EuroCommerce for retail & wholesale

Position Paper
1 June 2021

Ensuring a safe and trustworthy online environment for consumers & a level playing field for businesses

EuroCommerce believes the EU legal framework for a digital single market should:

(i) ensure high consumer trust;
(ii) provide legal certainty for all market players irrespective of which sales channels they use to offer their services;
(iii) ensure balanced responsibilities for all market players depending on their position in the supply chain; and
(iv) create a level playing field for all businesses that offer products to EU consumers wherever they are established.

Key recommendations

One framework for online services	EuroCommerce supports one horizontal framework for all online services targeted at EU based consumers.
Liability	Consumers should always be able to exercise their rights, and in conjunction with other EU law, competent authorities should always be able to identify the economic operator in the EU that is responsible for EU product safety law and liable for consumer protection law.
Know Your Business Customer	EuroCommerce supports the Know Your Business Customer principle, but more clarification is needed in Article 22.
Transparency obligations	More transparency is welcome, but we need to ensure legal consistency, that the burden is manageable, that business secrets are respected and this will really contribute to compliance and trust.
Notice & Action	EuroCommerce supports a strongly harmonised notice & action system across the EU. This will make it easier for cross-border operators.
Number of active users	The calculating methodology should be part of the DSA and aligned with the DMA
Enforcement	EuroCommerce supports efficient and effective enforcement, including the introduction of a legal representative and the country of origin, but is concerned about the high turnover-based fines and the proportionality of the Commission's enforcement powers
Codes of Conduct	It should be clear that codes of conduct are voluntary instrument
Application date	Online marketplaces need at least 12 months to implement all the new DSA requirements.

Contact:
Ilya Bruggeman - +32 2 738 06 41 -bruggeman@eurocommerce.eu

Transparency Register ID: 84973761187-60

Introduction

The European retail and wholesale sector is in the middle of a digital transformation. This is immensely accelerated by the **COVID19 pandemic**. Numerous consumers had or have to buy their non-food products online because stores were closed, but also online food sales are soaring and this will remain so a recent McKinsey-EuroCommerce study revealed.[1] Many retailers and wholesalers that did not have an online web shop, had to start offering their products online to be able to reach customers again while in lockdown. Often, online marketplaces were the only way to go online quickly for SMEs and this is expected to increase in the near future.

The digital transformation is fundamentally changing retail and wholesale business models, it changes the interaction with customers, marketing, it changes the supply chain itself, the information flowing through the supply chain and much more. The sector traditionally is a reseller of products, but is becoming more and more a mixture of support services around reselling, a leading generator and processor of data and an important user of AI. This is essential to respond to consumer demand and provide more relevant personalised offers. Businesses are developing a wide diversity of platforms or becoming one themselves. Many businesses are selling across multiple platforms as well as through their own digital and physical channels. This is contributing to an increased competition between the different online business models. While policy makers are still talking about online and offline sales, the most successful businesses are seamlessly integrating the online and offline environment into omnichannel, thereby offering consumers one experience. Consumers can for example search, buy and return products in any way they want.

Digitalisation is creating new opportunities and driving transformational change in supply chains by increasing efficiency, transparency and competition. In the retail and wholesale eco-system, digital increases choice, efficiency and sustainability and helps create new jobs. To remain competitive in a challenging environment, retailers and wholesalers **need a legal framework that gives them legal certainty and incentives to grow and invest in robust omnichannel strategies**.

In this context, the main focus of our sector regarding the Digital Services Act (DSA) is on the role and responsibilities of online marketplaces via which products are offered to consumers. Our focus is twofold: **many retailers and wholesalers are users of platforms, but also many are (becoming) one themselves.**

One of the main challenges our sector is facing is the **lack of a level playing field with third country traders**. Regularly media reports that products offered online by third country traders are non-compliant and even unsafe or dangerous products produced outside of the EU. This creates unfair competition with EU based traders that comply with EU rules that require that the products consumers buy are safe and consumer rights are respected. The problem is exacerbated by failing market surveillance and customs controls, topped by high compliance costs for law-abiding traders. For consumers, it is difficult to withstand the temptation of lower prices, and research shows that consumers increasingly buy from outside the EU. One study from 2020 suggests that almost 70% of EU consumers that buy cross-border have purchased products offered from China, a figure that was at about 15% in 2014.[2] Therefore, we welcome the Commission's proposal to tackle illegal online content and encourage the Commission to collect more data about non-compliant products sold in the EU that will support more targeted policy options.

Harmonised framework for innovation & growth needed

EuroCommerce strongly supports further integration and harmonisation of the EU Single Market. This is not only an exclusive European process. The Single Market is the EU's greatest economic asset but it is also competing with other economic giants like the US and China. Over the years, we have seen that more and more innovative digital formats and technologies are created there. The EU and the Member States have to step up their efforts to create the right framework in which companies can compete, innovate and serve their customers. The best way to do that, is by ensuring it is more attractive to invest and do businesses in the EU than elsewhere in the world.

[1] *Disruption & Uncertainty, The State of Grocery Retail 2021, Europe*, McKinsey & EuroCommerce

[2] E-commerce in Europe 2020, Postnord

Unfortunately, we still see that individual Member States think they can compete with the rest of the world or act unilaterally within the EU context. That this attitude is not paying off becomes clear when we look at the origin of the top 10 retailers in the world. In 2013 5 retailers were from Europe and 5 were from the US, [3] but in 2018 only 3 were from European and 7 from the US. [4] From the top 10 online marketplaces in the world in 2020, there were no European players, 4 were from the US, 3 from China, 2 from Japan and 1 from South America. The first EU platform is Allegro on number 15, which is mainly serving the Polish market.[5]

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. Transparency and reporting obligations will be relatively more burdensome for smaller businesses than for larger businesses who often have more expertise and resources to comply with additional obligations. Moreover, companies outside the EU may already be growing strongly in their home markets and there they may have to comply with less strict rules before expanding into the EU single market, whereas EU companies will have to apply the rules form the start. These rules will also impact the traders use of platform services, the cost, uncertainties, and frictions that traders will experience and ability to grow. We therefore have to strike the right balance in the DSA. We strongly urge EU policy makers to keep an open mind and look beyond the EU context, and help EU based companies grow and become international pioneers of the data and platform economy, and be globally competitive. This will ensure in the long run most opportunities for more growth, jobs and increasing consumer choice.

The EU market knows a wide diversity of online marketplaces that all operate in their own way; some marketplaces have stricter rules about giving access to their services by third-party traders than others which also effects the level or risk for consumers. This also means online marketplaces have different measures in place to ensure third-party traders are eligible and the products and services offered are safe and compliant with EU and national law. This relates to the conditions third-party traders must meet to get access to the marketplace, conditions and level of detail in contracts, the monitoring and selection of third-party traders, quality assurances processes, and compliance checks of products. We suggest taking this into account in the upcoming debates.

In this context, the Digital Services Act should become an effective and efficient instrument that helps **ensuring that the products offered for sale online are compliant** and that in case of non-compliance EU consumers can exercise their consumer rights.

However, the **DSA is just one piece of the puzzle**, and in conjunction with other EU law competent authorities should always be able to identify the economic operator in the EU that is responsible for **EU product safety law** and liable for **consumer protection law**. Other EU legislation that is instrumental is the effective implementation and application of the Market Surveillance Regulation (EU) 2019/1020, the Omnibus Directive (EU) 2019/2161, Sale of Goods Directive (EU) 2019/771, Platform to Business Regulation (EU) 2019/1150, the execution of the Customs Union Action Plan COM(2020) 581 final (including Import Control System 2 (ICS2)), and the revision of the General Product Safety Directive 2001/95/EC, the New Legislative Framework and the Product Liability Directive 85/374/EEC.

All these different pieces of legislation need to be aligned and properly enforced, in order to provide the right conditions for businesses to innovate and grow in the EU.

Below, we provide our comments and recommendations on the specific DSA provisions in more detail.

Scope

EuroCommerce supports that the DSA will apply to all intermediary services provided to EU based consumers. This provides additional clarity on whether online product offers by third country traders or via marketplaces are covered. Furthermore, we consider it positive that the scope of application only extends to intermediary services providers and not to all online service providers (including online traders). 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.

[3] Global Powers of Retailing 2015, Deloitte
[4] Global Powers of Retailing 2020, Deloitte
[5] The World's Top Online Marketplaces 2020, webretailer.com (figures are pre COVID)

Illegal Content

In our view, the definition of illegal content in Article 2(g) is quite vague, which will create legal uncertainty for businesses and may lead to unintended consequences for businesses, especially when operating cross-border. A more detailed definition of what is e.g., illegal, dangerous or unsafe would be welcome.

Digital services are very diverse and may pose different risks and solutions. We suggest maintaining a horizontal approach via the DSA, but have a differentiated approach between illegal services, illegal products and other illegal information where these obligations clearly diverge. Online marketplaces should not be subject to obligations that are primarily targeted for social media platforms to meet and vice versa.

Liability online marketplaces

EuroCommerce welcomes the codification of case law of the Court of Justice of the European Union in Article 5(3) and supports to maintain the general liability exemption from the eCommerce Directive in Article 5 of the DSA.

However, it is unlikely that the latter will help competent authorities to enforce, or consumers to find redress in all cases of non-compliance where an online trader or marketplace is established outside of the EU. We suggest clarifying further what "under their authority or control" means in practice and clarifying what is covered by "consumer protection liability".

Finally, it is unclear how Article 5(3) would be enforced where there is a legal representative as foreseen in Article 11. EuroCommerce members believe the DSA is an improvement, but some consider this the minimum required or insufficient to restore the level playing field with third country traders and marketplaces. Options to address the issue further via the DSA vary, but it is clear that the DSA should be in sync with other relevant EU law and upcoming revisions.

Know Your Business Customer

Article 22 -Traceability of traders

EuroCommerce supports the idea behind Article 22 to ensure that traders using online marketplaces can always be traced back when necessary. Especially in the case of third country traders this will help consumers to get redress and competent authorities to identify a real and contactable entity in the form of the trader to resolve or address a non-compliance.

However, from our perspective, it should be clarified:

- which information will really help effectively identify and find/contact the trader;
- which information is meant for and useful to consumers;
- which information is meant for and useful to authorities;
- which information is considered public and which is for authorities only, including that information for authorities is not meant to be shared with other traders;
- what does self-certification mean and whether incorrect self-certification by the trader would have consequences;
- whether Article 22 is GDPR compliant;
- what would be the reporting procedure in case a consumer thinks the information is incorrect.

The traceability requirements should be feasible and not unduly burdensome to platforms of all sizes.

In addition, the added value of self-certification (Art. 22(1)(f)) seems questionable and in practice may just pose an unnecessary burden. All traders targeting EU consumers need to compliant with EU law.

Another important question is how would this in practice be enforced in case of third country marketplaces.

Transparency obligations

The DSA introduces many new and tough transparency obligations for all intermediary services providers, for terms & conditions, notice & action, advertising, use of algorithmic / automated decision making and recommender systems. These will likely create high administrative burdens and costs.

The main question is what the purpose is of collecting this information and making it public, available to authorities and researchers. Will others use this information to increase the safety and rights of online users or will most of the information be ignored or misused? What will competitors do with all this information, and will this force platforms to (partially) disclose business secrets and will this be GDPR compliant? Shouldn't the principle of data minimisation be applied? Will enforcement authorities really examine all the data available in search of non-compliance with the DSA?

EuroCommerce supports greater transparency, but obliging companies to publish or give access to data without justifying why this data should be disclosed, how this data will be used and contribute to better compliance seems disproportionate.

Article 12 – Terms & Conditions

The term 'any policy' is very broad and this could oblige companies to publish business secrets that could be used by competitors and abused by actors with mal intentions. This article should be aligned with Article 3 of the P2B Regulation.[6]

Article 13 – Transparency reporting obligations for providers of intermediary services

See article below

Article 23 – Transparency reporting obligations for providers of online platforms

For both article 13 and 23: what is the purpose of making this information public, will it reduce non-compliance and how? For what and by whom will it be used? Will the reports be public or are the reports meant for the Commission and competent authorities?

Regarding Article 23, the Digital Services Coordinators (DSCs) have too much discretionary power: '*…may require the online platform to provide additional information as regards the calculation referred to in that paragraph,* ***including explanations and substantiations in respect of the data used***'. In the absence, of any details of the calculation of the 'average monthly active recipients' this is too widely formulated, and it should not give DSCs the possibility to demand access to sensitive business data without a reasoned request.

Ensure alignment with Article 4 of the P2B Regulation.

Article 15 – Statement of reasons.

The requirements in this article are very detailed and prescriptive. This will impose a high administrative burden on platforms. It is questionable whether such a long and detailed explanation is necessary for every decision to remove or disable access to online content. Especially, considering online product offerings where it is obvious that the online offering is illegal or where this happens on request of a competent authority.

As we understand, larger platforms take millions of times a year decisions to remove illegal content and the obligation to provide every time such detailed explanations will generate huge amount of data. It is unclear why this information should be made public by the Commission, what the purpose is for publication, what will be done with this information, and if this can be done in a GDPR compliant way. In addition, the emphasis is strongly on the service recipient that is suspected of illegal behaviour or at least not in line with the terms & conditions, and does not take into account the burden for platforms.

[6] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services

Such detailed information may also provide actors with mal intent insights in how to circumvent the safeguards put in place to prevent illegal content from being uploaded and play the system. This would have the opposite effect of what the DSA is trying to accomplish.

We suggest alignment with Article 4 of the P2B Regulation.

More on article 15 here.

Article 24 & 30 about online advertising transparency

Both articles will be very burdensome for platforms, and the level of detail may force platforms to publish sensitive data which could distort competition due to other companies (ab)using the information to their own benefit. It is again not clarified what the purpose is of forcing platforms to be transparent and who should use it for what. Some information may be relevant to competent authorities but not to the wider public.

From a general point of view, we understand that having more transparency regarding political advertising may be useful, but it is unclear what the purpose is regarding online products and services advertisements, and why all types of platforms (except micro and small enterprises) are covered. These are simply marketing and promotion tools to draw consumers attention, and the level of risk for consumers seems fairly low. The Unfair Commercial Practices Directive 2005/29/EC already provides a clear framework for assessment and enforcement in case of misleading advertising of products and services. Therefore, we suggest to either specify what type of advertisement is deemed to be of high risk to platform users and would require additional transparency requirements or what type of advertisement is considered low risk and should not be covered by additional transparency provisions.

Following recent debate on profiling and personalised advertising, this is already regulated in e.g., the GDPR and even further in the future ePrivacy Regulation. Consumers also benefit from targeted advertising for products by being offered the products they want. New obligations will likely only create costs and the benefits to consumers of such new obligations are opaque.

Article 31 – Data access and scrutiny

We question whether the Commissions should regulate the conditions under which researchers get access to business data and the technical conditions of how this information should be disclosed.

Transparency requirements regarding use of algorithmic / automated decision making & recommender system: Articles 12(1), 14(6), 15(2)c, 17(5), 23(1)c, 29, 57(2)

There are a lot of requirements in the DSA proposal for platforms to be more transparent about the use of algorithmic and automated decision making. This reflects the current public debate, where the use of these technologies is under scrutiny. However, in the context of the DSA proposal, we should strike the right balance between the interest of platforms and users. Algorithms are commercially valuable technologies and too much transparency should not lead to competitors taking advantage of that.

Notice & action, incl. remedies, orders, trusted flaggers

EuroCommerce supports the harmonised approach for content moderation taken by the Commission. It will remove the current patchwork of different national rules and approaches across the EU. However, on certain elements we would ask for further clarification or improvement.

Article 14 – Notice and action mechanisms

EuroCommerce welcomes harmonisation of what elements should be in a notice. Currently, platforms and retailers have sometimes difficulty to identify the notified content properly, thus making it more difficult or impossible to act.

By making it easier to notify we may expect a much higher rate of notices. This will improve safety and compliance but may also make it more difficult for platforms to process all notices properly. The use of automated decision-making will likely become unavoidable, and it may become difficult for platforms to use actual knowledge they have about what has been notified. Notice and action requirements should therefore be as specific as possible ensuring that platforms can identify the relevant products without doubt and act accordingly.

Furthermore, deadlines should remain workable also taking into account size. We therefore suggest that platforms and authorities have a certain level of discretion in assessing how quickly illegal content must be removed and recommends maintaining the wording "without undue delay". The time within which illegal content should be deleted, should be specified in sector-specific regulation (as already planned, for example, in the Directive on Terrorist Content) and should only be applicable to notices from authorities.

Additionally, it is unclear how a platform should act on a notice about illegal content that is not illegal in the country of establishment or residence of the platform, or in case of an EU trader the Member State of establishment, especially in the case of highly regulated goods like alcohol, non-prescription medicine, products that may require a specific certification for sale in a country, as well as language requirements.

Article 15 – statement of reasons

We support a harmonised approach regarding the statement of reasons. However, if the number of notices will go up the number of statements will go up to. This may lead to a massive increase of data to handle and may make it difficult for the recipient of the statement to exercise its rights.

Article 16 – exclusion for micro and small enterprises

EuroCommerce does not object against this exemption, but does question why for instance a micro or small enterprise should not notify a suspicion of a criminal offence. We do support that micro and small enterprises are exempt from burdensome reporting obligations, but in general rules regarding e.g. safety, environmental protection and consumer protection should remain applicable, including notification of suspicions of criminal offences. In addition, small platforms may have a wide reach and impact, and that in those cases it may be meaningful to have the possibility to impose similar obligations as on other platforms. In order words, linking risks or exemptions to only the number of employees and turnover may not prove sufficient, but linking it to scalability of the online services may prove more useful.

Article 17 – Internal complaint-handling mechanism

An effective and efficient complaint-handling mechanism is essential, and something that is often already provided for by many platforms. This is already a prerequisite in Article 4 and 11 of the P2B Regulation. It is unclear why the Commission already thinks that this Regulation that turned applicable on 12 July 2020 is inadequate for the P2B relationship.

Article 18 – Out-of-court dispute settlement

In national and EU consumer law already different forms of well-functioning out-of-court dispute settlement mechanisms are foreseen, such as in the P2B Regulation. It is not clear whether additional dispute resolution mechanisms are needed and it seems that already in several cases the system proposed is not compatible with existing systems.[7]It will be confusing to consumers to have a separate system for online marketplaces. Instead, we suggest bringing the proposed system in line with existing well-functioning systems and ensure alignment with the EU Directives on ADR and ODR. In addition, costs may become very high, certainly in cases where lawyers are involved and platforms seem to be carrying the highest cost burden. Experience shows, that introducing a small and proportionate entry fee to reduce abuse may be appropriate.

[7] In Denmark consumers can submit complaints for a small fee (DKK 100) to the 'Centre for Complaint Resolution and the Consumer Complaints Board'. The system is already in place for 40 years.

Article 19 – Trusted flaggers

EuroCommerce understands why the Commission proposed to formalise trusted flaggers but fear the system may not be scalable as proposed and might incite abuse. While the main focus of our members is on ensuring a safe online environment, such a system may be heavily tested by a huge number of notices of organisations pursuing a commercial interest. Therefore, we suggest that trusted flaggers should not represent any commercial interest but indeed a collective interest and focus solely on the main objectives of the DSA, ensuring a trustworthy and safe online environment. The Commission should provide guidance to ensure harmonised criteria for awarding the status of trusted flagger and supervision of the activities of trusted flaggers. Further, we suggest clarifying:

- what exactly is a 'collective interest' e.g., this should not represent a commercial interest of brands to avoid becoming a competitive tool;
- how to avoid that trusted flaggers may clog the system;
- how DSCs can act quickly against trusted flaggers abusing their position or making inadequate notices;
- liability in case of damages after removing or blocking access to online content due to an incorrect notice by a trusted flagger;
- the status of a trusted flagger if it only sent incorrect notices to specific platforms;
- what a significant number of insufficiently precise or inadequately substantiated notices is. Would this depend on the number of notices a platform receives, the number of notices a trusted flaggers sends in total or to a specific platform, or is it related to something else;
- whether quality criteria are needed;
- what 'with priority and without delay' means.

Article 20 – Measures and protection against misuse

EuroCommerce welcomes including this article, and suggests clarifying:

- what 'manifestly illegal content' means e.g. the product image is compliant but the delivered product not;
- whether a prior warning is always necessary in case the content is clearly illegal.

Article 21 – notification of suspicions of criminal offences

It would be helpful if it was clarified what 'serious criminal offence' means, as a platform would make strong accusations against a service recipient/client. Especially for smaller players a clearer definition would be helpful to avoid unnecessary burdens and legal uncertainty.

Number of active users

Article 25 – Very large online platforms

EuroCommerce understands the Commission's idea to have different regimes for different types of platforms. This differentiation based on the number of users is however not sufficiently clear. Depending on the type of services a platform provides the 'average monthly active recipient' may be very different e.g. a social media user may log in a few times a day, while for a fashion platform this may be a few times a month. Is an active user someone who is browsing the ails or buying a good? Is an active user the same for transactional and interaction platforms? In this context, leaving the answer to this question to an implementing act will create too much uncertainty. Hence, 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 they must be actual active users who use the platform. It also seems sensible to strive for coherence with the Digital Markets Act (DMA) proposal, maintain and strengthen the issues about market power in the DMA and focus on issues of risk that involve more than just scale in the DSA.

At this moment in time, the proposed threshold of 45 million average active monthly recipients only seems to cover a limited number of platforms active in the EU market, but we expect that within 5 to 10 years many more EU based platforms will grow strongly and reach the 45 million threshold. Keeping this in mind, it is important that the additional requirements for very large online platforms do not deter EU based players from investing in growth in order to avoid a regime that may be perceived as overly burdensome, especially for online marketplaces mainly selling products to consumers.

Enforcement

Enforcement should be effective and efficient, and risk-based focusing on the rogue trader or platform. This may particularly be a challenge digitally, as there are no borders as in the physical environment. Therefore, we support the extension of the scope to all online services provided by online intermediary services providers to EU based consumers. However, many of the online service providers are established outside the EU i.e. third country traders and third country marketplaces. It is unclear from the proposed text how national authorities or the European Commission will effectively supervise these online service providers. The legal representative for third country marketplaces is a good step forward, but it should be clarified how authorities will ensure effective implementation of relevant enforcement measures.

We support the Commission's proposal to clarify better the role and responsibilities via the Digital Services Coordinator, and the different provisions enhancing coordination and collaboration between the Digital Services Coordinator and the Commission. We support the country-of-origin principle. We do have concerns about the strong powers allocated to the European Commission. Below are our suggestions and comments in more detail.

Article 11 – Legal representative

EuroCommerce supports the introduction of a legal representative for third country marketplaces. Such a representative should bear as much as possible the 'ultimate' liability for obligations under EU law. It is questionable whether a legal representative will actually have sufficient resources to fulfil its obligations, a solution could be to require a legal guarantee of the company they represent. We suggest the following clarifications:

- what can enforcement authorities do when the legal representative lacks adequate resources? E.g. how can authorities force the third country marketplace to fulfil its obligations and is this realistic?;
- that the ultimate liability should remain with the third country marketplace, especially considering cases where the legal representative may not be able to fulfil its obligations;
- specify what the legal representative is liable for. Why would this not cover liability for other relevant EU law when not already foreseen specifically in other EU law?

Article 40 – Jurisdiction

We support maintaining the country-of-origin principle, this will ensure legal certainty for online platforms by having one set of rules to comply with in the Member State of establishment. As long as, the single market remains fragmented and Member States continue to adopt diverging national rules the country-of-origin principle remains the only way to provide legal certainty for businesses. Especially, in the digital economy, it would be overly burdensome for businesses needing to comply with 27 different sets of rules across the EU. It would undermine innovation and growth as businesses will focus on the market they know best to avoid legal uncertainty and be deterred from operating cross-border. At the same time, the principle should not prevent authorities to collaborate closely and coordinate cross-border cases to prevent lacking enforcement.

Article 42 & 59 about penalties & fines

In general, we are concerned about the strong drive to introduce more and more turnover-based fines (GDPR, DSA, DMA, Omnibus Directive, AI regulation, etc.) in EU law. This undermines legal certainty and it is unclear whether the nature, gravity and duration of the infringement is still relevant. High fines are unlikely to be of help to businesses that already strive to be compliant, which can make mistakes nevertheless. No matter how high or low the fines are they will do their best to be compliant. Therefore, instead of focussing on fines, enforcement authorities should focus on helping businesses to be compliant, to solve infringements quickly or to prevent infringements from occurring at all.
Therefore, we consider the turnover-based fines excessive. Fines should be based on the nature, gravity and duration of the infringement, and be effective dissuasive and proportionate and a measure of last resort.

Article 47 to 49 – European Board for Digital Services

EuroCommerce supports improving the structure for collaboration between Member State authorities. This will improve the efficiency and effectiveness of cross-border actions, increase an EU oversight and alignment of enforcement practices. However, it is important that stakeholders have access to such organisations on a structural basis. Regular consultation of and meetings with stakeholders should be part of the tasks of the Board and foreseen in public work programmes.

Article 50 to 66 – Supervision, investigation, enforcement and monitoring in respect of very large online platforms

EuroCommerce is concerned about the strong powers allocated to the Commission. This is heavily inspired by EU Competition Law and the Single Market Information Tool (COM/2017/0257 final) proposal which was rejected by the Council and European Parliament. Are such strong powers and the earlier mentioned high turnover-based fines really necessary under internal market rules.

Also, as stated earlier, it should not deter smaller platforms to invest in growth because they want to avoid being captured by a regime that is seen as overly burdensome.

Some more detailed questions and comments:

- Article 54: clearly define what 'explanations' mean, and how will this regime be enforced over legal representatives?
- Article 57: clarify the type of monitoring actions and introduce an end date. Now the Commission can monitor a platform indefinitely if it has been captured once by the special regime.

Codes of conduct

Article 35& 36 – Codes of conducts

EuroCommerce supports voluntary industry or stakeholder initiatives that promote a trustworthy and safe online environment. Many members are already part of such initiatives. Article 35 may cause doubt about whether a code of conduct would still remain voluntary. Especially, considering that the Digital Services Coordinator of establishment (DSCe) and the Commission will have to power under certain conditions to make commitment from codes of conduct binding which have no legal basis e.g., commitments regarding harmful but not unlawful content. A DSCe can make a commitment binding for any platform, and the Commission can make a commitment binding for very large online platforms. At the very least, another lighter version of a code of conduct could be foreseen as under Article 36. We suggest opening up the model for codes of conduct for online advertising to other types of initiatives. Voluntary initiatives should remain voluntary and not be defined and enforced by public bodies.

Application date DSA

Article 74 – Entry into force and application

A three-month transition period is impossible looking at the level of detail of the DSA, especially regarding the envisaged transparency obligations and notice & action system. Platforms will only know after the adoption of the DSA what the exact requirements are, and will need sufficient time to implement all the different provisions and hire new employees to be compliant.

Therefore we suggest to at least have a 12 months transition period after its entry into force.

In addition, we would like to point out that any implementing guidance accompanying the adoption of the DSA should be provided at least 6 months before the application date, to give online service providers sufficient time to implement the relevant provisions properly. This is a real concern, as we have seen with the P2B Regulation where the Commission published the implementing guidance months after the application date, causing legal uncertainty for businesses.