MINISTRY OF INDUSTRY, BUSINESS AND FINANCIAL AFFAIRS

8. September 2020

The Danish Government's response to the public consultation on the Digital Services Act

General Comments

The Danish Government looks forward to the Commission's upcoming Digital Services Act (DSA). The EU needs to modernise the legal framework for digital services and hence the Danish government supports this ambition.

The Danish Government notes how especially the rise of digital platforms have created new and unforeseen challenges that need to be addressed. Digital platforms serve important functions as gateways to information and facilitators of communication, why the largest platforms have become the equivalent of public spaces. It is hence highly problematic that these private companies effectively decide how freedom of expression and information can be exercised on their platforms. European citizens experience their fundamental rights infringed when their content is removed, or their accounts are blocked with no democratic safeguards or transparency/without explanation or due process. At the same time, the platforms' efforts are not proving adequate in the removal of illegal content, which is distributed with speed and efficacy on the platforms. In effect, citizens are increasingly exposed to terrorist content, appeals to violence, and the sharing of child pornography. On the platforms, consumers moreover risk inadvertently purchasing illegal and dangerous products and are increasingly exposed to unlawful and misleading marketing. For the individual citizen it can be a struggle to have illegal content removed when facing a large platform that does not respond to their complaints. This has especially proven an obstacle for victims who have had their intimate pictures disseminated widely on platforms without their consent. It is the experience that some platforms shed their responsibilities because they are not liable for content generated by others. Finally, platforms can position themselves in such a way that existing laws and regulations do not effectively apply to them and they go virtually unregulated. The Danish Government hence finds that there is a pressing need to establish a new framework with clear requirements for digital platforms' liability and responsibilities.

The criteria for success is a more responsible digital economy, where digital service providers take up greater responsibility in order to mitigate risks deriving from their services, and at the same time safeguard fundamental rights and setting high standards as regards the rebooting of our digital economy.

In the following, we have listed our main points to the public consultation on the DSA. These are elaborated in the attached annex.

- **The DSA should be a regulation to ensure effective and uniform application**

The DSA should ensure a true Single Market absent of regulatory fragmentation and with a level playing field based on uniform application, implementation and enforcement. Thus, the DSA should be tabled as a regulation.

- **Preserve the core principles of the e-commerce Directive in a modernized form**

The new legislative framework should foster a responsible platform economy by building on the core principles of the e-commerce Directive. In order to form a fairer platform economy, clear criteria and standards for the handling of content should be established building on the principle of origin. The prohibition to impose general monitoring obligations and the limited intermediary liability should be preserved in its core, but in a modernized form establishing greater responsibilities for digital platforms.

- **New and efficient tools to remove illegal content**

It is becoming disappointingly evident, that even though many digital service providers are taking steps to combat illegal content, further efforts are needed. Therefore, the DSA should introduce new tools to tackle the wide range of challenges related to online dissemination of illegal content to the detriment of EU citizens, consumers, and businesses.

- **Illegal and harmful content should not be equated**

In addressing the spread of harmful content online, it is important to emphasize that harmful content should never be equated with illegal content. Addressing harmful content in the same manner as illegal content may have detrimental repercussions for fundamental rights. Accordingly, measures introduced in the DSA to counter online harm should solely focus on *illegal* content.

- **Updating the liability regime by introducing a 'duty of care' requirement**

There is an urgent need for digital service providers to live up to their responsibility in order to create a more fair and safe digital economy. Therefore, the existing liability regime should be modernised. Specifically, an incentive for digital service providers to proactively combat illegal content is needed. A 'duty of care' requirement should be introduced in order to ensure that certain types of illegal activities are detected and prevented. In this way, digital platforms would only be covered by the liability exemption as long as they are taking measures that could reasonably be expected to proactively detect and remove illegal content on their services and collaborate with governments in a transparent manner.

- **Fast removal of illegal content in a harmonised notice and take-down procedure**

The new liability framework for digital platforms should be accompanied by a new set of responsibilities to ensure the fast and transparent removal of illegal content upon notification as well as to prevent infringements of fundamental rights. Hence, the DSA should establish a framework for notice and take-down with a clearly defined procedure, safeguards and timeline for acting on notifications on illegal content and ensure uniform procedures in all Member States.

- **Speedier removal of high impact content**

While it is necessary to grant digital platforms time to assess the legality of content, some user-generated content has a very high impact and may pose a greater threat to society or significant damage to the individual. Therefore, it would be prudent to have two sets of timelines with a shorter timeframe for such high impact content.

- **Combatting non-compliant products from third countries by introducing "Know-Your-Business-partner"-principle**

Third-country digital platforms should comply with the same "duty-of-care" and notice-and-action requirements set out in the DSA. This entails that both European and third-country platforms should be expected to know their business partner in order to avoid consumers to unknowingly buy dangerous products, cosmetics containing dangerous chemicals or phone chargers that set on fire.

- **Effective enforcement mechanism to protect European Citizens and consumers and ensure a level playing field**

In order to ensure effective and consistent enforcement of the new framework provided by the DSA, a new enforcement cooperation mechanism between authorities in Member States should be put in place. The mechanism should establish clear procedures for the cooperation between the relevant national authorities on concrete cases of non-compliance with the regulation. A special procedure should be established, whereby the Commission is given a central role in coordinating the investigation of and actions against digital services, where citizens, consumers or businesses from several Member States are affected.

- **Platforms as gatekeepers**

We refer to the Danish Government response to the IIA on gatekeeper platforms from June 2020.

Specific remarks to the different elements in Digital Services Act can be found in the attached document "Annex: Specific comments from the Danish Government's on the public consultation on the Digital Services Act".

Annex: Specific comments from the Danish Government on the public consultation on the Digital Services Act

1. A Strong Single Market for Digital Services

The overarching aim of the Digital Services Act (DSA) must be to preserve and strengthen the Single Market for digital services and ensure that European companies, consumers, and society can continue to benefit from the opportunities given by digital services. A new framework for digital services should establish clear and cohesive rules that provide legal certainty, promote the development and uptake of new technologies and business models, and support businesses' opportunities to operate and scale across borders. The DSA should ensure a true Single Market absent of regulatory fragmentation and with a level playing field based on uniform and effective application, implementation and enforcement, while at the same time safeguarding fundamental rights.

The e-commerce Directive established the framework conditions for digital innovations to emerge, ensured the freedom of establishment and the freedom to provide digital services across the Union. The core principles on intermediary liability exemption and country of origin as well as the prohibition to impose a general obligation to monitor content have further been instrumental in the development of a strong European platform economy.

1.1. Modernising the framework to address new challenges

Since the e-commerce Directive was introduced, a wide range of new challenges have developed. Significant challenges related to the online dissemination of illegal content are to the detriment of European citizens, consumers, and businesses. Citizens are for instance exposed to terrorist content, appeals to violence, and the sharing of child pornography, and citizens risk having their intimate material shared widely without their consent. Consumers risk inadvertently purchasing illegal and dangerous products and are increasingly exposed to unlawful and misleading marketing. Businesses that comply with Union law face an unlevel playing field, when businesses from third countries sell their non-compliant or copyright infringing products to European consumers via platforms. It is becoming disappointingly evident, that even though many digital service providers are taking steps to combat illegal content, further efforts are needed to foster a better and more responsible platform economy.

Going forward, a new legislative framework should tackle the challenges that have arisen over the years and which the e-commerce Directive does not address. However, it is crucial that this is done by building on the foundation of the core principles and conditions of the e-commerce Directive that have been essential in establishing the Digital Single Market. When addressing new challenges, we should be careful not to establish new bar-

riers in the Single Market. This would have disproportionate impact on European SMEs and start-ups. It is therefore essential to preserve the country of origin principle, as it both enables digital services to operate across borders and enables European SME's to reach consumers across the Single Market in a cost-efficient way. Further, the intermediary liability exemption and the prohibition to impose a general obligation to monitor content that have been instrumental in creating a European platform economy must be preserved, but in a modernised form.

1.2. Table DSA as a regulation to ensure uniform application

Some of the new challenges have been addressed at both Member State and European level[1]. A disadvantage of this is that digital services providers and internet intermediaries are increasingly being met with diverging legal and procedural requirements. Altogether, such legal fragmentation causes legal uncertainty, administrative burdens, and unnecessary barriers to trade within the Single Market. Rather than fostering a competitive environment, the fragmented legal landscape favours larger, well-established firms who can afford the compliance costs. Therefore, the DSA must have a main aim of establishing a regulatory framework that fosters an effective Single Market based on clear and harmonised rules that can overcome the complexity and legal fragmentation of the current framework. With a view to accomplishing these goals, the Danish Government urges the Commission to propose a Union Regulation that ensures harmonised and effective application.

2. Updating definition on intermediaries to reflect new types of digital services

In line with the e-commerce Directive, the DSA should continue to regulate all digital services, from hosting services and DNS (Domain Name Systems) registrators to e-commerce platforms. Therefore, the Danish Government finds it absolutely necessary for the Commission to clarify the legal status of digital platforms by determining what requirements a service must meet in order to be considered an "intermediary service provider" within the remit of the DSA. Further, the framework must still distinguish between two types of intermediaries, the passive ones, such as hosting services, and the more active ones interacting with third party content allowing for different responsibilities and liabilities.

The landscape of intermediary service providers has evolved and grown substantially since the adoption of the e-commerce Directive. Notably, the developments include the rise of digital platforms enabling user-generated

[1]Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)
Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC
Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

content in the public space, which have come to play an increasingly important role in society. Digital platforms can take many forms and can be based on a number of different business models that are continually evolving. The collaborative economy has patricularly brought about a new range of digital platforms that allow people to connect various goods and services, e.g. with respect to real estate, transport, labour, vacation and money lending. Depending on their particular configuration, some of these services may be considered intermediary services while others may not.

2.1. Necessary to provide clarity on what constitutes an intermediary

In the case of digital platforms, deciding what constitutes an intermediary service provider is rarely straightforward, as some platforms' business models balance on the line between being an optimising intermediary or a traditional service provider, an online seller or a mixture thereof. The assessment is further complicated in cases where the platform besides from hosting, performs additional activities that do not consist of hosting. Finally, intermediary service providers may be able to position themselves in such a way that existing laws and regulations in the underlying market do not clearly or effectively apply to them. In such situations of regulatory arbitrage, new intermediaries may gain an advantage over regulated entities operating in the same markets.

Altogether, due the lack of specificity of the intermediary service provider definition it is not always clear whether the new intermediary functions in the online environment, such as digital platforms, fall within the scope of the term. Where a service falls outside that definition, the service in question does not benefit from safe harbours in the e-commerce Directive and the question of liability will be settled under relevant national law. Thus, a regulatory gap exists where it is unclear whether a service is covered by the liability exemption and hence, under which legal regime it operates.

In order for the DSA to effectively regulate digital services, it must first and foremost provide clarity on what kind of services will be covered by the different provisions and requirements. A central task will be to provide clarity on what constitutes an "intermediary service povider" within the remit of the DSA and thus to clarify the legal status of digital platforms, dependent on their specific configuration. Ideally, the DSA should offer legal certainty both for existing services as well as for future services. Consequently, rather than a typology determining which existing types of services will be covered by the term "intermediary service provider", the DSA should introduce a framework for determining whether a service can be considered an intermediary. The framework should establish what requirements a service must meet in order to be covered, or which criteria will exclude the service from the scope. These criteria could take inspiration from relevant case law, and accordingly they could be based on whether a

service is involved in price setting, ranking, purchasing and reselling, drafting of commercial messaging or optimising the presentation of sales.

2.2. Maintaining two types of "intermediary service providers", allowing for different liabilities and responsibilities

A second issue arises with regard to the variation of those services that do fall within the scope of an intermediary service provider. Under the existing regime, the determination of whether an intermediary service provider can actually benefit from the liability exemption is dependent upon whether the role of the intermediary is considered to be "passive" or "active", and hence whether or not the intermediary has knowledge or control over the information which it stores or transmits. An intermediary that is considered to be active will, unlike the "passive" intermediary, loose privilege of the safe harbour and its role and responsibilities will be assessed according to the national intermediary liability regimes. This conceptual distinction works as intended to separate the "passive" conduit and caching services from other types of services.

There are still many services that clearly fulfils the role of a "passive" intermediary, and who ought not be held liable for user-generated content. However, some of today's digital services do not fall into the category of a passive intermediator, whose activities are merely of technical character, neither can they be claimed to have actual knowledge or control of all the content on their services. These intermediary services are most commonly digital platforms. Whether they are exempted from liability or retain full liability of the user-generated content, it would not correspond to the role they play in the value-chain, such as content moderation. Hence, distinguishing between what kind of intermediaries should either not be liable or maintain full liability for user-generated content on the basis of the concepts "passive" and "active" alone is no longer sufficient.

The DSA should distinguish between two types of intermediaries; the "content facilitators"[2] whose activities are solely passive in nature, and the "content intermediaries"[3] that take on a more active role, but cannot be considered as content providers, traditional service providers or other services that fall outside the scope of the new DSA intermediary framework[4]. This distinction shall allow for assigning two different liability exemptions to the "content facilitators" and the "content intermediaries" with a view to en-

[2] The term "content facilitator" is not an existing definition in Union-law but is applied here for clarity purposes. Services such as network operators, cloud infrastructure services, DNS registrators could be defined as "content facilitator".

[3] The term "content intermediary" is not an existing definition in Union-law but is applied here for clarity purposes.

[4] Inspiration could be taken from sector specific regulation, such as the revised Audiovisual Media Services Directive (AVMSD), which similarly distinguishes between information society services that are passive in nature and those that take on a more active role (video sharing platform services).

suring that their liabilities and responsibilities will correspond to their respective roles in the value chain. The DSA should provide clarity and clear criteria on whether a service would be considered as a passive "content facilitator" or the more active "content intermediary".

3. Updating Intermediary Liability for active "content intermediaries"

There is an urgent need to modernise the existing liability regime in order to align the regulatory framework with new market and technological developments and to create an incentive for digital service providers to proactively combat illegal content. The Danish Government finds that the liability should reflect the role a digital service provider plays in the value chain, and that the responsibility to act should correspond to the kind of measures the service has at its disposal. The existing framework of "either full liability or no liability at all" is no longer working and do not correspond to the digital services knowledge or moderation of content on the platforms. A more nuanced and modern approach should be taken.

The online dissemination of illegal content, which is especially prevalent on digital platforms, has become a growing challenge, which needs to be tackled. This will require both efficient legislation that establishes clear rules on liability, and an industry that assumes responsibility and makes a solid effort to detect and remove illegal content from their services.

The liability exemption in the e-commerce directive has been vital for the Digital Single Market, as it has enabled the very operation of several valuable digital services by exempting them from facing the threat of potential liability for third party content when performing the functions of mere conduit, caching, hosting and storing of information. In the current online environment, there are still clear-cut cases of "passive" content facilitators that have a merely technical role, as their service is constricted to the transmission of information, and who further have limited measures at their disposal for removing access to illegal content online. These "content facilitators" should continue to be protected under the existing liability framework as well as by the prohibition to impose a general obligation to monitor content. Such services include, but are not limited to internet service providers, network operators, cloud infrastructure services and DNS Registrars.

However, some digital services take on a more active role in the value chain as regards i.e. content moderation; hence they may be considered as "content intermediaries". The content intermediaries are most commonly online intermediaries who facilitate the sharing of content and provide services that connect different users in their respective ends of the value-chain, such as digital platforms. These content intermediaries should not automatically be fully liable for content generated by third parties. On the other hand, their liability ought to correspond to the more active role they play in the

value chain. Moreover, unlike the more passive "content facilitators", the digital platforms have the ability to take proportionate and pro-active measures to combat illegal content on their services but lack the legal incentive to do so. This is because the distinction made between active and passive actors entails a disincentive to act pro-actively to tackle illegal content. Consequently, digital services may avoid taking steps to pro-actively identify and remove illegal content for fear of becoming liable for all content on their services.

It has become clear that the dissemination of illegal content on digital platforms is a persistent challenge, and a reactive measure of notice-and-action requirements, whether in the existing form or an updated harmonised one, will not suffice. Awaiting notification before takedown results in a considerable delay, allowing the illegal content to be dispersed quickly and widely, which may have severe ramifications. It is important to the Danish Government that the digital platforms take on a more responsible and pro-active role in detecting and removing illegal content from their services and that they become a safer space for European citizens. To this end, the DSA should introduce a new liability framework for "content intermediaries" that do not fit the category of a "passive" actor, most notably the digital platforms.

3.1. Introducing a 'duty of care' requirement for digital platforms

The DSA should link the liability for digital platforms with a requirement to take pro-active measures to remove illegal content quickly and efficiently. With this approach, digital platforms would still not be liable for the illegal content as such but would face procedural requirements regarding their handling of illegal content on their services. At the same time it is important to ensure framework conditions that underpin a vibrant platform-economy in the EU and which enables the growth of start-ups and small platforms, why the threat of full liability must not make the business model unsustainable for new entrants. Further, it is essential that the framework does not introduce rigid standards, but allows for innovation and enables the platforms to develop new and more effective solutions to identifying and removing illegal content.

This could be achieved by introducing a 'duty of care' requirement inspired by recital 48 of the e-commerce Directive, which specifies the option of requiring service providers to apply duties of care, which can be reasonably expected from them in order to detect and prevent certain types of illegal activities. By introducing such a requirement, digital services would only be covered by the liability exemption as long as they are taking measures that could reasonably be expected from them to proactively identify and remove illegal content that has been uploaded to their services. In other words, the liability exemption would pose an incentive to act proactively as opposed to the disincentive inherent in the current liability exemption. It

should, however, continue to be forbidden to impose a general obligation to monitor content, and digital service providers should not be obliged to screen content before it is uploaded.

What constitutes sufficient measures taken by the platforms would depend on the size, ability, and business model of the digital platform in question, but should not be too rigidly specified by the regulation. For instance, all the largest platforms could be expected to ensure that content that once has been identified as illegal and removed, is quickly detected and removed again if a user re-uploads it. Social media platforms could be expected to utilise algorithmic systems to detect and remove illegal content, while online marketplaces, dependendent on size, should be expected to consult information on recalled and dangerous products on RAPEX and from enforcement authorities, and remove identified listings offering unsafe products.

The ‘duty of care’ principle would be futureproof as the measures that would be expected from the different kinds of platforms could change over time as markets and technologies develops. The platforms will be expected to continuously learn from their efforts and invest in new and improved solutions in order to keep up with the efforts of other platforms of similar size, ability and business model. Consequently, the demand for technological solutions to detect and remove illegal content will create a new market. Over time, a number of businesses will be offering effective technological solutions at a price affordable even to the smaller platforms. Altogether, the ‘duty of care’ principle should result in a continuously improving effort in the fight against illegal content for all digital platforms, regardless of size and type.

The platforms should prove that they live up to the ‘duty of care’ requirements in order to be covered by the liability exemption, why they should be required to regularly publish standardised reports on the actions taken as well as on the results. This will make it possible for the authorities to enforce the regulation, including assessing and commenting on the platforms’ efforts. Comparison of the reports will also allow the individual platforms to benchmark their performance to that of other platforms with a view to improving their efforts. Finally, publication of the reports will give the public a better understanding of the platforms’ content moderation practices.

When introducing such a requirement in the DSA, it is important to strike the right balance between flexible, functional requirements that are future-proof on the one hand, while on the other ensures legal clarity and foresee-ability. The legal text should provide legal certainty while not being too prescriptive. One way forward could be to introduce the general "duty of care" requirement in the legal text and provide examples in the recitals as

well as having the Commission in cooperation with Member State authorities provide guidance to businesses. It is paramount that the guidance ensures proportionality and ensures that ensure that start-ups will still be able to scale-up.

3.2 Introducing "know-your-business-partner" principle for online market places

When consumers buy products on digital platforms, many businesses may be involved in a sale and sometimes there are insufficient information about the identity, address and contact information of the businesses. Consumers often find it difficult to understand who is the contracting party and thus to whom the consumer may complain over non-compliant products. In addition, authorities have difficulties enforcing the rules if it is not clear which company is behind the sale.

Online marketplaces should therefore make an effort to verify the information and identity of its business partners. In this regard, the DSA should introduce the principle of "know-your-business-partner". Further, an effort should be made to verify that the information the business partners provide is up to date and to ensure that non-compliant sellers and counterfeiters are not allowed to continuously register as new sellers on the platform after once having been identified as fraudulent. In this regard, it should be noted, that harm to a seller on an e-commerce platform caused by the removal of a legal product is regulated in the Platform-to-Business regulation.

3.3. Adressing Legal Fragmentation of the Liability Exemption in Union law

The EU have since the e-commerce Directive sought to adress challenges related to illegal content online through sectorspecific regulation. Consequenlty, the copyright Directive, the audiovisual media services Directive, and the the Directive on combating the sexual abuse and sexual ex-ploitation of children and child pornography have introduced several exemptions to the horizontal liability framework of the e-commerce Directive and introduced diverging requirements on digital pltaforms with regards to the removal of illegal content. The adoption of the Commission's proposal[5] for a regulation on preventing the dissemination of terrorist content online is expected to add further to this list. And with the possible introduction of new liability and responsibility requirements for digital services in the DSA, there is a risk of adding further to the existing legal uncertainty and fragmentation. Hence, it is important for the Danish Government that the DSA rather than adding to the problem becomes the solution. Ideally, the new articles on liability and responsibility requirements in the

[5] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online

DSA should replace similar requirements/specific elements of above legislation with a view to ensuring horizontal rules. For instance, the Danish Government's suggested framework for digital platforms' liability for and responsibility to act would address the same challenges regarding digital platforms' liability for illegal content addressed in the sector-specific legislation.

4. Responsibility to Act – A harmonised procedure for notice and take-down

Today, digital services are required to take immediate steps to remove illegal content, once they have been made aware of it. Unfortunately, the experience is that digital platforms can be slow to remove content they have been made aware of. Further, platforms may be reluctant to remove flagged content when they are unsure of its illegality. This is highly problematic, as fast removal is essential in order to limit the wide dissemination that occurs at a fast pace and that can have damaging consequences for users, for companies and for society.

At the same time, the lack of appropriate and effective safeguards to prevent the removal of legal content may result in infringements on fundamental rights such as the freedom of speech or the right to information. Hence, it is necessary to establish a framework for notice and action with a clearly defined procedure, safeguards and timeline for acting on notifications on illegal content and ensure uniform procedures in all Member States. The framework should include both effective complaint- and redress mechanisms, standardized transparency reporting and sanctions.

4.1. Platforms should act upon notice within clearly defined timeframes and following a precautionary principle to handle high impact content

First, it is important that digital platforms are required to act upon a notice within clearly defined timeframes. While it is necessary to grant the platforms time to assess the legality of content, some user-generated content has a very high impact and may pose a greater threat to society, such as the rapid dissemination of terrorist content, or may cause significant damage to the individual, such as the non-consensual sharing of intimate content. Therefore, stricter timelines for high impact content should be imposed. This could for instance be done by introducing a precautionary principle, where high impact content should be removed first, and assessed afterwards. The platforms would only be liable for taking down legal content in this category, if they have not assessed and reposted the content within an extended timeframe. A longer timeframe should be set for the other category of illegal content, where the potential negative impact is not as high. There should be clear provisions in the DSA on what type of illegal content falls within the scope of each timeframe. In addition, the regulation should provide for the possibility to change the timeframes to act, if and when new developments enable quicker responses.

4.2. Platforms should have an easily accessible user complaint system

Second, platforms must be required to have a user-friendly and easily accessible complaint mechanism, as well as a transparent process for acting upon complaints. Clear guidelines should set the terms for what may constitute an easily accessible and user-friendly complaint mechanism. For content that is publicly available, it should be possible to notify the platform without having a user account. Due process safeguards must be put in place to ensure that users' fundamental rights are not encroached hence it is essential that users can challenge "over-removals" through an effective redress mechanism. In this regard, it is further important that the notice and action framework does not become a tool for harassment, why appropriate safeguards must be put in place. As users' fundamental rights can also be encroached on the basis of the platforms' proactive measures, it should be possible for the users to challenge the removal of content that did not originate from a notification.

4.3. Platforms should publish transparency reports

Third, platforms should be required to regularly publish transparency reports about the effectiveness of their moderation and removal efforts as well as on the lawful content that is mistakenly removed[6]. It is important that the reports reflect both content that has been removed as part of the reactive notice and takedown process and content that has been removed as part of the platforms' proactive measures. In this regard, a section of the transparency report should be dedicated to information on content that has been detected and removed by algorithmic systems. The reports should also include assessments of the content that the platforms are not able to remove effectively, such as assessments of the illegal content likely remaining on their platforms. If the platform has community guidelines or similar, which entails the removal of content that is not illegal, the transparency report should describe these guidelines and shed light on content that has been removed on the basis of these guidelines. Standards should be established, in order to ensure consistent reporting with comparable information, which will allow for better assessment of the overall impact of content moderation.

4.4. Sanctions should enforce the notice and take-down framework

Finally, sanctions should be imposed in order to enforce the notice and take-down framework. Fines should be imposed for failure to put the aforementioned procedures in place or for systematically failing to remove notified illegal content. With a view to ensuring that the threat of sanctions do not lead to unnecessary or excessive censorship, platforms should additionally be fined for systematically removing legal content.

[6] A similar requirement could be considered for disinformation and coordinated inauthentic behavior following the code of practice review.

For the requirements on platforms responsibility to act, a proportionality principle should be considered with a view to exempt smaller platforms.

5. Addressing the Challenge of Non-Compliant Products from third countries

There are growing problems stemming from third country companies that sell illegal products to European consumers via digital platforms established in the EU and in third countries. It is important that the DSA addresses this issue.

With the increasing cross border e-commerce and the emergence of digital platforms, European consumers buy products from all over the world. However, when consumers purchase products via digital platforms, it is not the platform, but the seller, that is liable for the product and required to live up to consumer protection rules. Hence, challenges arise when sellers from third countries do not abide by Union-law, as it is difficult for enforcement authorities to enforce the rules towards sellers in third countries

The digital platforms make the process of buying products from third countries just as simple and accessible for consumers as it is for them to buy products from EU-based companies, why consumers often do not realize when they are left unprotected as regards product safety and consumer protection rules. Consequently, consumers unknowingly buy and utilize products that do not live up to EU standards and requirements such as a lack of correct labelling or user instructions on the product, dangerous toys, cosmetics containing dangerous chemicals, or phone chargers that set on fire. In addition, the EU consumer protection legislation on e.g. misleading marketing, information on price, VAT, delivery costs may not be complied with when sellers from third countries sell to EU-based consumers via platforms. The result is a decrease in consumer welfare.

Furthermore, this leads to unfair competition for the European companies complying with Union-law. European businesses incur high compliance costs making sure their products are safe and live up to European standards, just as they make sure to comply with other consumer protection legislation. Hence, businesses from third countries gain an unfair advantage, when they via the platforms can sell non-compliant products directly to European consumers at a lower price-point than European comparable products.

5.1. Introducing "duty of care" for all platforms directing services at the EU"

The Danish Government finds that these challenges should be addressed in the DSA by imposing the Regulation on all digital platforms that direct their services at European consumers, regardless of whether they are estab-

lished within the EU or not, as with the GDPR. Thereby, third country digital platforms shall comply with the same "duty of care" and notice-and-action requirements as EU digital platforms. This entails that both e-commerce platforms established in the EU and those established in third countries should be expected to "know your business partner" (see chapter 3.2.) and take action if non-compliant sellers reappear. It would further include the obligation for large e-commerce platforms to ensure that illegal products listed in RAPEX are identified and removed effectively as well as making them liable if they do not remove illegal products or services when notified.

6. Effective Enforcement to Protect European Citizens and Consumers and Ensure a Level Playing Field

The Danish government supports initiatives in the Digital Services Act to strengthen enforcement on digital platforms, which is essential to protect citizens and consumers and to ensure a level playing field for the businesses complying with the rules.

It is the experience that the provisions in the e-commerce Directive are not always enforced properly or consistently, and that the enforcement on services located in other Member States and operating cross borders can prove challenging for Member State authorities in the existing framework.

6.1. Establishing an enforcement cooperation mechanism

In order to ensure effective and consistent enforcement of the new framework provided by the DSA a new enforcement cooperation mechanism between authorities in Member States should be put in place. The mechanism should establish clear procedures for the cooperation between the relevant national authorities on concrete cases of non-compliance with the regulation. The competent authorities in the country of origin should be required to respond to inquiries from other Member State authorities within fixed time limits. Each Member State should point out a liaison office that will work as a single point of contact on matters related to the DSA. The DSA should ensure that the necessary information and evidence legally can be exchanged between competent authorities with a view to ensure that non-compliant services can be held accountable.

For infringement cases that affect citizens, consumers or businesses in several Member States, it may prove difficult for national authorities to pursue enforcement steps, and a more coordinated approach may be called for. Hence, a special procedure should be established, whereby the Commission is given a central role in coordinating the investigation of and actions against the digital services that operate across borders. The special procedure should enable a legal case to be made against a service based on its infringements of Union law incurred in various Member States. Altogether,

the strengthened cooperation and coordination between Member State Authorities and the Commission should lead to a more consistent application and enforcement of the horizontal framework, also ensuring a level playing field for businesses.

It is important that the new enforcement mechanism complement cooperation between member states' enforcement authorities in other areas, such as the CPC-network.

6.2. The exemptions to the country of origin principle should be clarified
Looking at the existing framework, it is the experience that Member States have different interpretations of the exemptions to the country of origin principle, which is a hindrance to the consistent enforcement across the Single Market. The DSA provides an opportunity to clarify and update the exemptions to the principle, for instance with a view to limit the exemptions to areas that are harmonised in Union law. Taking into account that the Union consumer protection legislation to a great extent has been harmonized since the introduction of the e-commerce Directive, the exemption regarding consumer protection should be updated, so it becomes clear when the principle of origin applies or when consumer authorities in the receiving country may enforce Union-law. Consequently, the enforcement of Union-law will be improved, and the enforcement practice of Member States will become more consistent.

7. Cooperation Requirements Regarding Systemic Threats to Society
The largest digital platforms have a vast network of users, and consequently the content posted on their services can rapidly reach millions of users across the globe. Unfortunately, this unique interconnectedness provided by the largest platforms can pose a systemic threat to society when the platforms' services fall subject to abuse. Examples are the glorification of terrorist attacks, such as the terrorist attack in Christchurch, or attempts to influence democratic elections, such as the Cambridge Analytica case. On the other hand, the largest platforms' extensive networks are uniquely positioned to serve as information channels to the wider public. During the first months of the COVID-19 pandemic, the European Commission called for the cooperation of platforms in fighting dis- and misinformation as well as promoting content from official and verifiable sources, and the resulting cooperation between platforms and European authorities had a substantial effect. We should learn from these experiences and set up a legal framework to ensure that we are prepared for the next crisis.

Hence, the largest platforms should be subject to stricter requirements with a view to counter systemic threats to society. Such obligations ought to include a requirement of enhanced cooperation with authorities and the obligation to prioritise the dedication of their efforts on content moderation

to systemic threats when necessary. The largest digital platforms have already shown themselves to be capable of such efforts, as exemplified by the cooperation between select digital platforms and European authorities in combatting disinformation in relation to COVID-19. Additionally, it is imperative for the enforcement of criminal law that authorities can gain access to information from the platforms. Hence, the largest platforms should be required to share information with competent authorities that could help countering these systemic threats or lead to apprehending the perpetrators behind them.

8. Distinguishing between illegal content and harmful content

Challenges related to digital platforms are not limited to the dissemination of illegal content but also concern the spread of harmful content. Harmful content can take many forms verging from comments that may for some individuals be considered offensive to legal health-related misinformation with severe ramifications, as well as strategic disinformation campaigns aimed at undermining trust in our democratic institutions. The COVID-19 pandemic spurred an unprecedented amount of misinformation about the virus, which created confusion and distrust, undermined the public health response and caused a number of individuals physical harm due to false information on measures for protecting against or for curing the virus.

It is important to the Danish Government that the internet becomes a safer space for European citizens, and accordingly there is an increasing need to address the spread of harmful content online. However, it is important to emphasize that harmful content should never be equated with illegal content, and accordingly an important distinction should be made between the measures taken to address the two challenges.

Though the spread of harmful content can have serious ramifications, the term covers content which for various reasons have not been forbidden by law. What may be considered harmful content may differ not only from one Member State to the other, but also between different cultures or even on the individual level. Addressing harmful content in the same manner as illegal content may have detrimental repercussions for fundamental rights, notably the freedom of speech, the freedom of information, the right to privacy and due process.

Accordingly, the Danish Government finds that the measures introduced in the DSA to counter online harms should solely focus on illegal content. In order to tackle the spread of harmful content while safeguarding fundamental rights, a different toolbox than regulation is needed with regards to removal of content, whereas requirements to transparency and reporting with regard to harmful content could be options going forward. The Danish Government welcomes addressing the challenge of harmful content in the European Democracy Action Plan and as part of other initiatives.

The Danish Government further looks forward to addressing other challenges brought on by the emergence of digital platforms in the European Democracy Action Plan. One of which is how the public debate to a large extent has moved online to the social media platforms. While the digital platforms have contributed to broadening the democratic debate by giving an online voice to citizens, we must also acknowledge that the platforms' community guidelines and the way they moderate content is effectively shaping the course of the public debate. Accordingly, it is important to ensure that the digital platforms which effectively function as extensions of the public space facilitate a democratic online debate in full respect of fundamental rights.

9. Decent working conditions for all platform economy workers

The platform economy can contribute to foster labour market participation for people at the margins of the labour market, but the working conditions for platform economy workers must not lead to a race to the bottom. Decent working conditions should be ensured for all in the platform economy.

The main responsibility for ensuring decent working conditions should remain with the Member States, while the key EU focus should be on enforcement and exchange of best practices.

It is crucial that the social partners are involved in the dialogue and contribute to identifying challenges and solutions on the EU-level as well as the national level. It is vital that possible EU initiatives regarding platform economy workers respect the role and competences of Member States and the different labour market models, including those where social partners are responsible for pay and working conditions.

The Danish Government finds that working conditions for platform economy workers have a broader labour market perspective and should not be dealt with within the scope of the DSA. Further, a new "third" category in addition to workers and self-employed should not be introduced. Instead, possible EU initiatives regarding this question could be addressed separately to bring sufficient attention to this highly important issue.

The Danish Government looks forward to contributing to the debate in EU on how to ensure decent working conditions for all platform economy workers and taking into account concerns in relation to fair competition.

10. Streamlining information requirements in the e-Commerce Directive and other legislative acts

When evaluating the e-commerce Directive, it is important the Commission also focuses on consumer issues related to the e-commerce Directive. One of the initial purposes of the e-commerce directive was to promote cross

border e-commerce by amongst others granting consumers information of traders, since harmonized consumer legislation was limited at the time of the agreement of the e-commerce Directive.

Several information requirements exist in the current regulation related to e-commerce. The requirements are rarely identical but cover the same in terms of content. Thus, the information requirements in the e-commerce Directive should be aligned with the similar information requirements in the Services Directive and the Consumer Rights Directive. By unifying the wording of the information requirements, the consumers will more easily identify the relevant information, and the legal clarity will remove unnecessary burdens for businesses.

11. Clarified rules on commercial communication targeted children and young adults

With the emergence of social media platforms and the increasing number of influencers, challenges have arisen related to the marketing of products and services. Especially children and young adults have difficulty recognising when they are exposed to marketing on social media platforms and from influencers. Studies[7] show that this group is less likely to have the preconditions for interpreting the intentions and business models of marketing on social media, why there may be cause for further protection of consumers than the current framework provides. We invite the Commission to review Article 6 of the commerce Directive concerning commercial communication, to assess whether the Article is still fit for purpose or whether it should be extended or clarified in order to ensure better enforcement of marketing targeted children and young adults.

The Danish Competition and Consumer Authority is currently working on a behavioural analysis on this subject and will be happy to share the results with the Commission when they are available by December 2020.

12. Online commercials

Advertising banners are widely used. However, the at times also function as a channel that can be used by fraudulent websites to advertise directly targeted European consumers. E.g. consumers are let to think that they buy an authorised trademark product but in turn is a counterfeit good, most probably from a third country. Today, it is very difficult for EU authorities to take action against the seller. Further, digital services that has profited

---

[7] See i.e. B. Nardere, J. Matthes, F. Marquart & M. Mayrhofer (2018): "Childrens attitudinal and behavioral reactions to product placements: investigating the role of placement frequency, placement integration, and parental mediation". International Journal of Advertising.
S.C. Boerman & E.A. van Reijmersdal (2020): "attitudinal and behavioral reactions to product placements: investigating the role of placement frequency, placement integration, and parental mediation". Frontiers in Psychology.

from the advertising also cannot be held liable. The Danish Government encourages the Commission to analyse whether the DSA could address this problem.