HDE Handelsverband Deutschland

Position Paper

on the EU proposal for a "Regulation on a single market for digital services and amending Directive 2000/31/EC" (Digital Services Act)
COM(2020) 825 final

Status: 19 April 2021

[EU Transparency Register Number: 31200871765-41]

1. Background

For more than 100 years, the German Retail Association (Handelsverband Deutschland - HDE) has been the umbrella organisation of German retail - the third largest economic sector in Germany - with a total of three million employees and an annual turnover of more than 535 billion euros. It represents the concerns and interests of around 300,000 retail companies - from all sectors, locations and company sizes. With 50 million customer contacts daily, the retail trade supplies its customers with the complete range of products - using all sales channels.

On a national and European level, HDE is following with great interest the discussion about new regulations of the responsibility of platforms. German and European platforms find themselves in international competition. Chinese players, such as Shein and AliExpress, as well as platforms like Wish, are growing at great speed in Europe. Tax, customs, product safety, environmental, packaging and waste laws cannot be enforced against them to the same extent as against European players, which is why they enjoy significant competitive advantages. At the same time, there are concerns about the misuse of online service providers to distribute harmful content and products on the Internet.

Against this background, the European Commission has proposed with the Digital Services Act (DSA) a revision of the E-Commerce Directive 2000/31/EC and a far-reaching new regulation of requirements for platforms. This involves the freedom to offer digital services throughout the EU internal market according to the rules of the place of establishment, as well as a far-reaching limitation of liability for user-created content. Building on these principles, the Commission wants to create clearer rules on the obligations of online intermediaries, including non-EU intermediaries operating in the EU, as well as a more effective governance system.

2. Position

In discussing these issues, it is essential to keep in mind the benefits of the system established by the E-Commerce Directive in 2000, in particular the free movement of goods and services in the internal market and the promotion of innovation made possible by the system of limited liability and the prohibition of a general monitoring obligation.

The principle of a conditional liability exemption under the E-Commerce Directive should therefore remain our guiding principle and the "notice and take down" rule accompanying the limited liability system the standard for infringements. We therefore expressly welcome the fact that the Commission's DSA proposal upholds these cornerstones of the digital single market. We also welcome the fact that the scope of application only extends to online intermediaries and that traditional online retailers are not covered by the DSA. The latter are already subject to a wide range of regulations in the areas of product safety, consumer and data protection as well as product liability. At the same time, we are of the opinion that C2C online marketplaces and also closed platforms must be considered separately, in line with a risk-based approach (see in detail under c)).

Handelsverband Deutschland (HDE) e. V. – German Retail Federation
Fabian Fechner | Deputy Head of Office | E-Mail: fechner.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brussels | Tel.: +32 (0) 2 737 03 76 | Fax: +32 (0) 2 230 84 97
www.einzelhandel.de

a) General regulatory approach

The Commission shows many good approaches in its proposal. However, it must be ensured in the further course of the procedure that the new regulatory framework is defined in a technology-neutral and principle-based manner and is applied proportionately. The horizontal framework must be coherently complemented by the sector- or content-specific regulations that already exist (e.g. in the areas of copyright or terrorist content). In this way, the new approach can co-exist with the current rules and provide an overarching framework for Internet accountability, while allowing for rapid adaptation to emerging issues when there is a concrete need for it. Therefore, for all actors already covered by the Omnibus Directive and the P2B Regulation - i.e. online marketplaces - it is of elementary importance that the provisions of the DSA are designed coherently and with the greatest possible consistency with these legal acts in order to avoid unnecessary duplication.

One should also avoid misinterpreting any deficits in the area of enforcement as potential regulatory gaps. In the case of sales via platforms, there is always a (product) responsible, liable manufacturer or retailer, who however may be located in another EU country and cannot be prosecuted with the means available today (see next section). Customs and market surveillance must also be improved in this context.

The responsibility for compliance with consumer law (liability, warranty, information obligations, withdrawal, etc.) is also clearly regulated, not least by the recently adopted Omnibus Directive 2019/2161/EU with regard to each actor - manufacturer, retailer, platform. With regard to the topics of transparency on online marketplaces in general and of rankings in particular, we therefore see no need for further regulation. First, the new obligations for platforms, fulfilment service providers and other players from the Omnibus Directive 2019/2161/EU, the P2B Regulation 2019/1150/EU and the new EU Market Surveillance Regulation 2019/1020/EU should be implemented in practice and then carefully examined for their added value. If, on the other hand, a fundamental change of the current law was to be sought and, for example, a complementary or subsidiary liability for intermediaries was to be introduced, the enforcement problem would merely be shifted from the seller, who cannot be prosecuted, to the platform, which also cannot be prosecuted, in the case of platforms located in other EU countries.

b) Extraterritorial scope

In order to ensure a level playing field, the new legislation must also apply to providers based in countries outside the EU if they offer their services in the internal market, as is already the case with the GDPR, for example. The HDE therefore expressly welcomes the fact that the DSA is to apply to all online intermediary services that are aimed at recipients of these services based in the EU, regardless of where the service itself is based (Art. 1(3)). This means that platforms from EU third countries are also covered by the requirements. In addition, intermediaries that do not have an establishment in the EU but offer services in the EU must appoint a legal representative in a member state (Art. 11), which in our view is a further step in the right direction - especially since the obligations of the legal

representative are comprehensive and he can be held liable for non-compliance with the obligations under the DSA.

However, it is now important to ensure that these requirements do not only exist on paper, but are also effectively implemented in practice. In addition, forum shopping has to be prevented, where Member States compete for the loosest regime for legal representatives through rules of differing strictness or the interpretation thereof, with the aim of having as many companies as possible establish themselves in the country in question.

c) Closed platforms

The Commission has presented the DSA to close potential regulatory gaps that have emerged in the course of digitalisation in order to ensure the provision of secure, digital services in the EU. The DSA aims to minimise new risks. In relation to e-commerce, this can be summarised as clarity about the identity of the retailer, the products offered, the applicable law and modalities for accessing consumer protection rights. Here, technological innovations have created new risks that did not previously exist in brick-and-mortar retail.

However, closed e-commerce platforms essentially continue to function like brick-and-mortar retail shops. Therefore, these new risks, which the DSA is supposed to counteract, do not exist (to the same extent) in closed platforms. Cornerstones of a closed e-commerce platform are, for example:

- No third party access to the platform without individually agreed contracts
- Monitoring, selection and prior approval of all platform sellers
- Quality assurance processes take place before sellers gain access to the platform or before products are offered to consumers.

We therefore advocate that any new obligations targeting potential risks related to the digital business model of an open platform should, in practice, also primarily affect open platforms. Otherwise, the DSA would set up a parallel regulatory structure - with the following consequences:

- Competitive disadvantages for closed platforms
- Excessive administrative burden and use of resources by closed platforms without added value for consumers.
- Destabilisation of existing security systems

We therefore advocate for a differentiated view of closed platforms, as they show clear differences in structures, processes and business models. Some of the obligations provided for in the draft DSA are already inherent in the structure of a closed platform, other obligations would hinder the business model. In particular, the following provisions should take into account the closed platform model in terms of a risk-based regulatory approach (subject to further discussion below):

- Notice-and-action mechanisms (Art. 14): New notification and redress procedures are provided for in the DSA, which address risks that arise because, for example, providers are given free access to the online shelves of open platforms. However, unlike open platforms, closed

platforms, as in bricks-and-mortar retail, already have extensive quality and safety processes in place before each marketplace participant is approved and each product is offered. The existing processes are secure and would be destabilised by new obligations.

- Internal complaints management system (Art. 17): Closed platforms already have comprehensive internal coordination and complaints systems. The implementation of further obligations would mean a considerable additional effort for closed platforms without at the same time - for consumers - recognisable added value and would not be proportionate. Therefore, it should be clarified that existing internal complaints systems at the time of the entry into force of the DSA are sufficient and will be recognised if they meet the objectives of the DSA.
- Know-Your-Business-Customer principle (Art. 22): The same applies to KYBC as the defining element of a closed platform. Without this principle, a closed platform does not work. Article 22 should therefore primarily affect open platforms, ensure consistency with existing systems and thus not impose any additional requirements on closed platforms.

d) Defining illegal content (Art. 2 lit g)

In our view, the definition of illegal content is too broad and vague, thus creating a high degree of legal uncertainty and may lead to unintentional burdens on economic operators who are not actually the intended addressees of a regulation taking up this concept. Article 2 lit g DSA makes a general reference to Union law and the respective national law. A more specific definition of what is to be understood as illegal, dangerous or unsafe, for example, would be welcome, especially in view of the fact that the DSA is ultimately intended to apply in a cross-border context.

In our opinion, diverse digital services naturally pose different risks, each of which must be regulated individually. Therefore, we advocate a clear differentiation between and individual regulation of illegal services, illegal products and other illegal information. Economic operators in the field of e-commerce should not be subject to obligations that are aimed at economic operators in the field of social media and vice versa. Especially for SMEs, an unclearly defined catalogue of obligations would mean a disproportionate administrative burden.

Based on this categorisation, the risks typically emanating from the respective illegal content should be regulated separately and only those audit/compliance obligations should be imposed on economic operators that are necessary to eliminate/mitigate these individual risks.

From a retail perspective, illegal content should primarily be about products that are not in compliance with EU product safety law and therefore pose risks to consumers. The desirable, EU-wide uniform concretisation could be achieved by including a non-exhaustive list with examples in the Annex. This could make a significant contribution to legal certainty for the addressees of this regulation.

e) Tiered obligations and requirements for online platforms

Whenever we develop rules for the platform economy, we need to bear in mind that they will apply at an early stage to many SMEs, start-ups and other companies in the EU. The rules will be relatively more burdensome for these players than for larger companies that have the expertise and resources

to cope with the additional requirements. Moreover, companies outside the EU may already be growing strongly in their home markets and will only have to comply with these rules once they expand into the EU single market, whereas EU companies will have to apply the rules immediately. We must therefore weigh the obligations imposed in the DSA against their cost and benefit and design the legal framework in such a way that European companies nevertheless have the opportunity to become international pioneers in the data and platform economy.

We therefore expressly welcome the fact that the Commission has opted for a multi-level catalogue of obligations and requirements for online platforms, which on the one hand explicitly exempts micro and small enterprises from certain obligations (Article 16) and on the other hand prescribes certain requirements only for very large, systemically important platforms (Article 25). This takes into account a proportionate approach, which must be maintained in the further course of the procedure. Nevertheless, the obligation to prepare an annual transparency report (Art. 13) can also be a bureaucratic challenge for medium-sized companies. This obligation should therefore exist for all companies except VLOPs only at the request of the authorities.

f) Definition of VLOPs

Very Large Online Platforms ("VLOPs") must follow an additional set of specific requirements. These players are defined as online platforms reaching at least 45 million people (average/month) in the EU (Art. 25). In this context, the Commission will be required to propose a methodology for calculating this figure in a delegated act (Art. 25(3)). It should be clearly and comprehensibly defined how these "active users" are counted for the very different business models covered by the DSA. It should be explicitly noted that these must be actual active users who use the platform in question on a permanent or repeated basis and not just once or have become inactive in the meantime.

g) Liability of platforms under consumer protection law (Art. 5(3))

With the draft, the Commission commits itself to the basic principles of the free internet, which it established 20 years ago with the E-Commerce Directive (liability privilege, prohibition of general monitoring obligations, country of origin principle) and retains these basic pillars. However, Article 5(3) deviates from this for online marketplaces: Online platforms that enable consumers to conclude distance contracts (=online marketplaces) are to assume liability under consumer protection law if such an online platform presents the relevant information or facilitates the relevant transaction in such a way that an average and reasonably well-informed consumer can assume that the information or the product or service that is the subject of the transaction is provided either by the online platform itself or by a user acting under the supervision or control of the platform. I.e. if a platform does not convincingly make clear that it is not itself the seller (or controls the seller), it may still be liable under consumer protection law.

We consider this provision to be proportionate, also because it follows previous transparency obligations from the Omnibus Directive 2019/2161/EU. However, in the further course of the legislative procedure, it must be clarified - with legal certainty - what "under their supervision or control" means in

practice. In addition, so far it is unclear which (EU) regulations are to be covered by "consumer protection liability". Does it (only) concern the directives on the sale of goods, unfair commercial practices and consumer rights, or does it also include product safety? This also needs to be clarified conclusively.

At this point, the following should be mentioned: From HDE's perspective, it is appropriate that no further consumer protection provisions have been included in the proposal, as this is not a consumer protection instrument, but an internal market instrument, which should guarantee the offer of digital services in the internal market. The provisions for the protection of consumers - also and especially on platforms and online marketplaces - have just been updated by the Omnibus Directive.

h) Notice and Action Mechanisms (Art. 14 & 15)

Even before the publication of the proposal, HDE had called for formalising and harmonising the 'notice and action'-mechanism across Europe and eliminating the patchwork of rules currently existing in the Member States. Accordingly, HDE supports the intention to transform the E-Commerce Directive into a regulation in order to achieve an even higher degree of harmonisation and to create a common minimum standard for the responsibility of platform operators.

However, one thing is of central importance in this context: when we turn the appropriate screws, we must always be careful to find the right balance and weigh up the interests of operators of online marketplaces and their commercial users. If the hurdles for sales via online marketplaces are set too high, this will in the end also harm the commercial users (including those who already comply with the regulations). Sales via platforms and online marketplaces are the most important entry into online retail for small retailers - also as the increasing (EU) regulation of recent years (GDPR, geo-blocking, PSD2, etc.) has made it very costly and unattractive to set up one's own online shop. Platform retailing must therefore remain a viable and economically sensible path in the future.

The requirements for "notice and action" should therefore be as specific as possible so that platforms can identify the products concerned with certainty and act accordingly. If this is not the case, it will inevitably fall back on the retailers, who would have to reckon with more far-reaching "take downs". Furthermore, we are critical of specific deletion deadlines, as they can quickly overburden small and medium-sized platforms and are not appropriate in every case due to the highly divergent risk. We therefore call for discretionary powers for platforms and authorities in the question of how quickly an illegal content must be removed and would recommend sticking to the wording "without undue delay". Should the legislator consider deletion periods, these should be anchored in sector-specific regulation (as already planned, for example, in the Directive on Terrorist Content) and should only be applicable to notices from authorities.

Finally, we consider the comprehensive reporting obligations of Article 15 to be questionable in their details and disproportionately burdensome, especially for small players. While a large part of the obligations for online marketplaces is already sufficiently regulated by the P2B Regulation, the article seems to be strongly tailored to social media companies. As a result, not only would the retailers have to be fully informed of every blocked product (which is already provided for in the P2B Regulation),

but the user would also have to be informed of every deleted user review. This represents an extreme burden for companies of all sizes - especially since all these processes (which occur millions of times a day) are also to be reported to a central database of the Commission - in addition to the annual transparency report (Art. 13), which raises the compelling question of the concrete added value. We therefore call for online marketplaces to remain at the regulatory level of the P2B Regulation and for Article 15 to be applied only to social media platforms (and the like).

i) Trusted Flaggers (Art. 19)

Platforms (except micro and small ones) must ensure that notices (on illegal content) from so-called "trusted flaggers" are dealt with "without delay" (Art. 19). Trusted flaggers are to be appointed by the competent national enforcement authority ("Digital Services Coordinator") and must meet certain requirements. Platforms are to be protected against abuse through false/excessive notices.

In particular, HDE welcomes the requirement that trusted flaggers must represent collective interests. In our view, however, there is a need for further clarification as to what exactly constitutes a "collective interest". For example, it must be ensured that individual companies, e.g. individual brand manufacturers, cannot be appointed as trusted flaggers. At the same time, the number of trusted flaggers per industry and per member state should also be capped to prevent individual platforms from being completely overwhelmed by complaints. Thus, only qualified institutions should be considered as trusted flaggers, which are adequately equipped in terms of professional and financial resources to carry out their activities as trusted flaggers impartially and free from a profit motive. Trusted flaggers should therefore not develop into an instrument used in competition between companies, but should have as their sole objective to reduce the sale of non-compliant products.

In addition, the question of who is liable for the abuse of the trusted flagger status has not yet been clarified, because there is no provision that abusive blocking requests must also have consequences under liability law and oblige compensation for the resulting damage. Platform operators must have the possibility to refer to the trusted flagger if a deletion or blocking subsequently turns out to be unjustified and the provider concerned has suffered damage as a result. Furthermore, it should be ensured that forum shopping is avoided and that the requirements for and controls of trusted flaggers reach the same high level in all Member States.

j) Know Your Business Customer principle (Art. 22)

Operators of online marketplaces (with the exception of small/micro businesses and B2B platforms) must request certain information from sellers who wish to offer goods or services for sale, such as name, address, ID, bank details and commercial register entry (so-called Know Your Business Customer principle, or KYBC for short, Art. 22). In the case of providers from EU third countries, the information of the so-called "responsible economic operator" according to the new EU Market Surveillance Regulation 2019/1020/EU must also be requested, which we expressly welcome as a further element for the creation of fair competitive conditions. The platform must make "reasonable efforts" to verify the data received by cross-checking with publicly available sources ("freely accessible official online databases") and allow retailers to correct incorrect or incomplete data.

The same applies here as under g) above: It must be ensured that these processes are both feasible for platforms of all sizes - which is why we support the Article 16 exemption - and that they are manageable for the retailers concerned. It should therefore be more clearly regulated which obligations for verification are reasonable for marketplace operators, because the verification must not be unduly burdensome. In most cases, the platform operators could pass on the obligation to provide and verify the information to the suppliers, which in turn leads to additional effort and a further hurdle for them when selling online. It is therefore important to keep this hurdle as low as possible, which we believe is (just) achieved with the proposed rules.

However, the added value of self-certification (Art. 22(1f)) is questionable and in practice is merely a burden for the retailer, with no discernible added value for consumers. Regardless of any certification, a retailer is in any case legally obliged to offer only products that comply with EU law. The passage should be deleted.

k) Supervision and enforcement (Art. 38 et seq.)

Already in our original position on the DSA, we rejected the idea of creating a central, European supervisory authority to enforce the new DSA rules. Nevertheless, uniform enforcement remains the decisive factor for the success of the DSA. Enforcement should therefore be harmonised and improved through closer networking of the existing supervisory authorities, analogous to the developments in the area of data and consumer protection, or market surveillance. In this way, legal certainty and uniformity in the application of the law can be meaningfully guaranteed for companies operating throughout the EU.

The Commission has largely followed this position by proposing to empower the existing national regulatory authorities, as " Digital Services Coordinators", both to monitor compliance with the regulations and to impose potential fines if companies violate their obligations. They will be supported by the Commission and a new "European Digital Services Board" (Art. 47). On this basis, the right course must now be set so that the national supervisory authorities can effectively ensure that national and European regulations are also effectively observed. Competitive advantages due to a different location of the digital service provider on the national market can be effectively excluded in this way.

However, for the supervision and monitoring of very large online platforms, the Commission is separately responsible as an enforcement authority and can act on its own initiative (Art. 50 et seq.). The question here is how the competences of the Commission are delimited from those of the national authorities and where the dividing line between the respective competences runs.

l) Further points

- Good Samaritan Principle: We support that voluntary activities by providers of intermediary services to remove illegal content should not lead to a loss of the liability exemption (Art. 6). In principle, positive incentives should be set and proactive measures by the platform operators should be encouraged.
- Applicability: Article 74 provides for a transitional period of only three months until the regulations are to be applied by the companies concerned. This is decidedly too short and is not sufficient to

operationally implement the comprehensive and complex obligations, especially since small companies are also affected by numerous requirements. In the P2B Regulation, which in comparison deals with transparency and information obligations that are much easier to implement, a transition period of 12 months was provided for. The period should therefore be extended to at least 12 months. In order to ensure an effective implementation of the DSA, we plead for a flexible deadline. Implementation periods for individual provisions, which still have to be substantiated by secondary legislation, should start when the secondary legislation is actually adopted. This guarantees all economic operators the implementation period that the legislator with good reason originally envisaged.

- Fines: The fines for infringements are set by the Member States, but the proposed regulation sets an upper limit of 6 percent of the annual turnover (Art. 42). We consider these fines to be disproportionate and plead for them to be adapted to the level of the Omnibus Directive in consumer law and thus to be reduced to 4 percent of the annual turnover. Moreover, the percentage fines should only relate to the turnover generated by the platform activity of a company. Fines of up to 1 percent of annual revenue are to be imposed for providing "incorrect, incomplete or misleading information" or for failing to carry out an on-site inspection, for example. These fines can be imposed not only on platforms but also on "other persons" who are required to provide information in the context of a breach of the regulations, e.g. platform retailers (Art. 52 (1) in conjunction with Art. 59 (2)). Due to the heavy burden that a turnover-based fine can represent for (small) online retailers, we call for this maximum penalty to be applied only after several opportunities for rectification and in strict compliance with the principle of proportionality. Finally, we would welcome if Member States were obliged to issue guidelines on the justification and determination of sanctions in order to create additional clarity and legal certainty.
- Transparency of online advertising (Art. 24 & 29): Transparency obligations for online advertising should be proportionate and achievable in practice. Here, too, the rules should be in line with existing EU legislation that already deals with similar constellations. In principle, the topic of "profiling" or individualised online advertising is conclusively regulated in the General Data Protection Regulation and the future ePrivacy Regulation. Therefore, we see no need to take up this issue again here and to re-regulate it quasi-sectorally. Under no circumstances, however, should this provision be extended to platforms of all sizes or even to pure online retailers. Rather, the DSA should be limited to questions of political advertising, provided that there are concrete dangers to democracy and this is not already regulated in other legal acts.
- Transparency and reporting obligations (Art. 23): The obligations from this article, which go beyond Article 13, are disproportionately burdensome for platforms of any size. They also go significantly further than those from Article 11(4) of the P2B Regulation. Therefore, this information should only have to be provided upon request by the competent authority. Under no circumstances, however, should these obligations be extended to platforms of all sizes or even to pure online retailers.
- Out-of-court dispute resolution (Art. 18): Out-of-court dispute resolution is already regulated in a number of EU laws that overlap with the DSA, such as the P2B Regulation. It is not clear whether additional dispute resolution mechanisms are needed. We urge the Commission to harmonise these requirements, as well as ODR and ADR bodies for business-to-consumer disputes.

- In addition to an appropriate responsibility of online platforms, HDE also demands that the physical entry of parcels into the EU internal market be addressed and calls for a better control of shipments from third countries to individual consumers by customs authorities. Regardless of whether retailers from third countries use the services of European fulfilment service providers for the storage and shipment of their goods, the goods must be inspected by customs when they are imported from third countries. In our opinion, the capacities for this should be increased. Only customs has direct access to the goods when they are shipped directly to EU consumers by sellers from third countries and can withdraw them from circulation if they are defective. This is where controls are most effective. In the view of HDE, equipping customs authorities with the necessary resources for this task are of great importance for consumer protection and the strengthening of competition.

3. Conclusion

The EU Commission has refrained from comprehensive platform liability in the DSA proposal in line with HDE's demand. The notice-and-action principle remains the guiding principle for infringements. At the same time, binding requirements are imposed on various groups of platform operators in a graduated manner, which address the central problem of offering unsafe products (especially from outside the EU) on the internal market. We welcome this, as well as the relative relief for small intermediaries and the fact that providers and platforms from non-EU countries are explicitly taken into account. However, concrete requirements must now be thoroughly checked for their practicability and adapted if necessary.

The following points are of central importance to us:

- There is a need for differentiated and appropriate regulation depending on the risk, size, influence and type of platform (open/closed). We therefore support the fact that the Commission has opted for a multi-level catalogue of obligations and requirements for online platforms, which on the one hand explicitly exempts micro and small enterprises from certain obligations and on the other hand prescribes certain requirements only for very large platforms. This takes into account a proportionate approach, which must be maintained in the further course of the procedure.
- In this context, we also advocate a distinction between closed and open platforms, as these show clear differences in structures, processes and business models. Some of the obligations provided for in the draft DSA are already inherent in the structure of a closed platform, other obligations would hinder the business model.
- HDE welcomes the fact that the DSA is to apply to all online platforms aimed at users in the EU, regardless of where the service itself is located. This means that platforms from EU third countries are also covered by the requirements. However, it is now necessary to ensure that these requirements are also effectively implemented in practice. In addition, forum shopping between Member States must be prevented.

Handelsverband Deutschland (HDE) e. V. – German Retail Federation
Fabian Fechner | Deputy Head of Office | E-Mail: fechner.europa@hde.de
Avenue des Nerviens 85 | B-1040 Brussels | Tel.: +32 (0) 2 737 03 76 | Fax: +32 (0) 2 230 84 97
www.einzelhandel.de

- The definition of illegal content is too broad and vague. A narrower specification of what is to be understood as illegal, dangerous or unsafe would be welcome. From the point of view of retail, illegal content should primarily concern products that do not comply with EU product safety law and therefore pose a risk to the consumer.
- Particularly with regard to notice-and-action and KYBC, attention must be paid to the following: When the legislator turns certain screws, care must always be taken to find an appropriate balance of interests between operators of online marketplaces and their commercial users. If the hurdles for sales via online marketplaces are set too high, this will ultimately also harm commercial users (including those who already comply with the rules).
- We are critical of concrete deletion periods, as they can quickly overburden small and medium-sized platforms and are not appropriate in every case due to the strongly diverging risk. We therefore call for discretionary leeway in the question of how quickly an illegal content must be removed and recommend sticking to the wording "without undue delay".
- We consider the comprehensive reporting obligations in Article 15 to be inappropriate and therefore call for online marketplaces to remain at the regulatory level of the P2B Regulation and for Article 15 to be applied only to social media platforms (and the like).
- In the methodology for calculating the users of VLOPs, it should be noted that these must be actually active users who use the platform in question permanently or repeatedly and not only once or have become inactive in the meantime.
- Trusted flaggers must actually represent verifiable, collective interests. Accordingly, it must be ensured that individual companies are not appointed as trusted flaggers. Thus, only qualified institutions that carry out their activities impartially and free of profit motives should be considered as trusted flaggers.
- Platform operators must have the possibility to refer to trusted flagger if a deletion or blocking turns out to be unjustified afterwards and the provider concerned has suffered damage as a result. In addition, it must be ensured that forum shopping regarding the trusted flagger status between Member States is avoided.
- The maximum fine of up to 6 percent of the total annual turnover foreseen for DSA infringements is disproportionate in view of the risks associated with an infringement. Furthermore, we would welcome it if Member States were obliged to issue guidelines on the justification and determination of sanctions in order to create additional legal certainty.
- The transitional period from the entry into force of the Regulation to its applicability should be extended to at least 12 months. Implementation periods for individual provisions that still have to be specified by secondary legislation should only begin once the secondary legislation has actually been adopted.