Confederation of Danish Industry

SVENSKT NÄRINGSLIV
SWEDISH ENTERPRISE

Confederation of Finnish Industries

Nordic comments to the Digital Services Act

The Nordic confederations: Confederation of Danish Industry, Confederation of Swedish Enterprises, and the Confederation of Finnish Industries have in collaboration the following main messages on the Digital Services Act (DSA).

Key messages

- We emphasize the importance of achieving rules that are proportionate and - as far as possible - principle-based and technology-neutral. This is crucial for ensuring predictability, encouraging innovative power and creating a positive investment climate.
- We strongly support restricting the DSA to illegal content.
- We support the DSA to apply the Country of Origin principle.
- We support upholding the country-of-origin principle and welcome enhanced coordination and cooperation across the EU, as this will ensure consistent application of the DSA and its core principles in all Member States.
- We support the proposal of maintaining the existing exemptions from liability of the e-Commerce Directive. However, in the upcoming negotiations, we encourage the negotiating parties to discuss ex ante obligations for online marketplaces, where it allows consumers to conclude distance contracts regarding dangerous goods with traders.
- We welcome the DSA to encourage the important proactive work on countering the existence of illegal content online.
- We encourage sufficient funding to strengthen the market surveillance authorities to keep online and offline markets safe.
- We welcome the DSA to apply exterritorial.
- We ask for clarification regarding extraterritorial enforcement power. We also need a better understanding of the scope of the DSA as well as the transparency requirements.

Starting point for our comments

We welcome harmonizing rules to combat illegal content online and countering fragmentation of the internal market. We also support rules that build on the existing liability regime of the e-Commerce Directive. Digital platforms should be exempted from liability, as long they meet certain conditions.

As there is no *one size fits all* approach the conditions must differ between different types of service providers and they must - as far as possible – be principle-based and technology-neutral. This is crucial for ensuring predictability, encouraging innovative power and creating a positive investment climate.

In addition, the conditions must be proportionate if they are to achieve their desired effect. They must not undermine the overall business models of the services, given the broad positive impact and the opportunities and incentives for innovation that they bring.

Illegal, but not harmful, content is covered

The definition of illegal content in article 2 includes all information that does not comply with EU law or the law of a Member State. We strongly support that the DSA is restricted to counteracting illegal content, to

resolve the major societal damage such content may cause. Counteracting the presence of legal but harmful content online is better handled through other regulatory strategies.

Maintenance of the Country of Origin Principle

We support upholding the Country of Origin principle (article 3(2) of the eCommerce Directive). If anything, this should be strengthened to ensure the single market functions correctly. However, Member States have diverged from this principle in practice and frequently used the derogations available to them (article 3(4) of the eCommerce Directive). Aside from the fact that each Member State can exempt national rules, there is, in practice, no agreement in the EU on the interpretation of the Country of Origin principle. Some Member States, like Denmark, interpret the principle in a way that it only pertains to public law, whereas other Member States interpret the principle as also pertaining to civil law in several areas. The principle is therefore difficult for some companies to navigate by and it gives rise to great uncertainty.

This is fragmenting the single market and treating online business models differently. Ultimately, the best way to ensure the effectiveness of single market legislation is to strengthen the cooperation between Member States. We therefore welcome enhanced coordination and cooperation across the EU.

We also ask for the Commission to monitor more closely how the Country of Origin principle is being applied in practice and whether derogations are indeed proportionate to achieve Member State public interest aims. Hence, it is important that the European Board for Digital Services ensures consistent application of the DSA and its core principles. The interpretation of the Country of Origin principle should therefore be added to the activity reporting of article 44.

Online marketplaces facilitating the sale of dangerous goods to consumers

Each year illegal goods are sold to consumers through an online marketplace without having a market actor to hold responsible. This negatively affects the internal market, competition and exposes consumers to a high risk. The proposed safeguards in the DSA do not effectively protect consumers against this issue as they take place after the illegal goods have been sold.

Therefore, we find it important to address this issue before the goods are placed on the European market and sold. In the upcoming negotiations, we encourage the co-legislators to discuss the need for introducing an obligation to monitor for online marketplaces, where it allows consumers to conclude distance contracts with traders regarding dangerous goods .This will account for incidences such as the sale of goods between a seller in a 3rd country and a consumer in the EU, and where there is no other manufacturer or importer in EU. Moreover, such extended responsibility should only apply to situations where the product is covered by the regulation listed in article 4(5) in the Market Surveillance Regulation (MSR). This 'sector-specific legislation' covers 18 regulations for example the safety of toys, electrical equipment, radio equipment and gas appliances.

The extended responsibility must be enforced without harming innovation and development of the platform economy. And the extended responsibility should only be upheld in terms of the DSA regulation as we agree with the current limited liability schemes and with the proposal above, we don't want to address civil liability. Fines should be proportionate and the DSA should make clear what constitutes a violation.

Strengthening market surveillance

We welcome the DSA to encourage service providers to act more proactively to counteract the existence of illegal content. Also, as described above, additional due diligence obligations are relevant for online marketplaces to reduce the sale of illegal goods to consumers. Nonetheless, it is the market surveillance authorities and not private actors that bear the prior responsibility for detecting and combating illegality online. However, many market surveillance authorities and other regulators involved with keeping online and offline markets safe are grossly under resourced. Therefore, we urge Member States to uphold their political

intentions and sufficiently fund the respective authorities and regulators responsible for enforcing existing frameworks and the DSA.

Legal representative

We support a horizontal regulatory framework that will also apply to the providers of digital services, who are not established in the EU but offer services that reach the internal market. We also support the introduction of a requirement for these digital service providers to have a legal representative within the EU (article 11), to facilitate extraterritorial and enforcement issues.

The enforcement possibilities against digital service providers that are not established in the EU must be clarified. It must further be specified to which extent the legal representative's liability in the EU differs from/coincides with the responsible person's liability according to the MSR. Member States currently await the Commission's instruction on article 4 of the MSR which shall indeed clarify what the responsible person's liability involves according to the MSR.

Definition of service providers

The DSA covers four different types of providers: intermediary services, hosting services, online platforms, and very large platforms. As the distinctions between the categories are not very detailed, further descriptions and examples of service providers falling within the different categories would be useful, making it clear to the companies what obligations they are subjected to.

Apart from this, it is essential to clarify whether a fulfilment service provider in the MSR can also be an online platform as defined in the DSA and thus be comprised by both sets of rules.

Active recipients

We need a clearer definition of what constitutes an 'active recipient', as this is decisive for the types of obligations that the service provider is subjected to. From the Commission's glossary it only appears that a user is either a physical or legal person using a service, e.g. accessing and looking at goods on a site. It could advantageously be specified what is understood by 'using' a service, for instance that it requires that the user does something actively on a service. It is not clear from the present definition, whether it is enough to consider a person a user if a person just downloads an app on their phone, without opening the app or log into their profile. Or whether a person is comprised, if he enters a website without logging in.

Transparency

For hosting service providers, article 14 introduces proposals for harmonised rules on how notifications of illegal content are to be handled (the so-called 'Notice-and-Action' mechanism). Article 15 also contains an obligation for service providers to justify decisions to delete or block access to certain information. It is important for business users to be informed where information placed online is later deemed illegal. This is irrespective of whether the assessment was made by a supervisory authority or by an intermediary of hosting services. Any requirements for transparency must not, however, increase the risk of hosting services being misused. It is also important to ensure that any requirements for transparency or any removal of illegal information is proportionate. Also, the requirements must not complicate the jurisdiction of law enforcement agencies.

Know Your Own Business Consumer (KYBC)

We agree with the obligation for online platforms to receive, store, make reasonable efforts to assess the reliability of and publish specific information on the traders using their services where those online platforms allow consumers to conclude distance contracts with those traders (article 22). We caution however that not all Member States have national identification documents as referred to in article 22(1)(b).

Online Advertisement

Targeted advertising is a form of advertising directed towards an audience with certain traits, based on the product or person the advertiser is promoting. This is a positive tool to ensure benefits for both parties: the recipient receives information that is more meaningful, and the advertising company ensures more efficient investment of its resources.

We agree with the need to provide transparency through article 24 and 30 to clearly identify an advertisement and the business user on whose behalf it is displayed. We also believe it is positive to compile relevant information regarding that advertisement. On the other hand, we believe some of the information regarding the advertisement (e.g. total number of recipients and the number of targeted recipients) could expose business secrets. It could also be difficult to apply for smaller platforms that simply sell advertising space without collecting the data which the advert uses. Overall, the application of the provisions on the transparency of online advertising must comply with the legislation protecting the trade secret (Directive 943/2016).

Compliance

It must be easy to do the right thing. What is illegal offline must be illegal online. However, it should not be the duty of service providers to decide what is illegal. National regulators, legislators, and courts - not private actors - must be responsible for these decisions. Most digital services operate or aim at operating cross-border. And we therefore support efficient cooperation between Member States to strengthen regulatory compliance within the digital environment. Further, we welcome the establishment of bodies to handle cases of disagreement between an online platform and the user on the platform. It is important that this body can set up a precedent, so companies do not have to raise complaints on removal of identical or similar content repeatedly, e.g. anti-5G groups or other disinformation. It will be far too cumbersome if all cases must go through this body.

Sanctions

The DSA should make clear what constitutes a violation and is finable. Regarding the enforcement of fines, the Member States and the Digital Services Coordinator play an important role. We have experienced with the GDPR, that some Member States are not able to issue financial fines through the competent national authority and the case is therefore referred to the police as the next step. In these circumstances, it is important, that we learn from our previous experiences and put in place a smooth process from the beginning as it otherwise creates an insecure situation for the business involved.