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

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

Position on the Digital Services Act

Berlin, 8 September 2020

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

Introductory remarks

bevh[1] welcomes the opportunity to provide feedback to the European Commission's public consultation on the "Digital Services Act – deepening the internal market and clarifying responsibilities for digital services". As the consultation consists of two parts – one dealing with the potential update of the e-Commerce Directive (ECD) and one dealing with a potential new competition tool, these two topics are also reflected upon in our position paper.

I. Update of the e-Commerce Directive

Although there have been a lot of developments in the e-commerce market, in the digital world in general as well was in legislation since the adoption of the e-Commerce Directive 20 years ago, the fundamental principles of the ECD have to be maintained. However, where appropriate we recommend an update of terms and clarification where the ECD is not up to date anymore with technological and market developments.

1. Basic Principles to be ensured

In general, the revision needs to be future proof, which can be best achieved by applying a principle-based and channel neutral approach. Moreover, 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, P2B regulation etc. Most of the recently adopted legislation has just entered or still has to enter into application. Therefore, the Commission should ensure that there are no overlaps and only regulate if necessary. Where there is no further need for regulation for specific topics and sectors there should be no new provisions. When the Commission decides to become active, it needs to take into account a proportionate, targeted, risk-based approach that carefully differentiates, if and when needed, between the type of service provider and the type of service provided.

[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.

2. Scope

The horizontal scope of the ECD should also be maintained in the Digitals Services Act as it manages to combine horizontally applicable rules with a still differentiated approach taking into account the difference in business models and practices. This is very important as the services offered online already largely differ within one single sector such as e-commerce, where business models reach from price comparison websites, to platforms and marketplaces etc. Therefore, one-size fits all solutions do not really work beyond the basic principles that are applicable horizontally.

Thus, the Commission has to carefully take the differences between the service providers into account concerning their technological architecture, their size and type, when regulating in this area in order to ensure that provision are reasonable and proportionate for the service providers affected.

Moreover, it must be sufficiently clarified that rules are applicable to all players active on the European market in order to ensure a level playing field for EU-based businesses.

3. Country of Origin Principle to be maintained

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, was and still is the prerequisite – especially for SMEs - for cross-border activities that are characteristic of the digital economy. Therefore, this principle constitutes the basis for a functioning digital single market and should be further strengthened especially considering the still existing differences regarding the liability rules in Member States.

4. No General Monitoring Obligation

The prohibition of a general monitoring obligation together with the Country of Origin Principle were the main legal preconditions that allowed the digital economy to evolve. It is also key for further innovation, investment and growth in the digital sector. 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. In this sense, it is also important to ensure that this principle is not undermined with reference to recital 47 of the e-Commerce Directive that allows for monitoring obligations in specific cases. The jurisprudence of the ECJ has clarified that these specific monitoring obligations may only comprise cases where not every uploaded content/offer has to be checked for law infringements for an undetermined period of time.

5. Notice and Take Down Procedures to be Maintained

The notice-and-takedown procedure 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 it. Despite illegal content still being found on the internet, the mechanism has proven to be useful and should therefore be maintained. However, it could be improved where there are deficiencies by eliminating legal uncertainty for businesses for example. Moreover, guidelines could be provided clarifying which conditions a notification has to meet in order to be valid and to be processed by the platforms and what is necessary to avoid the abuse of and flaws in the system. This would allow for a better, faster and more flawless treatment and take down action by the platforms. To be able to successfully delete potentially infringing content, the following information needs to be provided to marketplaces:

- the complainant should be clearly identified and in a legitimate position to send a notification (e.g. market surveillance authority);
- the notification should be made in writing and the complainant should provide adequate information of the specific material alleged to be infringing (i.e. link to the listing);
- it should be sent to an e-mail address or other secure method reserved for this purpose by the service provider;
- it should clearly specify which information or activity the complaint relates to;
- it should include details, including legal ground to demonstrate the unlawful nature of the activity or content in question.

Moreover, there are different rules in different Member States existing today. Therefore, the Commission should carefully assess if a clarification and harmonisation of procedures could lead to a simplification for the economic actors who are active cross-border and to more effective take down procedures. This harmonisation would of course have to be proportionate and take the differences between the types and sizes of economic actors into account.

Concerning the Safety Gate, supervising authorities should step up their efforts in effectively contributing to the database that can be accessed by consumers to check the safety of the product they aim to buy and by digital services and sellers. In the latter case, interoperability has to be ensured. In both cases, it is vital that a minimum level of specificity is provided in the RAPEX notices to enable consumers and digital services to receive actionable information.

In case of a potentially unjustified removal of goods or banning of the seller, the seller has to be able to use a counter-notice procedure - especially when it comes to automated decisions that have been taken incorrectly by algorithms or AI. For this purpose and also in order to show its efforts to fight illegal, unsafe products and counterfeits, the platforms should be transparent about the steps that they have taken to remove the relevant content.

6. Differentiation between Responsibility and Liability of Actors Needed

The differentiation between responsibility and legal liability of the economic operators is essential. The liability privilege of platforms needs to be maintained in order for them to be able to continue to provide an enabling infrastructure for SMEs. However, the Commission should assess in proportion to the size and kind of service provider if it could take on further responsibility. The voluntary assumption of further responsibility within the framework established by the ECD should also always be possible for the platform providers.

In order to ensure the liability privilege, it is recommendable to maintain the basic technical architecture of the ECD that differentiates between active and passive actors (Articles 12-14 ECD). All of these actors can profit from the liability privilege, however under different conditions depending on the type of service they offer. However, where necessary the Commission should update and clarify these terms as well as harmonise the different interpretations of these rules by Member States in a balanced way in order to reduce the burden for businesses when acting cross-border.

However, the liability privilege should not be abused by platforms to evade liability obligations. When a marketplace fails to remove or correct a notified non-compliance in due time, the ECD safe harbor stops to apply and it has to be held liable for its inactivity.

An additional measure that could be taken on the side of platforms is the so called “know-your-business-customer-principle” where platforms and marketplaces check the business identity of their business users. This could potentially be a useful tool to support prosecution and deter fraudsters. However, the introduction of such obligation has to be proportionate also considering the size of the service provider and the kind of service provided. Moreover, there would have to be appropriate safeguards regarding the protection of privacy of lawful and legitimate users. The data to be checked for this purpose has therefore to be limited to the data that is really necessary and sufficient. In an impact assessment, the Commission should explore and assess the advantages and disadvantages of this possibility and if it should be included in the Digital Services Act.

7. ‘Good Samaritan Clause’ needed:

There should be incentives for service providers to voluntarily take proactive measures. Therefore, it should be clarified in a kind of ‘Good Samaritan Clause’ that the liability privilege is still in place when companies act proactively: only because a platform is voluntarily checking products and their compliance with one or more laws it does not mean that they know about the unlawfulness of other offers on their website that they have not (yet) checked for this purpose and also not about all kinds of legal infringements that could potentially be found on their website. Without such clarification and safeguards service providers acting in good faith could be deterred from taking proactive measures to contribute to a safer online environment. Moreover, the ‘Good

Samaritan Clause' would constitute an incentive to further innovate in this area and make even more use of digital technologies to establish future proof and even more effective systems that might even allow to prevent a removed product or seller from simply reappearing one day.

8. Harmonisation and effective enforcement needed:

In order to ensure a level playing field within the EU it is important to address legal fragmentation in so far it is undermining the single market. This should lead to further simplification for companies without creating an extra administrative or regulatory burden for them. Further harmonization will improve legal certainty for businesses who have or wish to establish cross-border activities. In this sense, we would also welcome the Digital Services Act to take the form of a regulation instead of a directive.

The prerequisite for the functioning of any existing legislative framework or new provisions is their enforcement. Experience has shown that national market surveillance (and customs) authorities often lack sufficient financial resources and staffing. Moreover, the collaboration, coordination and interaction among themselves and with stakeholders has to be further promoted in order to ensure the harmonized application of the rules and an enforcement level playing field at EU level.

However, this level playing field has not only to be ensured at EU level, but also with economic actors based in third countries. It has to be ensured that everybody active on the EU market complies with EU rules. Therefore, the capacity of market surveillance and customs authorities to better enforce EU legislation vis-à-vis these operators needs to be strengthened. Besides more resources, they also need more efficient instruments in order to efficiently check products and prevent non-compliant goods from entering the EU market. Thus, the European Commission should assess how better enforcement of EU rules vis-à-vis third country actors could be achieved e.g. by closing the responsibility gaps for third country economic operators or multilateral trade agreements etc. More efficient enforcement will also increase EU consumers' protection.

9. Consumer protection and commercial advertisement to be regulated separately

Consumer protection and transparency are essential to ensure consumers' trust. Recently, a lot of platform related issues such as fake reviews or endorsements and ranking transparency have been regulated in the New Deal for Consumers and the P2B regulation going already beyond the provisions of the ECD. Thus, the Digital Services Act might not be the right place to further update these rules.

Moreover, there is a great interest among service providers to ensure the trust of their users. Therefore, some of them meanwhile offer more information going beyond the legal requirements. However, if further transparency obligations were to be introduced, it must be clear that there must be safeguards that allow companies to keep their business secrets when it comes to

algorithms also to avoid the disclosure of sensitive information that could easily be compromised by hackers to the detriment of consumers.

Concerning online advertising, the DSA is not the right place to set further rules at least not as far as commercial advertising is concerned. Considering the question of political advertisement, the European Commission should carefully assess if the Digital Services Act is the right place to regulate on it.

For all new provisions that will potentially be included in the Digital Services Act, the Commission has to ensure that the Digital Services Act does not create any overlaps or inconsistencies with other already existing legislation in order to ensure legal certainty for businesses.

II. New Competition Tool

Since the advent of the internet, new technologies, commercial practices and business models have been evolving. Thus, there is a need to carefully assess if and how EU competition law has to be updated and adapted to these developments to ensure fair competition in the digital single market. It is clear that it needs to be refined and updated to be fit for today's market reality with a particular view to taking into account the diversity of players involved.

1. Scope:

Digitalisation is not only concerning what is generally considered the 'digital economy'. It is more and more becoming an integral part of value creation in all economic sectors. They all use the internet to distribute their products, embrace new technologies, offer new improved products and services and gain insights from data to better understand the market. Therefore, we would suggest that a change in competition law should not only affect and potentially ringfence businesses of the so-called 'digital economy', but new rules have to be valid and applicable in the same way for all economic actors. However, it is important that differences between the business models and practices of economic actors are taken into account. As an e-commerce association our feedback will mainly focus on the situation in online retail, but already in this sector, actors largely differ in terms of business models such as platforms and marketplaces, price comparison platforms or business practices as paid subscriptions, payments with data, collection of broker fees etc. Thus, in order to ensure a uniform applicability, new provisions need to be principle-based, technology-neutral and future-proof. Moreover, in order to ensure a level playing field also at global level the rules should be applicable and enforceable to all companies who are active on the European market no matter where they are based.

To ensure legal clarity for businesses and consistency in EU competition law, the relationship between Articles 101 and 102 TFEU, the competition proposals that will potentially be brought up in the Digital Services Act and between the potential New Competition Tool need to be carefully assessed and defined so that it remains clear when which tool is applicable. In this sense, it might

also be recommendable to stick to the traditional wording used in EU competition law when describing the potential anticompetitive misconduct of a platform. I.e. instead of introducing new concepts such as “large online platforms” or “gatekeepers” the Commission should stick to the clearly defined concept of “dominance” and “abuse”.

2. Potential ‘Anticompetitive Behaviour’

First of all, it must be clear that companies who successfully seized the opportunities of the digital economy should not be punished for their innovative potential and for having been able to gain a big market and consumer share through convenience, a convincing performance and the adaptation to user needs. Otherwise, this would be detrimental for innovation and investment in the EU and for the EU as an attractive location and market for digital businesses. Moreover, it would also run counter the EU’s desire to create European champions that are able to compete with leading digital companies at global level as it would become more difficult for them to gain scale. From a competition law point of view, there is nothing wrong as such with this capitalization on their innovative potential and assets and gaining e.g. a lot of users or a wide geographical reach.

This also creates advantages for business users: Marketplaces also play an indispensable role for sellers in particular for SMEs especially when trading cross-border as they lower barriers for market entry and allow them to easily gain reach and contribute to an increased offer for consumers. In this sense, platforms / marketplaces and sellers are mutually beneficial for each other and for the competition in the market. However, conflicts between them may arise when the provider of such intermediation infrastructure is at the same time a competitor of the seller using its services. This does not mean that two-sided platforms should be placed under general suspicion – it needs to be carefully assessed if there is any anticompetitive behaviour of a platform/marketplace.

Therefore, there is the need to set some standards to ensure that the behavior of platforms is not preventing or restricting competition e.g. in the areas of self-preferencing, avoidance of organic search results, abuse of business user data relevant for competition, preventing access to performance information, banning competitors from selling on their infrastructure for unjustified reasons or other unfair commercial practices. Especially, the access to data becomes a more and more relevant tool. Competition on the merits however should be allowed also if it involves leveraging data to create a new service in a related market as it is the same as using existing assets of a company to enter new markets. It may be legitimate to impose restrictions to the collection of data where it facilitates collusion or to require sharing it to avoid the elimination of competition. However, privacy rules need to be taken into account and the trust of users/consumers, who shared their data with a particular service provider, must not be undermined by these sharing obligations.

Although vertical integration can have positive effects for business users and consumers alike, problems arise where digital companies offer closed ecosystems where they do not leave a choice

to users to go elsewhere and where they force them to use all their integrated services leaving them basically no chance to compete in the market in another way. For the business user it must be possible to use existing service providers along with new ones and to switch providers (multi-homing). Therefore, in order to avoid that companies get locked in, data portability as provided for in the GDPR and interoperability needs to be ensured so that companies can really make use of this possibility. This includes the setting of standards for the creation of an interface and the ensuring of data quality.

Moreover, there should be transparency in favour of sellers and consumers. But it must be clear that companies must be allowed to protect their business secrets and intellectual property during this process otherwise they will lose their appetite for innovation and investment. The P2B regulation already sets out a couple of requirements and transparency obligations regarding data sharing, ranking criteria and about the platform's terms and conditions. Platforms also need to be transparent about any differentiated treatment between third party and own offers and clarify the use and transfer of data generated on the platforms. An assessment of the functioning of the P2B regulation and the development of the market can thus help to identify which types of business models lead to market failures.

3. Enforcement:

In order to ensure a level playing field within Europe it is essential that competition rules are applied uniformly across the EU. This is particularly important in the digital economy due to the cross-border character of online activities. Otherwise, gold-plating in single Member States would undermine the functioning of the European Digital Single Market. At the same time, it is essential that there is also an enforcement level playing field intra-EU but also towards third county players. This can only be ensured if the enforcement is done by one single entity. In our view, there is no need to create an extra authority for it. The European Commission should continue to fulfil its function as competition authority in the EU as it already does for the 'traditional' cases in competition law. Like this, it can be ensured, that there are no differences in treatment between sectors as all become digitalized. Moreover, decisions are at the crossroads of policy making and purely technical enforcement which makes the Commission the more adequate actor – especially because in competition law the Commission has autonomous decision powers. Transferring them to a new regulatory body that would then have the same powers would be disproportionate. Besides that, the new entity would have to build up the capacities and experience in enforcing competition law that the Commission has already acquired throughout the past years.

4. Ex-ante approach:

There have to be clear rules on when the Commission can take action. In an ex-ante scenario, the Commission would basically be empowered to become active without any concrete anticompetitive misconduct of a company taking place. Thus, there could be a potential risk that the Commission would create cases 'for itself'. However, a company should not have to fear

drastic measures just because of its strong presence on the market or the structure of the market. This could lead to legal uncertainty for businesses, which is detrimental to further development, innovation and investment into the European Digital Single Market and infrastructure and thus to creating convenience and value for consumers. A company also needs to be in a position to defend itself, this right of defense is endangered if the competent authority, in our view the Commission, can act without any violation of rules by the company being found. It needs to be assessed if, where and how market power is really abused before any action is taken. Without already automatically assuming that there is a market failure and that providers of digital infrastructures are automatically abusing their market dominance. Therefore, the Commission should continue to act upon a complaint and a careful assessment of the situation. In this sense, the necessary change in competition law is more about refining the existing rules to address new business models and potentially anticompetitive practices enabled by digitalization than about introducing a new tool that would be applicable ex-ante.

Therefore, instead of artificially separating the blacklist approach from case-by-case decisions, the Commission should stick to the competition tools that are currently in place which is the creation of case groups followed by a case-by-case decision on the anticompetitive conduct for each individual case. This combines the blacklist approach (setting up the case groups) with taking into account the differences between business models and practices of actors involved in the digital economy. One-size-fits all solutions as in mere blacklists would be impossible to apply. Moreover, this combination of both approaches ensures not only that the same rules apply to digital and non-digital actors and that thanks to clearly defined case groups misconduct can be identified easily and quickly, but also that thanks to the case-by-case assessment, the provisions remain flexible enough in order to cope with future developments of business models.