Bundesverband E-Commerce und
Versandhandel Deutschland e.V.
www.bevh.org

- Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh) -

Position Paper on the Digital Services Act

Berlin, 15 June 2021

Contact: Alien Mulyk, Manager Public Affairs EU & International, am@bevh.org

Introduction

Since the adoption of the e-Commerce Directive more than 20 years ago, there have been a lot of developments in the digital world in general, in the e-commerce market but also in terms of legislation at EU but also at Member State level. bevh[1] welcomes that the European Commission is taking these developments into account and proposing a harmonised framework for digital services. This will foster legal certainty for businesses and reduce regulatory burden and compliance costs for those operating cross-border within the EU's single market. However, there is need for a balanced approach that does not endanger the delicate infrastructure and synergies that exist between businesses and online marketplace and platforms in the e-commerce market. Especially during the Covid-19 crisis and several lockdowns, selling online allowed particularly SMEs to gain reach and compete at a global level as platforms reduce the barrier to market entry significantly by offering the infrastructure needed to sell online.

In this sense, we welcome that the Digital Services Act (DSA) maintains those principals that were essential to the growth of the digital single market such as the prohibition of a general monitoring obligation, the country-of-origin principle and the notice and action mechanism. However, we would like to highlight the specific implications that the proposed rules would have for the e-commerce sector and where their application could lead to unintended consequences especially for small online retailers.

1. Scope

Generally, we welcome that the horizontal scope of the E-Commerce Directive was maintained in the Digital Services Act proposal. However, it is important to take into account the particularities of each sector as business models and practices of services offered online largely differ. Already in the e-commerce sector, business models reach from price comparison websites to platforms and marketplaces etc. These differences have to be considered when it comes to setting obligations for intermediaries to ensure that they are proportionate to their (technical) capabilities, knowledge, and their role in the value chain. Thus, it needs to be ensured that the provisions in the DSA are principle-based, technology- and channel-neutral and proportionate – also in order to be future-proof.

[1] The German E-Commerce and Distance Selling Association (bevh) represents a dynamically growing membership of large and small distance selling businesses using the internet, catalogues, direct sales and TV as sales channels. The members of bevh represent more than 75% of the total industry turnover in Germany. In addition, more than 130 service providers from the e-commerce sector are affiliated to the association.

a. Legal Consistency

Legal consistency with other legislation containing obligations for online platforms have to be taken into account i.e., the VAT E-commerce Package, the Consumer Rights Directive - as amended by the Omnibus Directive, Market Surveillance Regulation, Platform-to-Business regulation and the Directive on Administrative Cooperation 7. Most of the recently adopted legislation has just entered or still has to enter into application or will soon be revised such as General Product Safety Directive and the Product Liability Directive. Therefore, it should be ensured that there are no overlaps and the DSA should only regulate in these areas if necessary. Where there is no further need for regulation for specific topics and sectors there should be no new provisions.

b. Extraterritoriality

We generally welcome that the proposed rules are applicable to all players active on the European market, no matter where they are based, as this will enhance a level playing field between EU and non-EU businesses. However, it remains unclear how the EU will enforce the provisions in third countries. According to Article 1.3, it is sufficient that a business offers a service to someone having his place of establishment or residence in the EU to fall within the scope of the DSA. This means that an offer by a US merchant on an Indian platform could be concerned, which would require further international agreements to enforce the provisions. Moreover, it should be clarified when exactly services are considered to be offered in the Union (Art. 2 (d)). Within the EU, the targeting to specific Member States is often determined based on an offer of translations or country-specific websites, but in an international context, it remains unclear, when services are specifically offered in the EU. The question is also which entity is offering the service – the intermediary or the one finally having the contract with the end-user. Finally, given the various intermediary services in scope of the DSA and their different forms of engagement with users the terms “significant number of users” and “users” should be further clarified. This is especially important in an e-commerce context, where we have business and end-users when it comes to platforms and online marketplaces.

c. Very Large Online Platforms (VLOPs)

In general, we welcome that the DSA takes a proportionate approach by linking certain obligations only to platforms exceeding certain thresholds such as the “number of active recipients”. However, this distinction is not sufficiently clear in an e-commerce context: someone who is just visiting or browsing a platform without making a purchase cannot be considered to be an active user. This and the fact that according to Art. 25.3 the Commission should lay down in delegated acts a specific methodology for the calculation of the average number of active recipients in the EU, creates legal uncertainty for businesses concerning this threshold. Thus, instead of leaving the definition to delegated acts the term “active recipient” should be clarified in the DSA itself. As the Digital Markets Act Regulation takes a similar approach but uses the concepts of “business user” and “end user” instead, while considering an identical threshold of 45 million users, we would recommend aligning the definitions applied in both legislative proposals. Moreover, besides this quantitative criteria, potential other criteria such as a risk-based approach could be considered.

Finally, in terms of a fair and balanced competition, the additional obligations should not prevent marketplaces from growing and turning into VLOPs.

d. Illegal content

We welcome that the DSA focuses on illegal rather than harmful content. However, we would like to stress that in an e-commerce environment illegal content can only refer to the product listings being on an e-commerce marketplace or platform and not to the product as such. Thus, questions of harm and losses caused by non-compliant products are not and should not be addressed under the DSA as questions of product safety are already subject of other legislation such as General Product Safety Directive and the Product Liability Directive that are currently in the process of being reviewed.

2. Intermediary Liability

The prohibition of a general monitoring obligation together with the country-of-origin principle, by which online providers of goods and services are subject to the law of the Member State in which they are established and not of the Member States where the good or service is accessible, were the main legal preconditions that allowed the digital economy to evolve. They are key for further innovation, investment and growth in the digital sector. Thus, we welcome that these basic principles of the e-commerce directive are maintained in the DSA.

The introduction of a general monitoring obligation would deter actors from opening their infrastructures for third party content and would therefore also prevent new business models from emerging and entering the market. As the infrastructure offered by platforms and marketplaces lowers the market entry barriers especially for SMEs and allows them to gain reach, this would especially be detrimental for smaller companies. In this sense, it is important that this principle is not undermined by Article 5.3. Whereas it is clear that a platform or marketplace has to fulfil the same obligations as a retailer when it is selling the products itself, a marketplace or platform cannot be considered having “authority or control” over a seller only because it sets out the terms and conditions for its use. Moreover, marketplaces and platforms are already obliged to indicate under the New Deal for Consumers and the P2B regulation if they are selling the products themselves or if the good is sold by a third party. The question is what else they are expected to do that “an average and reasonably well-informed consumer” understands who the seller is. If a platform would be automatically held liable because a consumer claims that it was unclear who the seller was, this would undermine the prohibition of a general monitoring obligation.

This equally applies to all proposals that try to oblige platforms to proactively take measures. Such obligations would not only be contradictory to the prohibition of a general monitoring obligation, but also to the Good Samaritan clause. Platforms are already today preventing about 95% of non-compliant products from being published on their website by applying filters on a voluntary basis (i.e., without any prior notice necessary). It is in their own interest that consumers can purchase goods safely from their website and have trust into their services. In so far, the Good Samaritan Principle is important and already applied. But it only works because this does not result in a general liability for illegal product offerings that are potentially not detected.

This also applies to the obligation to notify authorities in case of suspicions of criminal offences (Art. 21). It is crucial to clearly define in which cases "information (is) giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place". Otherwise, as nearly every product can be used to commit a crime, there is a risk that liability is shifted to marketplaces and platforms in unclear cases resulting in legal uncertainty for businesses. Article 9 of the regulation on explosive precursors, (EU) 2019/1148, is defining clearly when there are reasonable grounds for such suspicion. Such specification is needed in the DSA as well.

In general, any liability obligations always need to consider and be proportionate to what the platforms can technically do considering that they can primarily only check the product listings published on their websites.

3. Due Diligence Obligations

a. Notice and Action (Article 14 and 15)

The notice-and-action mechanism remains an essential tool for platforms and marketplaces to be notified and become aware of illegal content and products that are placed on their website by third parties and allows them to consequently take action and remove them. We therefore welcome that the DSA maintains this principle and improves the quality of notices by setting minimum standards such as the indication of the URL address, which will help marketplaces and platforms to identify and remove illegal content even more easily.
However, Article 14.3 suggests that a platform receiving any notice containing the elements laid down in Article 14.2 has already actual knowledge about the notified non-compliance. However, notices sometimes contain various pages that need to be checked and verified after reception – especially because they could also be unjustified and come e.g., from a business user who want to impede a competitor from selling during a certain important period e.g., on Black Friday or Christmas or from a person with no direct experience or expertise on the notified content. In order to make it easier for platforms to verify such notices, it would also be recommendable especially in the area of IP rights to indicate in the notice which IP rights are exactly violated. If legal content is removed or blocked based on an unjustified notice, harm will be done to the seller regardless of sanctions that will be imposed on the unjustified notifier afterwards. We would therefore like to ask the Commission to include a clarification in Article 14 as provided in Recital 22, stating that actual knowledge or awareness is obtained "in so far as those notices are sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and where appropriate act against the allegedly illegal content". It could also be considered to clarify that while Article 5 refers to "actual knowledge of illegal activity or illegal content", this actually refers to alleged illegal content.
It is important for the business user of the platform to know why his offer was removed. Thus, we welcome that Article 15 obliges the platform to state the reasons for the removal of an offering. However, in an e-commerce context, it is unclear whom the "recipient of the service" mentioned in the article refers to as it could mean both - the business user and the end-user. In order to avoid abuse of the notice and action mechanism it has to be ensured that the information on a platform's policy on misuse that has to be included in their terms and conditions can be kept rather

general in order to avoid that this information is abused to circumvent the procedures. Regarding the suspension of user, there is also further clarity needed regarding the definition of manifestly illegal content' and 'frequently' and 'gravity' referred to in Article 20.1 and 20.3. Finally, if a user is suspended multiple times as they frequently and repeatedly provide illegal content, platforms should be free to terminate the services permanently. The restriction, suspension and termination of business users should be aligned with the provisions in the P2B Regulation.

b. Trusted Flaggers (Article 19)

Although platforms are already working with trusted flaggers today, we welcome the introduction of trusted flaggers in the DSA. However, we would like to raise some concerns. As sectors, types of illegal content and business models of platforms vary a lot, it is crucial to involve platforms in the process of appointing such trusted flaggers as they are the ones best placed to judge their expertise and their suitability for this task. It is essential that trusted flaggers are real experts in the different fields of non-compliance as someone with expertise on hate speech may not be equally qualified to flag counterfeit products. Thus, the status of a trusted flagger should be directly linked to a competence in a specific area of infringements e.g., for each of the different IP rights.

However, having to give priority to the notices of trusted flaggers at all times could be problematic. Platforms must still be allowed to prioritize notices according to the type of non-compliance as notices not coming from trusted flaggers can nevertheless be more important if e.g., the type of non-compliance notified is linked to a higher risk.

We would welcome safeguards to be put in place against awarding trusted flagger status to unreliable entities and we underline the importance of transparency in the process of validating these entities in each Member State as officially accepted bodies. Article 19.6 should therefore include a clear procedure on the circumstances in which the trusted flagger status can be revoked, the exact timeframe and on whether there are limits to the number of trusted flaggers. Finally, national administrations should share their official list of trusted flaggers with the other Member States and update them regularly, so that their actions are valid and legitimate when they act at European level.

c. Legal Representatives (Article 11)

We welcome that non-EU based intermediary services need to appoint a legal representative (Art. 11) as this will contribute to a level playing field between EU and non-EU businesses. We welcome that the legal representative needs to be provided with the necessary resources and powers (Art. 11.2) and that it can be held liable for non-compliance with the obligations of the DSA (Art. 11.3). However, it is important to ensure coherence with the Market Surveillance Regulation's concept of economic operator, which has not yet entered into application.

d. Know your Business Customer & Traceability (Article 22)

Most e-commerce platforms and marketplaces already apply the 'know your business customer principle' (KYBC) as it is already an obligation under existing legislation such as the Anti-Money-

Laundering Directive, the Transfer of Funds Regulation and DAC7. Therefore, it needs to be ensured that the KYBC provisions in the DSA are aligned with these existing provisions.

The KYBC principle will enhance transparency, helps marketplaces to prevent misuse and reduce the offering of non-compliant products. However, only the data relevant to identify the seller on a marketplace should be collected in order not to overburden the seller nor the marketplace. Moreover, it is important to clarify who will have access to the different types of data collected: consumers, authorities, business partners etc. In addition, it is unclear what the self-certification process of the business customer entails and how it helps to ensure that sellers are only offering compliant products especially as with the acknowledgement of the terms and conditions of marketplaces sellers already commit to only sell goods compliant with applicable legislation.
The reference to the economic operator in Art. 22.1(d) also needs to be clarified as (1) economic operators under the Market Surveillance Regulation are connected to products rather than sellers (i.e. there is not necessarily only one economic operator per seller), and (2) as certain sellers may have no economic operator at all, either because somebody else is already fulfilling this function or because they do not sell any product falling under the scope of the Market Surveillance Regulation.
In Article 22.4, which requires the online platform to delete the obtained information when the contractual relationship with the trader has ended, it has to be added that the data can only be deleted if no contradicting obligation for data retention exists under the GDPR or other applicable legal obligation that the online platform must comply with.
Finally, the DSA does not specify how these provisions can be enforced towards third country actors. For example, it is unclear how platforms are supposed to check the validity of the data especially when the sellers are based in third countries. Moreover, the relations between third country actors are outside the EU's jurisdiction and the disclosure of such information could be in conflict with national legislation such as in China, which could make the enforcement difficult.

e. Terms & Conditions (Article 12)

As Art. 3 of the P2B Regulation already provides for provisions on terms and conditions, the DSA should be completely aligned with it. Moreover, Article 12 is overly broad as the platforms would have to include "information on ANY policies, procedures and tools" used for content moderation. We caution against the disclosure of such detailed information by platforms as this information could be misused by ill-intentioned actors wanting to sell illegal products or could be taken advantage of by competitors. To ensure that sensitive information and business secrets would not have to be published, a corresponding safeguard should be introduced.

f. Out of court dispute settlements (Article 18)

As the P2B regulation already provides for an 'out of court settlement' (OCC) mechanism, the provisions in the DSA should be aligned with them, making it a voluntary system. This would allow platforms to refuse OOC dispute settlements in case of obvious abuse. Finally, it is unclear if only public bodies qualify as OCC settlement bodies under the DSA. If yes, this provision should also be aligned with the P2B regulation and allow the use of mediators who were already appointed by platforms for this purpose. Finally, we would welcome the introduction of a safeguard allowing parties involved to challenge the certification of the OOC bodies in case there are doubts about

their independence or impartiality. Moreover, the provision that platforms have to "engage, in good faith, with the body selected" is not clear, as online platforms would have the obligation to participate in the settlement process anyway.

g. Algorithms and automated decision making

The DSA includes many requirements for platforms to be transparent about the use of algorithmic and automated decision making (Art. 12.1, 14.6, 15.2(c), 17.5, 23.1(c), 57.2). The right balance has to be found here between providing sufficient transparency and protecting business secrets of online platforms. In this sense, it would also be important that sensitive information such as the average number of active users per month (Art. 23.2) should only have to be made available to the Digital Services Coordinator of Establishment and not to the public in order to avoid market distortions. Regarding recommender systems (Article 29), it should be clarified what a recommender system means in an e-commerce context and how to avoid overlaps with the obligations on ranking in the P2B Regulation and the Consumer Rights Directive.

4. Advertisements to be regulated separately

Although we generally welcome more transparency regarding online advertisements, the DSA is in our opinion not the right place to set further rules at least not as far as commercial advertising of products or services is concerned as this is already sufficiently regulated in the Unfair Commercial Practices Directive.

The provisions in the Commission's proposal seem rather to be aimed at political advertising. In an e-commerce context, the broad definition of advertisements in Article 2 (d) raises the question if a mere promoted product listing would already qualify as an advertisement. It needs to be clarified that such product listing will not fall under the definition of an online advertising in the DSA. In an e-commerce context, the purpose of these additional transparency obligations is unclear as misleading advertisements of products and services are already regulated under the Unfair Commercial Practices Directive. In addition, advertisements on e-commerce marketplaces are in most cases internal advertisements for products and services offered on or by the marketplace itself. When it comes to third party advertisements online e.g., on the website of an online newspaper, often programmatic advertising is used. This means that advertisers purchase a digital advertising space via an intermediary based on pre-determined criteria. In these cases, the advertisements are just displayed passively, i.e., the actual advertiser and the publisher do not have a contractual relationship. Thus, the requested information cannot be provided by publisher. Instead, the advertising intermediary would be better suited to fulfil this obligation, as it has access to the advertiser and the data being used to display the ads. In general, it is important that the obligations laid down in Article 24 to disclose the basis on which an advertisement is shown to an individual does not result in an overburdening of consumers with information. Therefore, this information has to be limited to general statements about algorithms and should not be looking in each individual case in detail. At the same time these transparency obligations about online advertisements seem to be a bit contradictory to Article 5 (c) of the Digital Markets Act that would allow every business user to advertise their own web shop / website / social media

page on the platform via which he or she is selling. This will lead to a situation where the platform cannot control anymore what is advertised on its website.
Meanwhile a debate has evolved about the introduction of a general prohibition of targeted advertising in the DSA. We would like to point out that targeted advertising is not a bad thing per se. It also helps customers to find the products they need e.g., for a dog owner it does not make sense to get shown advertisements for cat food. Moreover, targeted advertisement is not a phenomenon limited to the online world. The advertisements we see in TV or print magazines for examples are also always targeted to a specific audience i.e., the readers of viewers of these media formats. In addition, in stationary retail, when a shop consultant consults a customer on which suit to buy, he or she will also screen the customer and make recommendations based on his or her size, style and the perceived wealth of the customer. To ensure equal treatment of sales channels as propagated by the Commission, everything that would be illegal online based on the DSA also would need to be illegal offline. Thus, these practices would need to be prohibited in stationary shops as well. As we are consequently surrounded by targeted advertising everywhere, the proposal to prohibit targeted advertisement to be shown to minors does equally not make any sense as it would deprive them of the possibility to learn how to deal with it.
Moreover, we would like to highlight that especially SMEs rely on targeted advertising and that its prohibition would have a significant negative effect on their competitiveness with larger economic actors and platforms. Finally, we would like to point out that targeted online advertisement is already regulated by the provisions of data processing laid down in the GDPR and that any potential provisions in the DSA should be fully aligned with it, i.e., targeted advertising should be allowed on all the legal grounds provided for in the GDPR.

5. Enforcement and application

The prerequisite for the functioning of any existing legislative framework or new provisions is their enforcement. Experience has shown that it is essential to ensure the harmonized application of the rules vis-à-vis third country actors, but also to ensure an enforcement level playing field at EU level. In this sense, it is crucial to ensure consistency and harmonisation across Member States when it comes to fines for the same infringements. We would also like to highlight that authorities should always try to help businesses with compliance when it comes to complex legal obligations before imposing a fine. In general, the maximum level of fines as proposed in the DSA is very high and as they are based on turnover it is crucial that the DSA clarifies what ‘annual income or turnover’ (Art. 42) and ‘total turnover’ (Art. 59) refer to, in particular whether it is global or only related to the market where the infringement took place.
To ensure the consistent application across the Union, we generally welcome the establishment of Digital Services Coordinators and the European Board for Digital Services which will contribute to the uniform application of the DSA provisions across the EU. However, it is crucial that the Coordinators have the right skills as platforms and products are very diverse. In addition, contrary to the European Data Protection Board, the European Board for Digital Services should not take a regulatory approach and be transparent concerning its activities and involve stakeholders through consultations and meetings etc.
Finally, as regards the entry into force, we would like to highlight that the proposed changes are far reaching and have great impact on business models. Thus, the proposed entry into force period of 3 months is too short and has to be extended to at least 2 years – similar to the GDPR.