonstrated (eg. a film with cars breaking the speed limit).

Harmful Content:

We agree with the results of the DSA's previous stakeholder consultation that 'harmful' (yet not illegal) content should not be covered by the DSA. Therefore, it should not be subject to removal obligations. We support the idea of codes of conduct to curtail "systemic risks" (that are not always illegal) on Very Large Online Platforms (VLOPs), but in support of the results of the stakeholder consultation and Parliament INI report (Saliba MEP, point 47) and the Commission's explanatory memorandum, we believe Art 35 should clarify that the codes of conduct (that can be developed by means of a self-regulatory process) should focus on tackling illegal content and reducing systemic risks with the reference to the assessment criteria defined in Article 26(1) only. In relation to Art 26(1)(b), on curtailing negative impacts on various fundamental rights, a specific focus on best practices of cyber resilience could be included.

COUNTRY OF ORIGIN

Upholding the "country of origin" principle (Art 3(2) of the eCommerce Directive) throughout the application of the DSA is of paramount importance. However, Member States have diverged from this principle in practice and frequently used the derogations available to them (Art 3(4) of the eCommerce Directive). Various Member States are currently derogating from the "country of origin" principle for disproportionate reasons. This is fragmenting the single market.

We are positive on the neutral stance of the DSA so that various types of illegality can be defined under separate specific legal frameworks but ask for more detail on how the process of cross border takedown orders would work in practice. While national rules will clearly continue to exist, it is legally unclear as to which provision would succeed in practice: the "country of origin principle" of the eCommerce Directive or the ability for Member States to ensure all businesses follow their national rules, whether established there or not (eg. Art 2(g)).

We ask for the Commission to monitor more closely how the country of origin principle is being applied in practice and whether derogations are indeed proportionate to achieve Member State public interest aims. Current powers of enforcement should be used to ensure that this principle is indeed functioning correctly. The application of the DSA should in no manner lead to the erosion of the country of origin principle or restrict the free movement of services for unjustified reasons.

We support clarity on how the proposals on cooperation between national Digital Services Coordinators (Art 45, 46, 49) will operate to support, and not undermine, the Country-of-Origin principle and oversight by the DSC of establishment.

[2] Confindustria does not agree with the text reported because it has an excessively generic formulation: the risk is to create an arbitrary interpretation on the scope of application of the DSA, in relation to B2B services, that could undermine the harmonization objective of the regulation. Furthermore, the risk associated with the generic nature of the sentence is regulatory vacuum, to the detriment of legal certainty.

LIABILITY

We agree that the current limited liability scheme of the eCommerce Directive (section 4) should continue to be upheld. The co-legislators should continue to remember that no matter how strict the rules we place on intermediaries to police the market, non-bona fide players will always attempt to cut corners and use the practical benefits of the platform economy to do so. We should not forget that proper enforcement of existing Intellectual Property and Product Safety frameworks by Member States should be better resourced and utilised to dissuade illegal actors from posting online in the first place. We welcome the recognition of this in the IP Action Plan, the Customs Action Plan and the recitals of the market Surveillance Regulation.

While providers of intermediary services should not intentionally mislead the consumer or their rights under law, we are concerned as to how Art 5(3) has been drafted in relation to "hosting" services. Currently phrased, it could be construed that if services present information of a 3rd party (eg. a business seller) in a standardised or organised way, as is commonplace on a variety of online services and that this "could be" interpreted by the "average and reasonably well-informed consumer" as being offered by the hosting service itself, then the usual limited liability would not be available to them. This is a concern as most hosting services present information in a standardised way to support consumer navigation purposes. It is important that hosting services adopt the highest standards of transparency to highlight that the information comes from a 3rd party which is not offered by the hosting service.

We understand the principle that intermediary services should have no general monitoring obligation (Art 7) and that the orders to act against illegal content (Art 8) should be harmonised more effectively and avoid unnecessary and burdensome formalities for notices (eg. including URLs as mandatory). The legal specifications for a notice should be defined by law according to the type of activity, this would allow to correctly identify the relevant types of content and action they should take to support legal certainty and maximum harmonization at EU level. Clearly similar and equivalent cases to the original order should also be rapidly dealt with.

Intermediaries should act against illegal goods & content on their services that have been presented to them by authorities or have been detected through their own investigative initiatives, without delay. Intermediaries should be encouraged to actively engage in illegal goods & content moderation, rather than just wait to receive reasonable knowledge. That is why we support the proposal that intermediaries are not ineligible from the exemption of liability if they voluntarily carry out their own investigations for legal compliance (Art 6), however this could be made clearer.

DUE DILIGENCE OBLIGATIONS

We agree with the approach in Chapter III to set graded due diligence obligations on relevant digital services providers to support a transparent and safe online environment.

In relation to the application of Art 15(4), it would be necessary to clarify methods of implementation which hosting services should uphold to publish the information of the decisions and reasons behind the removal of information online. In addition, the competent authority pursuing an Art 8 removal should be the one delegated to publish the information in the Commission's public register.

Diversity of opinions and scrutiny by the media is important for a democratic society and must be preserved. While we are therefore supportive of Art 12 as an important confirmation of the freedom of expression and information by referral to the "applicable fundamental rights of the recipients of the service as enshrined in the Charter", we propose adding a specific referral to Art 11 of the Charter itself to the text to highlight that freedom and pluralism of the media is a vital right to uphold within the DSA.

In relation to use of any “out-of-court dispute settlement” in Art 18, we support an evaluation of the impact its use has on commercial relationships to ensure no adverse impact of such provisions arise.

Notice & Action Mechanisms:

We support the notice & action mechanism within Art 14 to permit “any individual” or “entity” that “considers” information to be illegal online to submit it to a hosting service or online platform (Art 14(1)). This would greatly aid a safer online experience for consumers and business users.

Often known as “flagging”, these practices already exist in online marketplaces and social media. Their use and what it demonstrates widely varies across different business models. Overall, the predominant use of flagging today attempts to make the online user experience safer. It also permits the digital service provider to efficiently design how the flagging system is designed to suit the needs of its own business model. We therefore support Art 14 as it would help standardise and substantiate requests to act on illegal goods & content, particularly through demonstrating the criteria needed in a notice through Art 14(2).

Art 14(3) demonstrates that if Art 14(2) criteria are fulfilled by the “flagger” then it “shall be considered to give rise to actual knowledge”. It is currently unclear as to effect of this “actual knowledge” in practice.

While some digital services could feel confident to take decisions in certain instances where the facts presented are obvious, it is by no means that all digital services, for example, online marketplaces permitting thousands of various business users to sell on them, could always be correct. For this reason, it is important that this mechanism is not confused with the procedure established in Art 8. Also, permitting “any individual” or “entity” that “considers” information to be illegal could be open to unintended consequences such as mistakes or abuse.

Therefore, we support further legal clarity to ensure that the Art 14 notification truly creates a virtuous collaboration between platforms, commercial and end users to combat illegal goods and content. It is important that the notification ensures immediate action to be taken by the platform to rapidly verify the validity of the notification.

In cases where the platform can identify clearly that indeed the goods or content notified is illegal then it should be acted upon without delay. This responsibility should in no way be abused however and relevant entities should support actions to achieve a safer, more predictable and trusted online environment. Clearly similar and equivalent cases should also be rapidly dealt with, particularly when identified through proactive measures (eg. Art 6).

However, if there is a genuine demonstrable doubt, the platform should have the option to seek assistance for further clarification with a relevant authority. This option should

not be used as a means to curtail obligations expressed within Art 14 or delay immediate investigation by the platform on the receipt of a notification under Art 14. Otherwise, authorities should respond to such requests for assistance from platforms within 5 working days. This would ensure that platforms can follow up with appropriate actions on the basis of "actual knowledge" being clarified in cases where it was not immediately apparent.

Art 14 should not impact the application of Art 6.

Trusted Flaggers:

Art 19 creates the status of a "trusted flagger". Once Art 19(2) obligations are fulfilled and the status approved (Art 19(3)) by the national Digital Service Coordinator, "trusted flaggers" enjoy their Art 14 notifications to be dealt with by digital service providers as a "priority" or "without delay" (Art 19(1)). Clearly similar and equivalent cases should also be rapidly dealt with, including where they can be identified under Art 6.

It is helpful that an authority does a credential check of the applicant under Art 19(2) and approve their status formally. Accuracy is a fundamental qualification. Inaccurate notices would otherwise only put users at risk, distract platforms from acting on valid notices and proactive tasks, overall undermining this process for handling illegal content.

However, we note that application of a "trusted flagger" may not be possible for most businesses (eg. rights holders, brand owners) due to Art 19(2)(b). This needs to be amended so that businesses with a vested interest in operating online can play a role in ensuring the online user experience is safer. Once approved trusted flaggers would notify individual instances of potential illegality directly to the online platform for a decision to be taken immediately without delay or the involvement of any authority.

We highlight support for monitoring "trusted flaggers" as described within Art 19(5) & (6) and propose that Digital Services Coordinators update the trusted flagger lists and share information at European level.

It should be noted that appointment of Digital Services Coordinators should be selected by Member States to carry out their duties under this "trusted flagger" mechanism (eg. approval of status) with clear independence and be granted sufficient funding to ensure the system works efficiently.

Know Your Own Business Customer (KYBC):

We agree that Art 22 should apply to online platforms that allow consumers to conclude distance contracts with 3rd party traders for the sale of goods or provision of services. Online platforms allowing consumers to buy from 3rd party traders should collect information from those traders to identify who they are should issues arise. This would greatly aid traceability for counterfeit or dangerous products and for illegal content.

Art 22 mentions the offer of "services" within this provision, for legal certainty, a specific reference to "content" should clearly be demonstrated to ensure that Art 22 indeed covers online platforms that allow consumers to conclude distance contracts with 3rd party traders in relation to the sale of content alongside products. This would aid the

traceability of counterfeit or dangerous products and illegal content equally, in particular to protect intellectual property.

We caution that not all Member States have national identification documents as referred to in Art 22(1)(b) and verifiability of information provided is not always possible. Further to this, 3rd countries are likely have even more diverse systems. We therefore believe that a passport should be listed in Art 22 as a possibility instead. We also recommend clarifying that the trader should provide all the information required under Article 22 to the online platform (including the information under Article 22(1)(d), given it would be impossible for the online platform to chase information about economic operators down the value chain), and that the online platform should not be held liable for information provided by the trader that ends up being inaccurate.

We are also concerned that these obligations could be avoided by professional sellers if they attempt to present themselves as private sellers. Obligations therefore need strengthening to ensure that these provisions apply to platforms which indeed host professional traders.

Each year unsafe goods are sold to consumers via an online channels without having a market actor to hold responsible. This negatively affects the internal market, competition and exposes consumers to a great risk. The proposed safeguards in the DSA – such as notice-and-take-down – do not effectively protect consumers against this issue as they take place after the dangerous goods have been sold.

We find it important to address this issue, particularly for "high-risk" goods before they are placed on the European market and sold. Therefore, online platforms that: facilitate the sale of harmonised consumer goods; between a seller in a 3rd country and a consumer in the EU; and where there is no other manufacturer or importer in EU, should verify that the product bears the required conformity mark (CE mark) and that it has other relevant documents (eg. EU declaration of conformity). This could be achieved through ensuring that when such business users send other relevant Art 22 information, they simply confirm that these documents are indeed in existence should enforcement activities be needed at a later date.

While the online platform cannot be held responsible for the legality of the product itself, they should be responsible to carry out this basic due diligence to ensure these types of players at least confirm they possess the documents required for any potential enforcement activities by European market surveillance authorities. This due diligence check could be carried out by the online platform only in these specific instances in parallel to collecting the business users traceability details.

Online Advertisement:

Targeted advertising is a form of advertising directed towards an audience with certain traits, based on the product or person the advertiser is promoting. This is a positive tool to ensure benefits for both parties: the recipient receives information that is more meaningful and the advertising company ensures more efficient investment of its resources.

We therefore agree with the need to provide transparency through Art 24 & 30 to clearly identify an advertisement and the business user on whose behalf it is displayed. We also believe it is positive to compile relevant information regarding that advertisement. We understand that the provision of the main parameters to determine the recipient of the

advertisement should be done in a manner that does not interfere with the advertisement itself (eg. appearing instantly upon consumer request). On the other hand, we believe some of the information regarding the advertisement (eg. total number of recipients and the number of targeted recipients) could expose business secrets. It could also be difficult to apply for smaller platforms that simply sell advertising space without collecting the data which the advert uses. Overall, the application of the provisions on the transparency of online advertising must comply with the legislation protecting the trade secret (Directive 943/2016).

Data Access and Scrutiny:

Art 31 rightly permits access to data of very large platforms to enable monitoring to assess compliance of this Regulation. National Digital Service Coordinators and the Commission would both gain access for these specific purposes. However, they would also gain access alongside researchers affiliated to academic institutions, to aid identification of systemic risks (Art 31(2)). In this context, a clearer definition of "vetted researcher" is needed.

ENFORCEMENT

Digital Services Coordinators and the Commission should be granted appropriate powers within Chapter IV to effectively enforce this Regulation, particularly cross-border, we highlight that many Member States market surveillance authorities and other regulators involved with keeping online and offline markets safe are already grossly under resourced. Therefore, we implore Member States to uphold their political intentions and sufficiently fund their authorities and regulators responsible for enforcing existing frameworks and the DSA.

In order to foster harmonisation in the implementation of this Regulation in the Member States, it is necessary support strong alignment between the Commission and national Digital Services Coordinators through promoting guidelines in support of Art 19(7) for: defining criteria for awarding and revoking trusted flaggers but also coordination of the notice & action mechanism (Art 14) and for orders to act against illegal content (Art 8). These guidelines should be issued without delaying the entry into force of this Regulation.

To support legal certainty, we would welcome clarity on the triggers for the exercise of investigation and enforcement powers; the proposed calculation of fines; and safeguards around the provision of commercially sensitive information to authorities. Many of these aspects are left to delegated acts. This clarity will guide oversight bodies and support proportionate regulation. We encourage the Commission to use the new Multi-annual Financial Framework (MFF) to fund modern tools and training on online enforcement techniques for those authorities.

We remain concerned in relation to the potential impact on supply chains regarding powers of investigation under Art 41. More legal certainty is needed for the powers which are granted to authorities to investigate 3rd parties that are in business relations with digital service providers covered under this Regulation. What exactly can these 3rd parties be asked and on what basis? Many 3rd parties will be SMEs, therefore any enforcement measures pursuant to investigations due to mistaken or untimely responses should be proportionate. See, for example, fines mentioned in Art 42(1) which should be a last resort.

We also believe it is disproportionate for Art 59(2) to refer to 3rd parties (which could be a business user or other subject) in order to fine them 1% of turnover for simply unintentionally not giving complete or correct information. Information requested may not always be easy for others in the supply chain to collect and provide. We would therefore suggest deletion of the word “negligently” in Art 59(2) so that fines can only be used for clearly intentional conduct.

We also request a longer application period than 3 months in Art 74 as this will not be a sufficient time for businesses to prepare for such a Regulatory evolution. All relevant business models will need longer to adjust to this new reality. A period of 24 months may be more desirable to put the necessary resources in place.

* * *