EPP Group Position on

THE DIGITAL SERVICES ACT (DSA)

19 January 2021

A) Harmonise the existing rules on the removal of illegal content: maintain the general concept behind Art 13/14 in the Directive on electronic commerce as well as the current notice-and-action procedures (notice and notice, notice and takedown, notice and stay down) as a baseline requirement for all platforms providing services in the European Digital Single Market. Harmonise those rules across Europe as much as possible and focus on clear definitions and effective procedures. However, the DSA should also go beyond that: proportional proactive measures (e.g. automated tools, repeating offender policies, the use of trusted flaggers, bulk notifications submissions, identity management) for platforms are necessary when illegal content becomes systemic, where the illegal character of the content has already been established (either through a substantiated notice or a judicial decision) or where the type of content and its nature of illegality is such that contextualisation is not necessary. The deployment of any such measures should, however, be accompanied with appropriate safeguards to make sure that content moderation practices are proportionate. Especially, in cases of incitement to terrorism, illegal hate speech, or child sexual abuse material as well as infringements of Intellectual Property Rights, we need a strong coordinated EU-wide approach to ensure that service providers take effective measures to remove illegal content from their services and ensure that such content remains inaccessible after being removed.

(B) Harmful content: legal takedown obligations should only concern illegal content, which is any content not in compliance with Union law or the law of a Member State. In spite of this, legal yet harmful content such as misinformation and disinformation on COVID-19 causes or remedies remain a serious problem. Harmful content therefore deserves a targeted (co-)regulatory approach outside of the DSA in order to clearly separate the procedures of tackling harmful or illegal content.

(C) Horizontal legislation: for maximum clarity and cohesion, the DSA should be a horizontal framework that is complemented by existing and future sector specific legislation, such as lex specialis (like Copyright, TCO, AVMSD, GDPR, etc.). The legislator shall avoid the collision of provisions and shall streamline definitions in the DSA and the respective sector specific legislations, recognising not only the general principles in the horizontal provisions but also the effect of the specific requirements in sister legislation, thereby avoiding any unintended consequences.

(D) Level playing field: recognises that there is nothing illegal or anti-competitive about building a successful business, which is what many large platforms are. Sees, however, the need to further differentiate between platforms (as much as this is legally possible) since some of them have developed excessive market power in the past decades and are abusing it. Therefore, they should not be subject to the same rules as small providers. Where it is demonstrated that consumer welfare is being eroded and innovation is being stifled by 'gatekeeper platforms' and where it is demonstrated that there is potential for increased competition in digital markets, that these markets are not contestable, and where innovation is being stifled by large platforms, then proportionate measures will be needed. Besides the goal of protecting European start-ups and SMEs, we need to consider - among others - the

size or the scale of reach of platforms as this is influencing their capability to operate proactive measures against illegal content online.

(E) Active/Passive platforms: review the classification of "active" or "passive" behaviour by incorporating the latest ECJ rulings and by streamlining DSA with the Copyright Directive. The DSA should also consider whether these types of platforms, as either hosting or caching, are still relevant since the role played by platforms today has become far more complex. The DSA should look at the purpose of the type of platform and provide appropriate definitions, roles and responsibilities in that context.

(F) Scope: extend the territorial scope of the DSA in order to also cover the activities of companies and service providers established in third countries as long as they offer their services also in the Digital Single Market. Oblige those third country providers to designate a legal representative for consumer interests within the EU, modelled after the GDPR. If a platform imports products into the EU, it always has to respect EU law on product safety, environmental and consumer protection, labelling or intellectual property, all of this according to our 'European Way of Life.' To better enable European companies to compete, innovate and scale up it is essential that we do not burden them with disproportionate administration and regulation. This is especially important for SMEs that have small margins and were already very highly impacted by the implementation of the GDPR.

(G) General monitoring: preserve the prohibition of imposing a general monitoring obligation (Art 15 e-commerce Directive). Combined with new mandatory transparency measures, platforms should, however, be allowed and even encouraged to use automated tools to detect manifestly illegal content voluntarily (e.g. by legal clarification that platforms are not liable if they deploy automated measures). The DSA could explore the possibility of a liability exemption for platforms related to their activity in the field of the fight against illegal content (also taking into account the US Good Samaritan principle).

(H) Oversight: aim for a full European harmonisation of legal obligations on procedures, procedural safeguards, moderation and transparency, including clear legal responsibilities and effective cross-border enforcement of those responsibilities on an EU level. Since not all Member States are adequately equipped - both in terms of tools and expertise - to enforce all obligations, the European Commission shall play a strong role in overseeing, coordinating and supporting the national enforcement bodies in order to ensure that no disproportionate burden falls on the regulatory body of one, or a small number of, Member States. The EPP Group does not advocate a new agency if this harmonisation can be done through a network of national enforcement bodies similar to the ECN (European Competition Network). The transparency obligations shall include the use and underlying source codes of algorithmic processes that handle the content. The compliance with these additional transparency and explainability requirements shall not be audited by private companies but shall fall under the competence of market surveillance authorities.

(I) Targeted advertising: targeted advertising shall be regulated under GDPR/ePrivacy/P2B. Some additional limitations in the DSA can be considered when the context is harmful to our democracy and if it is not yet covered by other legislation. Considers that, as a general principle, targeted advertising can have a positive economic and societal impact and points to the fact that existing legislation needs to be fully and properly enforced to ensure the respect of users' privacy. A ban on targeted advertisement is not supported by the EPP Group.

(J) Liability of platforms/media/users: use modern technology to identify, more effectively, how and by whom illegal content was published, thereby streamlining the accountability of the platform. The EPP Group firmly supports the right to be anonymous on the Internet (as it is acknowledged by the GDPR) but at the same time rejects the idea of being unidentifiable online (= what is illegal offline, is illegal online). To make sure that, while maintaining anonymity, everyone is digitally identifiable where this is necessary, a protected European digital identity should be created, using, for example, the block chain technology. The level of responsibility of the platforms should be tailored to the identifiability of the users. The responsibility of platforms for the content of media that they are hosting shall be reduced when the media (and thus also its content) is already regulated by the Member States. As a compromise, the EPP Group could accept that the DSA or another upcoming piece of legislation, such as the eIDAS-update, which makes a European digital identity

system mandatory for some platforms (e.g. selling physical goods, eGovernance services).

(K) Judicial order: establish a clear and efficient procedure for collaboration with law enforcement and judicial authorities, making sure that illegal content is not just taken down but also followed up on by law enforcement, and that responsibilities on platforms are coupled with effective enforcement measures.

(L) Public reporting obligations: require platforms and national competent authorities to report their action and thereby aim for a structured analysis of illegal content removal and blocking at EU level. Those obligations should be proportionate and moderate for SMEs and start-ups and, at the same time, exclude micro companies.

(M) Transparency obligations: require digital intermediaries (in business to business relations only) including domain name registrars, web hosting providers, marketplaces and online advertisers to put in place effective 'Know Your Business Customer Verification' schemes. Moreover, platforms should be transparent with regards to the policy they adopt when it comes to repeat infringers.