



TEXTS ADOPTED

P9_TA(2020)0272

Digital Services Act: Improving the functioning of the Single Market

European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL))

The European Parliament,

- having regard to Article 225 of the Treaty on the Functioning of the European Union,
- having regard to Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’)¹,
- having regard to 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 services²,
- having regard to Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services³,
- having regard to Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC⁴,
- having regard to Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’)⁵,

¹ OJ L 178, 17.7.2000, p. 1.

² OJ L 186, 11.7.2019, p. 57.

³ OJ L 136, 22.5.2019, p. 1.

⁴ OJ L 136, 22.5.2019, p. 28.

⁵ OJ L 149, 11.6.2005, p. 22.

- having regard to Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011¹,
- having regard to Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market²,
- having regard to its resolution of 21 September 2010 on completing the internal market for e-commerce³,
- having regard to its resolution of 15 June 2017 on online platforms and the digital single market⁴,
- having regard to the Communication from the Commission of 11 January 2012, entitled “A coherent framework for building trust in the Digital Single Market for e-commerce and online services” (COM(2011)0942),
- having regard to the Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online⁵ and the Communication from the Commission of 28 September 2017, entitled “Tackling Illegal Content Online: Towards an enhanced responsibility of online platforms” (COM(2017)0555),
- having regard to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 26 April 2018 on Tackling online disinformation: a European Approach (COM(2018)0236), which covers false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm,
- having regard to the Memorandum of Understanding on the sale of counterfeit goods via the internet of 21 June 2016 and its review in the Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee of 29 November 2017, entitled “A balanced IP enforcement system responding to today’s societal challenges” (COM(2017)0707),
- having regard to the opinion of the Committee of the Regions (ECON-VI/048) from 5 December 2019 on “a European framework for regulatory responses to the collaborative economy”,
- having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)⁶,

¹ OJ L 169, 25.6.2019, p. 1.

² OJ L 376, 27.12.2006, p. 36.

³ OJ C 50 E, 21.2.2012, p. 1.

⁴ OJ C 331, 18.9.2018, p. 135.

⁵ OJ L 63, 6.3.2018, p. 50.

⁶ OJ L 119, 4.5.2016, p. 1.

- having regard to 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/EC¹,
- having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)²,
- having regard to Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases³, Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society⁴ and 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)⁵,
- having regard to the Communication from the Commission of 10 March 2020, entitled “An SME Strategy for a sustainable and digital Europe” (COM(2020)0103),
- having regard to the White Paper on Artificial Intelligence - A European approach to excellence and trust” of 19 February 2020 (COM(2020)0065),
- having regard to the communication from the Commission of 19 February 2020, entitled “Shaping Europe’s digital future” (COM(2020)0067),
- having regard to the commitments made by the Commission in its “Political Guidelines for the next European Commission 2019-2024”,
- having regard to the study by the European Parliamentary Research Service, entitled “Mapping the cost of Non-Europe 2019-2024” that shows that the potential gain of completing the Digital Single Market for services could be up to €100 billion,
- having regard to the study by the European Parliament’s Policy Department for Economic, Scientific and Quality of Life Policies, entitled “The e-commerce Directive as the cornerstone of the Internal Market” that highlights four priorities for improving the e-Commerce Directive,
- having regard to the studies provided by the Policy Department for Economic, Scientific and Quality of Life Policies for the workshop on “E-commerce rules, fit for the digital age” organised by the Internal Market and Consumer Protection (IMCO) committee,

¹ OJ L 130, 17.5.2019, p. 92.

² OJ L 201, 31.7.2002, p. 37.

³ OJ L 77, 27.3.1996, p. 20.

⁴ OJ L 167, 22.6.2001, p. 10.

⁵ OJ L 95, 15.4.2010, p. 1.

- having regard to the European added value assessment study carried out by the European Parliamentary Research Service, entitled “Digital Services Act: European added value assessment”¹,
 - having regard to the Vade-Mecum to Directive 98/48/EC, which introduces a mechanism for the transparency of regulations on information society services,
 - having regard to Rules 47 and 54 of its Rules of Procedure,
 - having regard to the opinions of the Committee on Transport and Tourism, Committee on Culture and Education, Committee on Legal Affairs and Committee on Civil Liberties, Justice and Home Affairs,
 - having regard to the report of the Committee on the Internal Market and Consumer Protection (A9-0181/2020),
- A. whereas e-commerce influences the everyday lives of people, businesses and consumers in the Union, and when operated in a fair and regulated level playing field, may contribute positively to unlocking the potential of the Digital Single Market, enhance consumer trust and provide newcomers, including micro, small and medium enterprises, with new market opportunities for sustainable growth and jobs;
- B. whereas Directive 2000/31/EC (“the E-Commerce Directive”) has been one of the most successful pieces of Union legislation and has shaped the Digital Single Market as we know it today; whereas the E-Commerce Directive was adopted 20 years ago, the Digital Services Act package (“DSA”) should take into account the rapid transformation and expansion of e-commerce in all its forms, with its multitude of different emerging services, products, providers, challenges and various sector-specific legislations; whereas since the adoption of the E-Commerce Directive, the European Court of Justice (“the Court”) has issued a number of judgments in relation to it;
- C. whereas currently Member States have a fragmented approach to tackling illegal content online; whereas, as a consequence, the service providers concerned can be subject to a range of different legal requirements which are diverging as to their content and scope; whereas there seems to be a lack of enforcement and cooperation between Member States, and challenges with the existing legal framework;
- D. whereas digital services need to fully comply with rules related to fundamental rights, especially privacy, the protection of personal data, non-discrimination and the freedom of expression and information, as well as media pluralism and cultural diversity and the rights of the child, as enshrined in the Treaties and the Charter of Fundamental rights of the European Union (“the Charter”);
- E. whereas in its Communication “Shaping Europe’s digital future”, the Commission committed itself to adopting, as part of the DSA, new and revised rules for online platforms and information service providers, to reinforcing the oversight over platforms’ content policies in the Union, and to looking into *ex ante* rules;
- F. whereas the COVID-19 pandemic has brought new social and economic challenges that deeply affect citizens and the economy; whereas, at the same time, the COVID-19

¹ [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654180/EPRS_STU\(2020\)654180_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654180/EPRS_STU(2020)654180_EN.pdf)

pandemic is showing the resilience of the e-commerce sector and its potential as a driver for relaunching the European economy; whereas the pandemic has also exposed shortcomings of the current regulatory framework in particular with regard to consumer protection acquis; whereas that calls for action at Union level to have a more coherent and coordinated approach to address the difficulties identified and to prevent them from happening in the future;

- G. whereas the COVID-19 pandemic has also shown how vulnerable EU consumers are to misleading trading practices by dishonest traders selling illegal products online that are not compliant with Union safety rules and other unfair conditions on consumers; whereas the COVID-19 pandemic has shown in particular that platforms and online intermediation services need to improve their efforts to detect and take down false claims and to tackle the misleading practices of rogue traders in a consistent and coordinated manner, in particular of those selling false medical equipment or dangerous products online; whereas the Commission welcomed the approach by the platforms after sending them the letters on 23 March 2020; whereas there is a need for an action at Union level to have a more coherent and coordinated approach in order to combat these misleading practices and to protect consumers;
- H. whereas the DSA should ensure a comprehensive protection of the rights of consumers and users in the Union and therefore, its territorial scope should cover the activities of information society service providers established in third countries when their services, falling within the scope of the DSA, are directed at consumers or users in the Union;
- I. whereas the DSA should clarify the nature of the digital services, falling within its scope, while maintaining the horizontal nature of the E-Commerce Directive, applying not only to online platforms, but to all providers of information society services as defined in Union law;
- J. whereas the DSA should be without prejudice to Regulation (EU) 2016/679 (“GDPR”) setting out a legal framework to protect personal data, Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market, Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services, and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector;
- K. whereas the DSA should not affect Directive 2005/29/EC as amended by Directive (EU) 2019/2161, as well as Directives (EU) 2019/770 and (EU) 2019/771 on certain aspects concerning contracts for the supply of digital content and digital services and contracts for the sale of goods, and Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services;
- L. whereas the DSA should be without prejudice to the framework set out by Directive 2006/123/EC on services in the internal market;
- M. whereas certain types of illegal content, constituting a major cause for concern, have already been defined in national and Union law, such as illegal hate speech, and should not be redefined in the DSA;
- N. whereas enhancing transparency and helping citizens to acquire media and digital literacy regarding the dissemination of harmful content, hate speech and disinformation,

as well as to develop critical thinking, and strengthening independent professional journalism and quality media will help promote diverse and quality content;

- O. whereas the WHOIS database is a publicly accessible database which has been a useful instrument to find the owner of a particular domain name on the internet as well as the details and contact person of every domain name;
- P. whereas the DSA should aim at ensuring legal certainty and clarity, including in the short-term rental market and mobility services, by promoting transparency and clearer information obligations;
- Q. whereas the Commission's agreement with certain platforms of the short-term rental sector on data sharing reached in March 2020 will enable local authorities to better understand the development of the collaborative economy and will allow for reliable and continuous data sharing and an evidence based policy making; whereas further steps to initiate a more comprehensive data sharing framework for short-term rental online platforms is needed;
- R. whereas the COVID-19 pandemic had a serious impact on the Union tourism sector and showed the need to continue supporting cooperation on green corridors in order to ensure the smooth functioning of Union supply chains and movement of goods across the Union transport network;
- S. whereas the evolving development and use of internet platforms for a wide set of activities, including commercial activities, transport and tourism and sharing goods and services, have changed the ways in which users and companies interact with content providers, traders and other individuals offering goods and services; whereas the Digital Single Market cannot succeed without users' trust in online platforms that respect all applicable legislation and their legitimate interests; whereas any future regulatory framework should also address intrusive business models, including behavioural manipulation and discriminatory practices, which have major effects to the detriment of the functioning of the Single Market and to users' fundamental rights;
- T. whereas Member States should make efforts to improve access to, and the efficiency of, their justice and law enforcement systems in relation to determining the illegality of online content and in relation to dispute resolution concerning removal of content or disabling access;
- U. whereas the DSA requirements should be easy to implement in practice by providers of information society services; whereas online intermediaries might encrypt or otherwise prevent access to content by third parties, including the hosting intermediaries storing the content itself;
- V. whereas an effective way to decrease illegal activities is allowing new innovative business models to flourish and strengthening the Digital Single Market by removing unjustified barriers to the free movement of digital content; whereas barriers, which create national fragmented markets, help create a demand for illegal content;
- W. whereas digital services should provide consumers with direct and efficient means of user-friendly, easily identifiable and accessible communication, such as email addresses, electronic contact forms, chatbots, instant messaging or telephone callback, and should provide for the information relating to those means of communication to be

accessible to consumers in a clear, comprehensible and, where possible, uniform manner, and for consumers requests to be directed between different underlying digital services of the digital service provider;

- X. whereas the DSA should guarantee the right for consumers to be informed if a service is enabled by artificial intelligence (“AI”), makes use of automated decision-making or machine learning tools or automated content recognition tools; whereas the DSA should offer the possibility to opt-out, limit or personalise the use of any automated personalisation features especially in view of rankings and more specifically, offer the possibility to see content in a non-curated order, give more control to users on the way content is ranked;
- Y. whereas the protection of personal data, subject to automated decision-making processes, is already covered, among others, by the GDPR and the DSA should not seek to repeat or amend such measures;
- Z. whereas the Commission should ensure that the DSA preserves the human centric approach to AI, in line with the existing rules on free movement of AI enabled services, while respecting the fundamental values and rights as enshrined in the Treaties;
- AA. whereas the national supervisory authorities, where allowed by Union law, should have access to the software documentation and data sets of algorithms under review;
- AB. whereas the concepts of transparency and explainability of algorithms should be understood as requiring that the information provided for the user is presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- AC. whereas it is important to lay down measures to ensure effective enforcement and supervision; whereas the compliance with the provisions should be reinforced with effective, proportionate and dissuasive penalties, including the imposition of proportionate fines;
- AD. whereas the DSA should balance the rights of all users and ensure that its measures are not drafted to favour one legitimate interest over another and to prevent the use of measures as offensive tools in any conflicts between businesses or sectors;
- AE. whereas the *ex ante* internal market mechanism should apply where competition law alone is insufficient to adequately address identified market failures;
- AF. whereas the legislative measures proposed as part of the DSA should be evidence based; whereas the Commission should carry out a thorough impact assessment, based on relevant data, statistics, analyses and studies of the different options available; whereas that impact assessment should also assess and analyse unsafe and dangerous products sold through online marketplaces; whereas the impact assessment should also take into account the lessons learned from the COVID-19 pandemic and take into account the resolutions from the European Parliament; whereas the DSA should be accompanied by implementation guidelines;

General principles

1. Welcomes the Commission’s commitment to submit a proposal for a Digital Services Act package (“DSA”), which should consist of a proposal amending the E-Commerce

Directive and a proposal for *ex ante* rules on systemic operators with a gatekeeper role, on the basis of Article 225 of the Treaty on the Functioning of the European Union (TFEU); calls on the Commission to submit such a package on the basis of Articles 53(1), 62 and 114 TFEU, following the recommendations set out in the Annex to this resolution, on the basis of a thorough impact assessment which should include information on the financial implications of the proposals and be based on relevant data, statistics and analyses;

2. Recognises the importance of the legal framework set out by the E-Commerce Directive in the development of online services in the Union and believes that the principles that governed the legislators when regulating information society services providers in the late 90s are still valid and should be used when drafting any future proposals; highlights that the legal certainty brought by the E-Commerce Directive has provided small and medium enterprises (SMEs) with the opportunity to expand their business and to operate more easily across borders;
3. Is of the opinion that all providers of digital services established outside the Union must adhere to the rules of the DSA when directing services to the Union, in order to ensure a level playing field between European and third country digital service providers; asks the Commission to evaluate in addition whether there is a risk of retaliatory measure by third countries, while raising awareness on how Union law applies to service providers from third countries targeting the Union market;
4. Underlines the central role that the internal market clause, establishing the home country control and the obligation on Member States to ensure the free movement of information society services, has played in the development of the Digital Single Market; stresses the need to address the remaining unjustified and disproportionate barriers to the provision of digital services, such as complex administrative procedures, costly cross-border disputes settlements and access to information on the relevant regulatory requirements, including on taxation, as well as to ensure that no new unjustified and disproportionate barriers are created;
5. Notes that under the Union rules on free movement of services, Member States may take measures to protect legitimate public interest objectives, such as protection of public policy, public health, public security, consumer protection, combating the rental housing shortage, and prevention of tax evasion and avoidance, provided that those measures comply with the principles of non-discrimination and proportionality;
6. Considers that the main principles of the E-Commerce Directive, such as the internal market clause, freedom of establishment, the freedom to provide services and the prohibition on imposing a general monitoring obligation should be maintained; underlines that the principle of “what is illegal offline is also illegal online”, as well as the principles of consumer protection and user safety, should also become guiding principles of the future regulatory framework;
7. Highlights the importance of collaborative economy platforms, including in the transport and tourism sectors, on which services are provided by both individuals and professionals; calls on the Commission, following a consultation with all relevant stakeholders to initiate a more comprehensible sharing of non-personal data and coordination framework between platforms and national, regional and local authorities, aiming especially at sharing best practices and establishing a set of information obligations, in line with the EU Data Strategy;

8. Notes that the data protection regime has been significantly updated since the adoption of the E-Commerce Directive and emphasises that the rapid development of digital services requires a strong futureproof legislative framework to protect personal data and privacy; stresses in this regard that digital service providers need to comply with the requirements of Union data protection law, namely the GDPR and Directive 2002/58/EC (“the e-Privacy Directive”), currently under revision, with the broad framework of fundamental rights including, the freedom of expression, dignity and non-discrimination, and the right to an effective judicial remedy, and to ensure the security and safety of their systems and services;
9. Believes that the DSA should ensure consumer trust and clearly establish that consumer law and product safety requirements are complied with, in order to ensure legal certainty; points out that the DSA should pay special attention to users with disabilities and guarantee the accessibility of information society services; asks the Commission to encourage service providers to develop technical tools that allow persons with disabilities to effectively access, use and benefit from information society services;
10. Stresses the importance of maintaining the horizontal approach of the E-Commerce Directive; stresses, that “one-size-fits-all” approach is not suitable to address all the new challenges in today’s digital landscape and that the diversity of actors and services offered online needs a tailored regulatory approach; recommends distinguishing between economic and non-economic activities, and between different type of digital services hosted by platforms, rather than focusing on the type of the platform; considers, in this context, that any future legislative proposals should seek to ensure that new Union obligations on information society service providers are proportional and clear in nature;
11. Recalls that a large number of legislative and administrative decisions and contractual relationships use the definitions and the rules of the E-Commerce Directive, and that any change to them will, therefore, have important consequences;
12. Stresses that a predictable, future-proof, clear and comprehensive Union-level framework and fair competition are crucial in order to promote the growth of all European businesses, including small-scale platforms, SMEs, including micro companies, entrepreneurs and start-ups, to increase cross-border provision of information society services, to remove market fragmentation and to provide European businesses with a level playing field that enables them to fully take advantage of the digital services market and to be globally competitive on the world stage;
13. Underlines that the future internal market instrument on *ex ante* rules on systemic platforms and the announced new Competition Tool aiming at addressing gaps in competition law should be kept as separate legal instruments;
14. Recalls that the E-Commerce Directive was drafted in a technologically neutral manner to ensure that it is not rendered obsolete by technological developments arising from the fast pace of innovation in the IT sector and stresses that the DSA should continue to be future-proof and applicable to the emergence of new technologies with an impact on the digital single market; asks the Commission to ensure that any revisions continue to be technology-neutral in order to guarantee long-lasting benefits to businesses and consumers;

15. Takes the view that a level playing field in the internal market between the platform economy and the offline economy, based on the same rights and obligations for all interested parties - consumers and businesses - is needed; considers that the DSA should not tackle the issue of platform workers; believes therefore that social protection and social rights of workers, including of platform or collaborative economy workers, should be properly addressed in a separate instrument, in order to provide an adequate and comprehensive response to the challenges of today's digital economy;
16. Considers that the DSA should be based on the common values of the Union that protect citizens' rights and should aim to foster the creation of a rich and diverse online ecosystem with a wide range of online services, a competitive digital environment, transparency and legal certainty to unlock the full potential of the Digital Single Market;
17. Considers that the DSA provides an opportunity for the Union to shape the digital economy, not only at Union level, but also be a standard-setter for the rest of the world;

Fundamental rights and freedoms

18. Notes that information society services providers, and in particular online platforms, including social networking sites, have a wide-reaching ability to reach and influence broader audiences, behaviour, opinions, and practices, including vulnerable groups such as minors, and should comply with Union law on protecting users, their data and society at large;
19. Recalls that recent scandals regarding data harvesting and selling, such as Cambridge Analytica, fake news, disinformation, voter manipulation and a host of other online harms (from hate speech to the broadcast of terrorism) have shown the need to work on better enforcement and closer cooperation among Member States in order to understand the advantages and shortcomings of the existing rules and to reinforce the protection of fundamental rights online;
20. Recalls in this respect that certain established self-regulatory and co-regulatory schemes such as the Union's Code of Practice on Disinformation have helped to structure a dialogue with platforms and regulators; suggests that online platforms should place effective and appropriate safeguards, in particular to ensure that they act in a diligent, proportionate and non-discriminatory manner, and to prevent the unintended removal of content which is not illegal; such measures should not lead to any mandatory 'upload-filtering' of content which does not comply with the prohibition of general monitoring obligations; suggests that measures to combat harmful content, hate speech and disinformation should be regularly evaluated and developed further;
21. Reiterates the importance of guaranteeing freedom of expression, information and opinion, and of having a free and diverse press and media landscape, also in view of the protection of independent journalism; insists on the protection and promotion of freedom of expression and on the importance of having a diversity of opinions, information, the press, media and artistic and cultural expressions;
22. Stresses that the DSA should strengthen the internal market freedoms and guarantee the fundamental rights and principles set out in the Charter; stresses that consumers' and users' fundamental rights, including those of minors, should be protected from harmful online business models, including those conducting digital advertising, as well as from behavioural manipulation and discriminatory practices;

23. Emphasises the importance of user empowerment with regard to the enforcement of their own fundamental rights online; reiterates that digital service providers must respect and enable their users' right to data portability as laid down in Union law;
24. Points out that biometric data is considered to be a special category of personal data with specific rules for processing; notes that biometrics can and are increasingly used for identification and authentication of individuals, which, regardless of its potential advantages, entails significant risks to, and serious interferences with, the rights to privacy and data protection, particularly when carried out without the consent of the data subject, as well as enabling identity fraud; calls on the DSA to ensure that digital service providers store biometric data only on the device itself, unless central storage is allowed by law, to always give users of digital services an alternative for using biometric data set by default for the functioning of a service, and the obligation to clearly inform the customers on the risks of using biometric data;
25. Stresses that, in the spirit of the case-law on communications metadata, public authorities shall be given access to a user's subscriber data and metadata only to investigate suspects of serious crimes with prior judicial authorisation; is convinced, however, that digital service providers must not retain data for law enforcement purposes unless a targeted retention of an individual user's data is directly ordered by an independent competent public authority, in line with Union law;
26. Stresses the importance to apply effective end-to-end encryption to data, as it is essential for trust in and security on the Internet, and effectively prevents unauthorised third party access;

Transparency and consumer protection

27. Notes that the COVID-19 pandemic has shown the importance and resilience of the e-commerce sector and its potential as a driver for relaunching the European economy, but at the same time how vulnerable EU consumers are to misleading trading practices by dishonest traders selling counterfeit, illegal or unsafe products, and providing services online that are not compliant with Union safety rules or who impose unjustified and abusive price increases or other unfair conditions on consumers; stresses the urgent need to step up enforcement of Union rules and to enhance consumer protection;
28. Stresses that this problem is aggravated by difficulties in establishing the identity of fraudulent business users, thus making it difficult for consumers to seek compensation for the damages and losses experienced;
29. Considers that the current transparency and information requirements set out in the E-Commerce Directive on information society services providers and their business customers, and the minimum information requirements on commercial communications, should be strengthened in parallel with measures to increase compliance with existing rules, without harming the competitiveness of SMEs;
30. Calls on the Commission to reinforce the information requirements set out in Article 5 of the E-Commerce Directive and to require hosting providers to compare the information and identity of the business users with whom they have a direct commercial relationship, with the identification data by the relevant existing and available Union databases, in compliance with data protocol legislation; hosting providers should ask their business users to ensure that the information they provide is accurate, complete

and updated and should be entitled and obliged to refuse or cease to provide their services to the latter, if the information about the identity of their business users is false or misleading; business users should be the ones in charge of notifying the service provider about any change in their business activity (for example, cessation of business activity);

31. Calls on the Commission to introduce enforceable obligations on information society service providers aiming at increasing transparency, information and accountability; calls on the Commission to ensure that enforcement measures are targeted in a way that takes into account the different services and does not inevitably lead to a breach of privacy and legal process; considers that those obligations should be proportionate and enforced by appropriate, effective, proportionate and dissuasive penalties;
32. Stresses that existing obligations, set out in the E-Commerce Directive and the Unfair Commercial Practices Directive on transparency of commercial communications and digital advertising, should be strengthened; points out that pressing consumer protection concerns about profiling, targeting and personalised pricing should be addressed, among others, by clear transparency obligations and information requirements;
33. Stresses that online consumers find themselves in an unbalanced relation to service providers and traders offering services supported by advertising revenue and advertisements that are directly targeting individual consumers, based on the information collected through big data and AI mechanisms; notes the potential negative impact of personalised advertising, in particular micro-targeted and behavioural advertisement; calls, therefore, on the Commission to introduce additional rules on targeted advertising and micro-targeting, based on the collection of personal data and to consider regulating micro- and behavioural targeted advertising more strictly in favour of less intrusive forms of advertising that do not require extensive tracking of user interaction with content; urges the Commission to also consider introducing legislative measures to make online advertising more transparent;
34. Underlines the importance, in view of the development of digital services, of the obligation for Member States to ensure that their legal system allows for contracts to be concluded by electronic means, while ensuring a high level of consumer protection; invites the Commission to review the existing requirements on contracts concluded by electronic means, including as regards notifications by Member States, and to update them if necessary; notes, in that context, the rise of “smart contracts” such as those based on distributed ledger technologies and asks the Commission to assess the development and use of distributed ledger technologies, including “smart contracts”, such as regards questions of validity and enforcement of smart contracts in cross-border situations, to provide guidance thereon, in order to ensure legal certainty for businesses and consumers, and to take legislative initiatives only if concrete gaps are identified following that assessment;
35. Calls on the Commission to introduce minimum standards for contract terms and general conditions, in particular with regard to transparency, accessibility, fairness and non-discriminatory measures, and to further review the practice of pre-formulated standard clauses in contract terms and conditions, which have not been individually negotiated in advance, including End-User Licensing Agreements, to seek ways of making them fairer and to ensure compliance with Union law, in order to allow easier engagement for consumers, including in the choice of clauses, to make it possible to obtain better informed consent;

36. Stresses the need to improve the efficiency of electronic interactions between businesses and consumers in light of the development of virtual identification technologies; considers that in order to ensure the effectiveness of the DSA, the Commission should also update the regulatory framework on digital identification, namely Regulation (EU) No 910/2014¹ (“the eIDAS Regulation”); considers that the creation of a universally accepted, trusted digital identity and trusted authentication systems would be a useful tool allowing to establish securely individual identities of natural persons, legal entities and machines in order to protect against the use of fake profiles; notes, in this context, the importance for consumers to securely use or purchase products and services online without having to use unrelated platforms and unnecessarily share data, including personal data, which is collected by those platforms; calls on the Commission to carry out a thorough impact assessment with regard to the creation of a universally accepted public electronic identity as an alternative to private single sign-in systems and underlines that this service should be developed so that data gathered is kept to an absolute minimum; considers that the Commission should assess the possibility to create an age verification system for users of digital services, especially in order to protect minors;
37. Stresses that the DSA should not affect the principle of data minimisation established by the GDPR, and, unless required by specific legislation otherwise, intermediaries of digital services should enable the anonymous use of their services to the maximum extent possible and only process data necessary for the identification of the user; that such collected data should not be used for any other digital services than those that require personal identification, authentication or age verification and that they should only be used with a legitimate purpose, and in no way to restrain general access to the internet;

AI and machine learning

38. Stresses that while AI-driven services or services making use of automated decision-making tools or machine learning tools, currently governed by the E-Commerce Directive, have the enormous potential to deliver benefits to consumers and service providers, the DSA should address the concrete challenges they pose in terms of ensuring non-discrimination, transparency, including on the datasets used and on targeted outputs, and understandable explanation of algorithms, as well as liability, which are not addressed in existing legislation;
39. Stresses furthermore that underlying algorithms need to fully comply with requirements on fundamental rights, especially privacy, the protection of personal data, the freedom of expression and information, the right to an effective judicial remedy, and the rights of the child, as enshrined in the Treaties and the Charter;
40. Considers that it is essential to ensure the use of high quality, non-discriminatory and unbiased underlying datasets, as well as to help individuals acquire access to diverse content, opinions, high quality products and services;
41. Calls on the Commission to introduce transparency and accountability requirements regarding automated decision-making processes, while ensuring compliance with

¹ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

requirements on user privacy and trade secrets; points out the need to allow for external regulatory audits, case-by-case oversight and recurrent risk assessments by competent authorities and to assess associated risks, in particular risks to consumers or third parties, and considers that measures taken to prevent those risks should be justified and proportionate, and should not hamper innovation; believes that the ‘human in command’ principle must be respected, *inter alia*, to prevent the rise of health and safety risks, discrimination, undue surveillance, or abuses, or to prevent potential threats to fundamental rights and freedoms;

42. Considers that consumers and users should have the right to be properly informed in a timely, concise and easily understandable and accessible manner, and that their rights should be effectively guaranteed when they interact with automated decision-making systems and other innovative digital services or applications; expresses concerns with regard to the existing lack of transparency as to the use of virtual assistants or chatbots, which may be particularly harmful to vulnerable consumers and underlines that digital service providers should not exclusively use automated decision-making systems for consumer support;
43. Believes, in that context, that it should be possible for consumers to be clearly informed when interacting with automated decision-making, and about how to reach a human with decision-making powers, how to request checks and corrections of possible mistakes resulting from automated decisions, as well as to seek redress for any damage related to the use of automated decision-making systems;
44. Underlines the importance to strengthen consumer choice, consumer control and consumer trust in AI services and applications; believes, therefore, that the set of rights of consumers should be expanded to better protect them in the digital world and calls on the Commission to consider in particular accountability and fairness criteria and control and the right to non-discrimination and unbiased AI datasets; considers that consumers and users should have more control on how AI is used and the possibility to refuse, limit or personalise the use of any AI-enabled personalisation features;
45. Notes that automated content moderation tools are incapable of effectively understanding the subtlety of context and meaning in human communication, which is necessary to determine whether assessed content may be considered to violate the law or terms of service; stresses therefore that the use of such tools should not be imposed by the DSA;

Tackling Illegal Content and Activities Online

46. Stresses that the existence and spread of illegal content and activities online is a severe threat that undermines citizens’ trust and confidence in the digital environment, harms the development of healthy digital ecosystems, and may also have serious and long-lasting consequences for the safety and fundamental rights of individuals; notes that, at the same time, illegal content and activities can be proliferated easily and their negative impact amplified within a very short period of time;
47. Notes that there is no ‘one size fits all’ solution to all types of illegal content and activities; stresses that content that might be illegal in some Member States, may not be ‘illegal’ in others, as only some types of illegal content are harmonised in the Union; calls for a strict distinction to be made between illegal content, punishable acts and illegally shared content on the one hand, and harmful content, hate speech and

disinformation on the other, which are not always illegal and cover many different aspects, approaches and rules applicable in each case; takes the position that the legal liability regime should concern illegal content only as defined in Union or national law;

48. Believes, however, that, without prejudice to the broad framework of fundamental rights and existing sector-specific legislation, a more aligned and coordinated approach at Union level, taking into account the different types of illegal content and activities and based on cooperation and exchange of best practices between the Member States, will help address illegal content more effectively; underlines also the need to adapt the severity of the measures that need to be taken by service providers to the seriousness of the infringement and calls for improved cooperation and exchange of information between competent authorities and hosting service providers;
49. Considers that voluntary actions and self-regulation by online platforms across Europe have brought some benefits, but a clear legal framework for the removal of illegal content and activities is needed in order to ensure the swift notification and removal of such content online; underlines the need to prevent imposing a general monitoring obligation on digital service providers to monitor the information which they transmit or store and to prevent actively seeking, moderating or filtering all content and activities, neither *de jure* nor *de facto*; underlines that illegal content should be removed where it is hosted, and that access providers shall not be required to block access to content;
50. Calls on the Commission to ensure that online intermediaries, who, on their own initiative, take allegedly illegal content offline, to do so in a diligent, proportionate and non-discriminatory manner, and with due regard in all circumstances to the fundamental rights and freedoms of the users; underlines that any such measures should be accompanied by robust procedural safeguard and meaningful transparency and accountability requirements; and asks, where any doubts exist as to a content's 'illegal' nature, that this content should be subject to human review and not be removed without further investigation;
51. Asks the Commission to present a study on the removal of content and data before and during the COVID-19 pandemic by automated decision-making processes and on the level of removals in error (false positives) that were included in the number of items removed;
52. Calls on the Commission to address the increasing differences and fragmentations of national rules in the Member States and to adopt clear and predictable harmonised rules and a transparent, effective and proportionate notice-and-action mechanism; it should provide sufficient safeguards, empower users to notify online intermediaries of the existence of potentially illegal online content or activities and help online intermediaries react quickly and be more transparent with the actions taken on potentially illegal content; is of the opinion that such measures should be technology-neutral and easily accessible to all actors to guarantee a high level of users' and consumers' protection;
53. Stresses that such a 'notice-and-action' mechanism must be human-centric; underlines that safeguards against the abuse of the system should be introduced, including against repeated false flagging, unfair commercial practices and other schemes; urges the Commission to ensure access to transparent, effective, fair, and expeditious counter-notice and complaint mechanisms and out-of-court dispute settlement mechanisms and to guarantee the possibility to seek judicial redress against content removal to satisfy the right to effective remedy;

54. Welcomes efforts to bring transparency to content removal; calls on the Commission to ensure that reports with information about the notice-and-action mechanisms, such as the number of notices, type of entities notifying content, nature of the content subject of complaint, response time by the intermediary, the number of appeals as well as the number of cases where content was misidentified as illegal or as illegally shared should be made publicly available;
55. Notes the challenges concerning the enforcement of legal injunctions issued within Member States other than the country of origin of a service provider and stresses the need to investigate this issue further; maintains that hosting service providers shall not be required to remove or disable access to information that is legal in their country of origin;
56. Stresses that the responsibility for enforcing the law, deciding on the legality of online activities and content, as well as ordering hosting service providers to remove or disable access to illegal content and that those orders are accurate, well-founded and respect fundamental rights, rests with independent competent public authorities;
57. Stresses that maintaining safeguards from the legal liability regime for online intermediaries set out in Articles 12, 13, 14 of the E-Commerce Directive and the general monitoring prohibition set out in Article 15 of the E-Commerce Directive are pivotal for facilitating the free movement of digital services, for ensuring the availability of content online and for protecting the fundamental rights of users and need to be preserved; in this context, underlines that the legal liability regime and ban on general monitoring should not be weakened via a possible new piece of legislation or the amendment of other sections of the E-commerce Directive;
58. Acknowledges the principle that digital services playing a neutral and passive role, such as backend and infrastructure services, are not responsible for the content transmitted over their services because they have no control over that content, have no active interaction with it or do not optimise it; stresses however, that further clarification regarding active and passive role by taking into account the case-law of the Court on the matter is needed;
59. Calls on the Commission to consider a requirement for hosting service providers to report illegal content, which may constitute a serious crime to the competent law enforcement authority, upon becoming aware of it;

Online marketplaces

60. Notes that, while the emergence of online service providers, such as online marketplaces, has benefited both consumers and traders, notably by improving choice, reducing costs and lowering prices, it has also made consumers more vulnerable to misleading trading practices by an increasing number of sellers, including from third countries, who are able to offer online illegal, unsafe or counterfeit products and services which often do not comply with Union rules and standards on product safety, and do not sufficiently guarantee consumer rights;
61. Stresses that consumers should be equally safe when shopping online or in stores; stresses that it is unacceptable that Union consumers are exposed to illegal, counterfeit and unsafe products, containing dangerous chemicals, as well as other safety hazards that pose risks to human health; insists on the necessity to introduce appropriate

safeguards and measures for product safety and consumer protection in order to prevent the sale of non-compliant products or services on online marketplaces, and calls on the Commission to reinforce the liability regime on online marketplaces;

62. Stresses the importance of the rules of Regulation (EU) 2019/1020 on market surveillance and compliance of products about conformity of products entering the Union from third countries; calls on the Commission to take measures to improve compliance with legislation by sellers established outside the Union where there is no manufacturer, importer or distributor established in the Union and to remedy any current legal loophole which allows suppliers established outside the Union to sell online to European consumers products which do not comply with Union rules on safety and consumer protection, without being sanctioned or liable for their actions and leaving consumers with no legal means to enforce their rights or being compensated by any damages; stresses, in this context, the need for a possibility to always identify manufacturers and sellers of products from third countries;
63. Emphasises the need for online marketplaces to inform consumers promptly once a product they have purchased has been removed from the marketplace following a notification on its non-compliance with Union product safety or consumer protection rules;
64. Stresses the need to ensure that the providers of online marketplaces consult RAPEX and notify competent authorities as soon as they become aware of illegal, unsafe and counterfeit products on their platforms;
65. Considers that the providers of online marketplaces should enhance their cooperation with market surveillance authorities and the customs authorities, including by exchanging information on the seller of illegal, unsafe and counterfeit products;
66. Calls on the Commission to urge Member States to undertake more joint market surveillance actions and to step up collaboration with customs authorities in order to check the safety of products sold online before they reach consumers; asks the Commission to explore the possibility of the creation of an international network of consumer centres to help EU consumers in handling disputes with traders based in non-EU countries;
67. Asks the Commission to ensure that where online marketplaces offer professional services, a sufficient level of consumer protection is achieved through adequate safeguards and information requirements;
68. Believes that, in the tourism and transport market, the DSA should aim at ensuring legal certainty and clarity by creating a governance framework formalising the cooperation between platforms and national, regional and local authorities aiming especially at sharing best practices and establishing a set of information obligations of short-term rental and mobility platforms vis-à-vis their service providers concerning relevant national, regional and local legislation; calls on the Commission to further remove unjustified barriers by devising a sector-specific EU-coordinated effort involving all stakeholders to agree on sets of criteria, such as permits, or licenses, or, where applicable, a local or national registration number of a service provider, in line with Single Market rules, necessary to offer a service on a short term rental or mobility platform; stresses the importance to avoid imposing disproportionate information

obligations and unnecessary administrative burden on all providers of services with particular emphasis on peer-to-peer service providers and SMEs;

69. Calls on the DSA, in line with the European Green deal, to promote sustainable growth and sustainability of e-commerce; stresses the importance of online marketplaces for promoting sustainable products and services and encouraging sustainable consumption; calls for measures to tackle misleading practices and disinformation regarding products and services offered online, including false ‘environmental claims’ while calling on the providers of online marketplaces to promote sustainability of e-commerce by providing consumers with clear and easily understandable information on the environmental impact of the products or services they buy online;
70. Invites the Commission to examine thoroughly the clarity and consistency of the existing legal framework applying to the online sale of products and services in order to identify possible gaps and contradictions and lack of effective enforcement; asks the Commission to conduct a thorough analysis of the interaction between the DSA and the Union product safety and chemicals legislation; asks the Commission to ensure consistency between the new rules on online marketplaces and the revision of Directive 2001/95/EC¹ (“the General Product Safety Directive”) and Directive 85/374/EEC² (“the Product Liability Directive”);
71. Notes the continued issues of the abuse or wrong application of selective distribution agreements to limit the availability of products and services across borders within the Single Market and between platforms; asks the Commission to act on this issue within any wider review of Vertical Bloc Exemptions and other policies under Article 101 TFEU, while refraining from its inclusion in the DSA;

***Ex ante* regulation of systemic operators**

72. Notes that, today, some markets are characterised by large operators with significant network effects which are able to act as de facto “online gatekeepers” of the digital economy (“systemic operators”); stresses the importance of fair and effective competition between online operators with significant digital presence and other providers in order to promote consumer welfare; asks the Commission to conduct a thorough analysis of the different issues observed in the market so far and its consequences including on consumers, SMEs and the internal market;
73. Considers that by reducing barriers to market entry and by regulating systemic operators, an internal market instrument imposing *ex ante* regulatory remedies on those systemic operators with significant market power has the potential to open up markets to new entrants, including SMEs, entrepreneurs, and start-ups, thereby promoting consumer choice and driving innovation beyond what can be achieved by competition law enforcement alone;
74. Welcomes the Commission’s public consultation on the possibility of introducing, as part of the future DSA, a targeted *ex ante* regulation to tackle systemic issues which are

¹ Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4).

² Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29).

specific to digital markets; stresses the intrinsic complementarity between internal market regulation and competition policy, as emphasised in the report by the Commission's special advisers entitled "Competition Policy for the Digital Era";

75. Calls on the Commission to define 'systemic operators' on the basis of clear indicators;
76. Considers that the *ex ante* regulation should build upon Regulation (EU) 2019/1150 ("the Platform to Business Regulation") and its measures should be in line with the Union's antitrust rules and within the Union's policy on competition, which is currently under revision, to better address the challenges in the digital age; the *ex ante* regulation should ensure fair trading conditions applicable to all operators, including possible additional requirements and a closed list of the positive and negative actions such operators are required to comply with and/ or forbidden to engage in;
77. Calls on the Commission to analyse in particular the lack of transparency for recommendation systems of systemic operators including for the rules and criteria for the functioning of such systems and whether additional transparency obligations and information requirements need to be imposed;
78. Highlights that the imposition of *ex ante* regulatory remedies in other sectors has improved competition in those sectors; notes that a similar framework could be developed for identifying systemic operators with a "gatekeeper" role taking into account the specificities of the digital sector;
79. Draws attention to the fact that the size of business users of systemic operators varies from multinationals to micro-enterprises; underlines that *ex ante* regulation on systemic operators should not lead to the "trickling down" of additional requirements for the businesses that use them;
80. Underlines that the accumulation and harvesting of vast amounts of data and the use of such data by systemic operators to expand from one market into another, as well as the further possibility to push users to use a single operator's e-identification for multiple platforms, can create imbalances in bargaining power and, thus, leads to the distortion of competition in the Single Market; considers that increased transparency and data sharing, between systemic operators and competent authorities is crucial in view of guaranteeing the functioning of an *ex ante* rule regulation;
81. Underlines that interoperability is key to enable competitive market, as well as users' choice and innovative services, and to limit the risk of users' and consumers' lock-in effect; calls on the Commission to ensure appropriate levels of interoperability for systemic operators and to explore different technologies and open standards and protocols, including the possibility of a technical interface (Application Programming Interface);

Supervision, cooperation and enforcement

82. Believes that, in view of the cross-border nature of digital services, effective supervision and cooperation between Member States including exchange of information and best practices, is key to ensure the proper enforcement of the DSA; stresses that the imperfect transposition, implementation and enforcement of Union legislation by Member States creates unjustified barriers in the digital single market; calls on the Commission to address those in close cooperation with Member States;

83. Asks the Commission to ensure that Member States provide national supervisory authorities with the adequate financial means and human resources and enforcement powers to carry out their functions effectively and to contribute to their respective work;
84. Stresses that cooperation between national as well as other Member States' authorities, civil society and consumer organisations is of utmost importance for achieving effective enforcement of the DSA; proposes to strengthen the country-of-origin principle through increased cooperation between Member States in order to improve the regulatory oversight of digital services and to achieve effective law enforcement in cross-border cases; encourages Member States to pool and share best practices and data sharing between national regulators, and to provide regulators and legal authorities with secure interoperable ways to communicate to each other;
85. Calls on the Commission to assess the most appropriate supervision and enforcement model for the application of the provisions regarding the DSA, and to consider the setup of a hybrid system, based on coordination and cooperation of national and Union authorities, for the effective enforcement oversight and implementation of the DSA; considers that such supervisory system should be responsible for the oversight, compliance, monitoring and application of the DSA and have supplementary powers to undertake cross-border initiatives and investigation and be entrusted with enforcement and auditing powers;
86. Takes the view that EU coordination in cooperation with the network of national authorities should prioritise addressing complex cross-border issues;
87. Recalls the importance of facilitating the sharing of non-personal data and promoting stakeholder dialogue; and encourages the creation and maintenance of a European research repository to facilitate the sharing of such data with public institutions, researchers, NGOs and universities for research purposes; calls on the Commission to build such tool upon existing best practices and initiatives such as the Platform observatory or the EU Blockchain Observatory;
88. Believes that the Commission, through the Joint Research Centre, should be empowered to provide expert assistance to the Member States, upon request, towards the analysis of technological, administrative, or other matters in relation to the Digital Single Market legislative enforcement; and calls on national regulators and the Commission to provide further advice and assistance to Union SMEs about their rights;
89. Calls on the Commission to strengthen and modernise the existing Union framework for out-of-court settlement under the E-Commerce Directive, taking into account developments under Directive 2013/11/EU¹, as well as court actions to allow for an effective enforcement and consumer redress; underlines the need to support consumers to use the court system; believes any revision should not weaken the legal protections of small businesses and traders that national legal systems provide;

Final aspects

¹ Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) (OJ L 165, 18.6.2013, p. 63).

90. Considers that any financial implications of the requested proposal should be covered by appropriate budgetary allocations;

◦

◦ ◦

91. Instructs its President to forward this resolution and the accompanying detailed recommendations to the Commission, the Council, and to the parliaments and governments of the Member States.

ANNEX TO THE RESOLUTION: RECOMMENDATIONS AS TO THE CONTENT OF THE PROPOSAL REQUESTED

I. GENERAL PRINCIPLES

The Digital Services Act package (“DSA”) should contribute to the strengthening of the internal market by ensuring the free movement of digital services and the freedom to conduct a business, while at the same time guaranteeing a high level of consumer protection, and the improvement of users’ rights, trust and safety online.

The DSA should guarantee that online and offline economic activities are treated equally and that they are on a level playing field, which fully reflects the principle according to which “what is illegal offline is also illegal online”, taking into account the specific nature of the online environment.

The DSA should provide consumers and economic operators, especially micro, small and medium-sized enterprises, with legal certainty and transparency. The DSA should contribute to supporting innovation and removing unjustified and disproportionate barriers and restrictions to the provision of digital services.

The DSA should be without prejudice to the broad framework of fundamental rights and freedoms of users and consumers, such as the protection of private life and the protection of personal data, non-discrimination, dignity, the freedom of expression and the right to effective judicial remedy.

The DSA should build upon the rules currently applicable to online platforms, namely the E-Commerce Directive and the Platform to Business Regulation.

The DSA should include:

- a comprehensive revision of the E-Commerce Directive, based on Articles 53(1), 62 and 114 TFEU, consisting of:
 - a revised framework with clear obligations with regards to transparency and information;
 - clear and detailed procedures and measures related to effectively tackling and removing illegal content online, including a harmonised legally-binding European notice-and-action mechanism;
 - effective supervision, cooperation and proportionate, effective and dissuasive sanctions;
- an internal market legal instrument based on Article 114 TFEU, imposing *ex ante* obligations on large platforms with a gatekeeper role in the digital ecosystem (“systemic operators”), complemented by an effective institutional enforcement mechanism.

II. SCOPE

In the interest of legal certainty, the DSA should clarify which digital services fall within its scope. The DSA should follow the horizontal nature of the E-Commerce Directive and apply not only to online platforms, but to all providers of information society services as defined in Union law.

A one-size-fits-all approach should be avoided. Different measures might be necessary for digital services offered in a purely business-to-business relationship, services which only have limited or no access to third parties or general public, and services which are targeted directly to consumers and the general public.

The territorial scope of the DSA should be extended to cover also the activities of companies, service providers and information society services established in third countries, when their activities are related to the offer of services or goods to consumers or users in the Union and directed at them.

If the Commission, following its review, considers that the DSA should amend the Annex of the E-Commerce Directive in respect of the derogations set out therein, it should not amend in particular the derogation of contractual obligations concerning consumer contracts.

The DSA should ensure that the Union and the Member States maintain a high level of consumer protection and that Member States can pursue legitimate public interest objectives, where it is necessary, proportionate and in accordance with Union law.

The DSA should define in a coherent way how its provisions interact with other legal instruments, aiming at facilitating free movement of services, in order to clarify the legal regime applicable to professional and non-professional services in all sectors, including activities related to transport services and short-term rentals, where clarification is needed.

The DSA should also clarify in a coherent way how its provisions interact with recently adopted rules on geo-blocking, product safety, market surveillance, platforms to business relations, consumer protection, sale of goods and supply of digital content and digital services¹, among others, and other announced initiatives such as the AI regulatory framework.

The DSA should apply without prejudice to the rules set out in other instruments, such as the GDPR, Directive (EU) 2019/790 (“the Copyright Directive”) and Directive 2010/13/EU (“the Audiovisual Media Services Directive”).

III. DEFINITIONS

In the definitions to be included therein, the DSA should:

- clarify to what extent new digital services, such as social media networks, collaborative economy services, search engines, WiFi hotspots, online advertising, cloud services, web hosting, messaging services, app stores, comparison tools, AI driven services, content delivery networks, and domain name services fall within its scope;

¹ Rules provided for in Directive (EU) 2019/770 and Directive (EU) 2019/771.

- clarify the nature of content hosting intermediaries (text, images, video, or audio content) on the one hand, and commercial online marketplaces (selling goods, including goods with digital elements, or services) on the other;
- clarify the difference between economic activities and content or transactions provided against remuneration, as defined by the Court, which also cover advertising and marketing practices on the one hand, and non-economic activities and content on the other;
- clarify what falls within the remit of the “illegal content” definition by making it clear that a violation of Union rules on consumer protection, product safety or the offer or sale of food or tobacco products, cosmetics and counterfeit medicines, or wildlife products also falls within the definition of illegal content;
- define the term “systemic operator” by establishing a set of clear indicators that allow regulatory authorities to identify platforms which enjoy a significant market position with a “gatekeeper” role, thereby playing a systemic role in the online economy; such indicators could include considerations such as whether the undertaking is active to a significant extent on multi-sided markets or has the ability to lock-in users and consumers, the size of its network (number of users), and the presence of network effects; barriers to entry, its financial strength, the ability to access data, the accumulation and the combination of data from different sources; vertical integration and its role as an unavoidable partner and the importance of its activity for third parties’ access to supply and markets, etc.;
- seek to codify the decisions of the Court, where needed, and having due regard to the many different pieces of legislation which use those definitions.

IV. TRANSPARENCY AND INFORMATION OBLIGATIONS

The DSA should introduce clear and proportionate transparency and information obligations; those obligations should not create any derogations or new exemptions to the current liability regime set out under Articles 12, 13, and 14 of the E-Commerce Directive and should cover the aspects described below:

1. General information requirements

The revised provisions of the E-Commerce Directive should strengthen the general information requirements with the following obligations:

- the information requirements in Article 5 and Articles 6 and 10 of the E-Commerce Directive should be reinforced;
- the “Know Your Business Customer” principle, limited to the direct commercial relationships of the hosting provider, should be introduced for business users; hosting providers should compare the identification data provided by their business users against the EU VAT and Economic Operator Identification and Registration (“EORI”) databases, where a VAT or EORI number exists; where a business is exempt from VAT or EORI registration, proof of identification should be provided; when a business user is acting as an agent for other businesses, it should declare themselves as such; hosting providers should ask their business users to ensure that all information provided is accurate and up-

to-date, subject to any change, and hosting providers should not be allowed to provide services to business users when that information is incomplete or when the hosting provider has been informed by the competent authorities that the identity of their business user is false, misleading or otherwise invalid;

- the measure of exclusion from services referred to above should apply only to contractual business-to-business relationships and should be without prejudice to the rights of data subjects under the GDPR. That measure should be without prejudice to the protection of online anonymity for users, other than business users. The new general information requirements should further enhance Articles 5, 6 and 10 of the E-Commerce Directive in order to align those measures with the information requirements established in recently adopted legislation, in particular Directive 93/13/EEC¹ (“the Unfair Contract Terms Directive”), Directive 2011/83/EU² (“the Consumer Rights Directive”) and the Platform to Business Regulation;
- Article 5 of the E-Commerce Directive should be further modernised by requiring digital service providers to provide consumers with direct and efficient means of communication such as electronic contact forms, chatbots, instant messaging or telephone callback, provided that the information relating to those means of communication is accessible to consumers in a clear and comprehensible manner;

2. Fair contract terms and general conditions

The DSA should establish minimum standards for service providers to adopt fair, accessible, non-discriminatory and transparent contract terms and general conditions in compliance, with at least the following requirements:

- to define clear and unambiguous contract terms and general conditions in a plain and intelligible language;
- to explicitly indicate in the contract terms and general conditions what is to be understood as illegal content or behaviour according to Union or national law and to explain the legal consequences to be faced by users for knowingly storing or uploading illegal content;
- to notify users whenever a significant change that can affect users’ rights is made to the contract terms and general conditions and to provide an explanation thereof;
- to ensure that pre-formulated standard clauses in contract terms and general conditions, which have not been individually negotiated in advance, including in End-User Licensing Agreements, start with a summary statement based on a harmonised template, to be set

¹ Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, most recently amended by Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (OJ L 328, 18.12.2019, p. 7).

² Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ L 304, 22.11.2011, p. 64).

out by the Commission;

- to ensure that the cancellation process is as effortless as the sign-up process (with no “dark patterns” or other influence on consumer decision);
- where automated systems are used, to specify clearly and unambiguously in their contract terms and general conditions the inputs and targeted outputs of their automated systems, and the main parameters determining ranking, as well as the reasons for the relative importance of those main parameters as compared to other parameters, while ensuring consistency with the Platforms-to-Business Regulation;
- to ensure that the requirements on contract terms and general conditions are consistent with and complement information requirements established by Union law, including those set out in the Unfair Contract Terms Directive, the Unfair Commercial Practices Directive, the Consumer Rights Directive, as amended by Directive (EU) 2019/2161, and with the GDPR;

3. Transparency requirements on commercial communications

- The revised provisions of the E-Commerce Directive should strengthen the current transparency requirements regarding commercial communications by establishing the principles of transparency-by-design and transparency-by-default.
- Building upon Article 6 and 7 of the E-Commerce Directive, the measures to be proposed should establish a new framework for Platform to Consumer relations on transparency as regards online advertising, digital nudging, micro targeting, recommendation systems for advertisement and preferential treatment; those measures should:
 - include the obligation to disclose clearly defined types of information about online advertisement to enable effective auditing and control, such as information on the identity of the advertiser and the direct and indirect payments or any other remuneration received by service providers; that should also enable consumers and public authorities to identify who should be held accountable in case of, for example, false or misleading advertisement; the measures should also contribute to ensuring that illegal activities cannot be funded via advertising services;
 - clearly distinguish between commercial and political online advertisement and ensure transparency of the criteria for the profiling targeted groups and the optimisation of advertising campaigns; enable consumers with a by default option not to be tracked or micro-targeted and to opt-in for the use of behavioural data for advertising purposes, as well as an opt-in option for political advertising and ads;
 - provide consumers with access to their dynamic marketing profiles, so that they are informed on whether and for what purposes they are tracked and if the information they receive is for advertising purposes, and guarantee their right to contest decisions that undermine their rights;
 - ensure that paid advertisements or paid placement in a ranking of search results should be identified in a clear, concise and intelligible manner, in line with Directive 2005/29/EC, as amended by Directive (EU) 2019/2161;

- ensure compliance with the principle of non-discrimination and with minimum diversification requirements, and identify practices constituting aggressive advertising, whilst encouraging consumer-friendly AI-technologies;
- introduce accountability and fairness criteria for algorithms used for targeted advertising and advertisement optimisation, and allow for external regulatory audits by competent authorities and for the verification of algorithmic design choices that involve information about individuals, without risk to violate user privacy and trade secrets;
- provide access to advertising delivery data and information about the exposure of advertisers, when it comes to where and when advertisements are placed, and the performance of paid vs unpaid advertising;

4. Artificial Intelligence and machine learning

The revised provisions should follow the principles listed below regarding the provision of information society services which are enabled by AI or make use of automated decision-making tools or machine learning tools, by:

- ensuring that consumers have the right to be informed if a service is enabled by AI, makes use of automated decision-making or machine learning tools or automated content recognition tools, in addition to the right not to be subject to a decision based solely on automated processing and to the possibility to refuse, limit or personalise the use of any AI-enabled personalisation features, especially in view of ranking of services;
- establishing comprehensive rules on non-discrimination and transparency of algorithms and data sets;
- ensuring that algorithms are explainable to competent authorities who can check when they have reasons to believe that there is an algorithmic bias;
- providing for a case-by-case oversight and recurrent risk assessment of algorithms by competent authorities, as well as human control over decision-making, in order to guarantee a higher level of consumer protection; such requirements should be consistent with the human control mechanisms and risk assessment obligations for automating services set out in existing rules, such as Directive (EU) 2018/958¹ (“the Proportionality Test Directive”), and should not constitute an unjustified or disproportionate restriction to the free movement of services;
- establishing clear accountability, liability and redress mechanisms to deal with potential harms resulting from the use of AI applications, automated decision-making and machine learning tools;
- establishing the principle of safety, security by design and by default and setting out effective and efficient rights and procedures for AI developers in instances where the algorithms produce sensitive decisions about individuals, and by properly addressing and

¹ Directive (EU) 2018/958 of the European Parliament and of the Council of 28 June 2018 on a proportionality test before adoption of new regulation of professions (OJ L 173, 9.7.2018, p. 25).

exploiting the impact of upcoming technological developments;

- ensuring consistency with confidentiality, user privacy and trade secrets;
- ensuring that, when AI technologies introduced at the workplace have direct impacts on employment conditions of workers using digital services, there needs to be an comprehensive information to workers;

5. Penalties

The compliance to those provisions should be reinforced with effective, proportionate and dissuasive penalties, including the imposition of proportionate fines.

V. MEASURES RELATED TO TACKLING ILLEGAL CONTENT ONLINE

The DSA should provide clarity and guidance regarding how online intermediaries should tackle illegal content online. The revised rules of the E-Commerce Directive should:

- clarify that any removal or disabling access to illegal content should not affect the fundamental rights and the legitimate interests of users and consumers and that legal content should stay online;
- improve the legal framework taking into account the central role played by online intermediaries and the internet in facilitating the public debate and the free dissemination of facts, opinions, and ideas;
- preserve the underlying legal principle that online intermediaries should not be held directly liable for the acts of their users and that online intermediaries can continue moderating content under fair, accessible, non-discriminatory and transparent terms and conditions of service;
- clarify that a decision made by online intermediaries as to whether content uploaded by users is legal should be provisional, and that online intermediaries should not be held liable for it, as only courts of law should decide in the final instance what is illegal content;
- ensure that the ability of Member States to decide which content is illegal under national law is not affected;
- ensure that the measures online intermediaries are called to adopt are proportionate, effective and adequate in order to effectively tackle illegal content online;
- adapt the severity of the measures that need to be taken by service providers to the seriousness of the infringement;
- ensure that the blocking of access to, and the removal of, illegal content does not require blocking the access to an entire platform and services which are otherwise legal;
- introduce new transparency and independent oversight of the content moderation procedures and tools related to the removal of illegal content online; such systems and procedures should be accompanied by robust safeguards for transparency and

accountability and be available for auditing and testing by competent authorities.

1. A notice-and-action mechanism

The DSA should establish a harmonised and legally enforceable notice-and-action mechanism based on a set of clear processes and precise timeframes for each step of the notice-and-action procedure. That notice-and-action mechanism should:

- apply to illegal online content or behaviour;
- differentiate among different types of providers, sectors and/or illegal content and the seriousness of the infringement;
- create easily accessible, reliable and user-friendly procedures tailored to the type of content;
- allow users to easily notify by electronic means potentially illegal online content or behaviour to online intermediaries;
- clarify, in an intelligible way, existing concepts and processes such as “expeditious action”, “actual knowledge and awareness”, “targeted actions”, “notices’ formats”, and “validity of notices”;
- guarantee that notices will not automatically trigger legal liability nor should they impose any removal requirement, for specific pieces of the content or for the legality assessment;
- require notices to be sufficiently precise and adequately substantiated so as to allow the service provider receiving them to take an informed and diligent decision as regards the effect to be given to the notice, and specify the requirements necessary to ensure that notices contain all the information necessary for the swift removal of illegal content;
- notices should include the location (URL and timestamp, where appropriate) of the allegedly illegal content in question, an indication of the time and date when the alleged wrongdoing was committed, the stated reason for the claim, including an explanation of the reasons why the notice provider considers the content to be illegal, and if necessary, depending on the type of content, additional evidence for the claim, and a declaration of good faith that the information provided is accurate;
- notice providers should have the possibility, but not be required, to include their contact details in a notice; where they decide to do so, their anonymity should be ensured towards the content provider; if no contact details are provided, the IP address or other equivalent can be used; anonymous notices should not be permitted when they concern the violation of personality rights or intellectual property rights;
- set up safeguards to prevent abusive behaviour by users who systematically, repeatedly and in bad faith submit wrongful or abusive notices;
- create an obligation for the online intermediaries to verify the notified content and reply in a timely manner to the notice provider and to the content uploader with a reasoned decision; such a requirement to reply should include the reasoning behind the decision,

how the decision was made, if the decision was made by a human or an automated decision agent, and information about the possibility to appeal the decision by either party, with the intermediary, courts or other entities;

- provide information and remedies to contest the decision via a counter-notice, including if the content has been removed via automated solutions, unless such a counter-notice would conflict with an ongoing investigation by law enforcement authorities;
- safeguard that judicial injunctions issued in a Member State other than that of the online intermediaries should not be handled within the notice-and-action mechanism.

The DSA notice-and-action mechanism should be binding only for illegal content. That, however, should not prevent online intermediaries from being able to adopt a similar notice-and-action mechanism for other content.

2. Out-of-court dispute settlement related with the notice-and-action mechanisms

- The decision taken by the online intermediary on whether or not to act upon content flagged as illegal should contain a clear justification on the actions undertaken regarding that specific content. The notice provider should receive a confirmation of receipt and a communication indicating the follow-up given to the notification;
- The providers of the content that is being flagged as illegal should be immediately informed of the notice and, that being the case, of the reasons and decisions taken to remove, suspend or disable access to the content; all parties should be duly informed of all existing available legal options and mechanisms to challenge this decision;
- All interested parties should have the right to contest the decision through a counter-notice which must be subject to clear requirements and accompanied by an explanation; interested parties should also have recourse to out-of-court dispute settlement mechanisms;
- The right to be notified and the right to issue a counter-notice by a user before a decision to remove content is taken shall only be restricted or waived, where:
 - (a) online intermediaries are subject to a national legal requirement that online intermediation services terminate the provision of the whole of its online intermediation services to a given user, in a manner which does not allow it to respect that notice-and-action mechanism; or,
 - (b) the notification or counter-notice would impede an ongoing criminal investigation that requires to keep the decision to suspend or remove access to the content a secret.
- The rules of Article 17 of the E-Commerce Directive should be revised to ensure that independent out-of-court dispute settlement mechanisms are put in place and are available to users in the event of disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by them;
- The out-of-court dispute settlement mechanism should meet certain standards, in particular in terms of procedural fairness, independence, impartiality, transparency and

effectiveness; such mechanisms shall enable disputes to be settled impartially and shall not deprive the user of legal protection afforded by national law, without prejudice to the rights of users to have recourse to efficient judicial remedies;

- If the redress and counter-notice have established that the notified activity or information is not illegal, the online intermediary should restore the content that was removed or suspended without undue delay or allow for re-upload by the user;
- When issuing, contesting or receiving a notice, all interested parties should be notified of both the possibility of making use of an alternative dispute resolution mechanism and of the right to recourse to a competent national court;
- The out-of-court dispute settlement mechanisms should in no way affect the rights of the parties involved to initiate legal proceedings.

3. Transparency of the notice-and-action mechanism

The notice-and-action mechanisms should be transparent and publicly available; to that end, online intermediaries should be obliged to publish annual reports, which should be standardised and contain information on:

- the number of all notices received under the notice-and-action mechanism and the types of content they relate to;
- the average response time per type of content;
- the number of erroneous takedowns;
- the type of entities that issued the notices (private individuals, organisations, corporations, trusted flaggers, etc.) and the total number of their notices;
- information about the nature of the content's illegality or the type of infringement for which it was removed;
- the number of contested decisions received by online intermediaries and how they were handled;
- the description of the content moderation model applied by the hosting intermediary, as well as of any automated tools, including meaningful information about the logic involved;
- the measures they adopt with regards to repeated offenders to ensure that those are effective in tackling such systemic abusive behaviour.

The obligation to publish that report and the detail it requires should take into account the size or the scale on which online intermediaries operate and whether they have only limited resources and expertise. Microenterprises and start-ups should be required to update this report only where there is significant change from one year to the next.

Online intermediaries should also publish information about their procedures and timeframes

for intervention by interested parties, such as the time for the content uploader to respond with a counter-notification, the time at which the intermediary will inform both parties about the result of the procedure, and the time for different forms of appeal against any decision.

4. Safe harbour provisions in Article 12, 13 and 14 of the E-Commerce Directive

The DSA should protect and uphold the current limited exemptions from liability for information society service providers (online intermediaries) provided for in Article 12, 13, and 14 of the E-Commerce Directive.

5. Active and Passive hosts

The DSA should maintain the derogations in the E-Commerce Directive for intermediaries playing a neutral and passive role and address the lack of legal certainty regarding the concept of “active role” by codifying the case-law of the Court on that matter. It should also clarify that the hosting providers play an active role when creating the content or contributing to a certain degree to the illegality of the content, or if it amounts to adoption of the third-party content as one’s own, as judged by average users or consumers.

It should ensure that voluntary measures taken by online intermediaries to address illegal content should not lead to them being considered as having an active role, solely on the basis of those measures. However, the deployment of any such measures should be accompanied with appropriate safeguards and content moderation practices should be fair, accessible, non-discriminatory and transparent.

The DSA should maintain the exemptions from liability for backend and infrastructure services, which are not party to the contractual relations between online intermediaries and their customers and which merely implement decisions taken by the online intermediaries or their customers.

6. Ban on General Monitoring - Article 15 of the E-Commerce Directive

The DSA should maintain the ban on a general monitoring obligation under Article 15 of the E-Commerce Directive. Online intermediaries should not be subject to general monitoring obligations.

VI. ONLINE MARKETPLACES

The DSA should propose specific new rules for online marketplaces, for the online sale, promotion or supply of products and for the provision of services to consumers.

Those new rules should:

- be consistent with, and complementary to, a reform of the General Product Safety Directive;
- cover all entities that offer and direct services and/or products to consumers in the Union, including if they are established outside the Union;
- distinguish online marketplaces from other types of service providers, including other ancillary intermediation activities within the same company activity; if one of the services provided by a company fulfils the criteria necessary to be considered as a

marketplace, the rules should fully apply to that part of the business regardless of the internal organisation of that company;

- ensure that online marketplaces make it clear from which country the products are sold or services are being provided, regardless whether they are provided or sold by that marketplace, a third party or a seller established inside or outside the Union;
- ensure that online marketplaces remove quickly any known misleading information given by the supplier, including misleading implicit guarantees and statements made by the supplier;
- ensure that online marketplaces, offering professional services, indicate when a profession is regulated within the meaning of Directive 2005/36/EC, in order to enable consumers to make both an informed choice and to verify, where necessary, with the relevant competent authority if a professional meets the requirements for a specific professional qualification;
- ensure that online marketplaces are transparent and accountable and cooperate with the competent authorities of the Member States in order to identify, where serious risks of dangerous products exist and to alert them as soon as they become aware of such products on their platforms;
- ensure that online marketplaces consult the Union Rapid Alert System for dangerous non-food products (RAPEX) and carry out random checks on recalled and dangerous products and, wherever possible, take appropriate action in respect to products concerned;
- ensure that once products have been identified as unsafe and/or counterfeit by the Union's rapid alert systems, by national market surveillance authorities, by customs authorities or by consumer protection authorities, it should be compulsory to remove products from the marketplace expeditiously and maximum within two working days of receiving notification;
- ensure that online marketplaces inform consumers once a product they bought therein has been removed from their platform following a notification on its non-compliance with Union product safety and consumer protection rules; they should also inform consumers of any safety issues and of any action required to ensure that recalls are carried out effectively;
- ensure that online marketplaces put in place measures to act against repeat offenders who offer dangerous products, in cooperation with authorities in line with the Platform to Business Regulation, and that they adopt measures aimed at preventing the reappearance of dangerous product, which had been already removed;
- consider the option of requiring suppliers which are established in a third country to set up a branch in the Union or designate a legal representative established in the Union, who can be held accountable for the selling of products or services which do not comply with Union rules of safety to European consumers;
- address the liability of online marketplaces for consumer damages and for failure to take adequate measures to remove illegal products after obtaining the actual knowledge of such illegal products;

- address the liability of online marketplaces when those platforms have predominant influence over suppliers and essential elements of economic transactions, such as payment means, prices, default terms conditions, or conduct aimed at facilitating the sale of goods to a consumer in the Union market, and there is no manufacturer, importer, or distributor established in the Union that can be held liable;
- address the liability of online marketplaces if the online marketplace has not informed the consumer that a third party is the actual supplier of the goods or services, thus making the marketplace contractually liable vis-à-vis the consumer; liability should also be considered in case the marketplace knowingly provides misleading information;
- guarantee that online marketplaces have the right to redress towards a supplier or producer at fault;
- explore expanding the commitment made by some e-commerce retailers and the Commission to respectively remove dangerous or counterfeit products from sale more rapidly under the voluntary commitment schemes called “Product Safety Pledge” and “Memorandum of Understanding on the sale of counterfeit goods via the internet” and indicate which of those commitments could become mandatory.

VII. EX ANTE REGULATION OF SYSTEMIC OPERATORS

The DSA should put forward a proposal for a new separate instrument aiming at ensuring that the systemic role of specific online platforms will not endanger the internal market by unfairly excluding innovative new entrants, including SMEs, entrepreneurs and start-ups, thereby reducing consumer choice;

To that end, the DSA should, in particular:

- set up an *ex ante* mechanism to prevent (instead of merely remedy) market failures caused by “systemic operators” in the digital world, building on the Platform to Business Regulation; such a mechanism should allow regulatory authorities to impose remedies on systemic operators in order to address market failures, without the establishment of a breach of competition rules;
- empower regulatory authorities to impose proportionate and well-defined remedies on those companies which have been identified as “systemic operators”, based on criteria set out within the DSA and a closed list of the positive and negative actions those companies are required to comply with and/ or are prohibited from engaging in; in its impact assessment, the Commission should make a thorough analysis of the different issues observed on the market so far, such as:
 - the lack of interoperability and appropriate tools, data, expertise, and resources deployed by systemic operators to allow consumers to switch or connect and interoperate between digital platforms or internet ecosystems;
 - the systematic preferential display, which allows systemic operators to provide their own downstream services with better visibility;
 - data envelopment used to expand market power from one market into adjacent

markets, incurring in self-preferencing of their own products and services and engaging in practices aimed at locking-in consumers;

- the widespread practice of banning third-party business users from steering consumers to their own website through the imposition of contractual clauses;

- the lack of transparency of recommendation systems used by systemic operators, including of the rules and criteria for the functioning of such systems;

- ensure that systemic operators are given the possibility to demonstrate that the behaviour in question is justified;
- clarify that some regulatory remedies should be imposed on all “systemic operators”, such as transparency obligations in the way they conduct business, in particular how they collect and use data, and a prohibition for “systemic operators” to engage in any practices aimed at making it more difficult for consumers to switch or use services across different suppliers, or other forms of unjustified discrimination that exclude or disadvantage other businesses;
- empower regulatory authorities to adopt interim measures and to impose penalties on “systemic operators” that fail to respect the different regulatory obligations imposed on them;
- reserve the power to ultimately decide if an information society service provider is a “systemic operators” to the Commission, based on the conditions set out in the *ex ante* mechanism;
- empower users of “systemic operators” to be informed, to deactivate and be able to effectively control and decide what kind of content they want to see; users should also be properly informed of all the reasons why specific content is suggested to them;
- ensure that the rights, obligations and principles of the GDPR – including data minimisation, purpose limitation, data protection by design and by default, legal grounds for processing – are observed;
- ensure appropriate levels of interoperability requiring “systemic operators” to share appropriate tools, data, expertise, and resources deployed in order to limit the risks of users and consumers’ lock-in and the artificially binding users to one systemic operator with no realistic possibility or incentives for switching between digital platforms or internet ecosystems as part of those measures, the Commission should explore different technologies and open standards and protocols, including the possibility of a technical interface (Application Programming Interface) that allows users of competing platforms to dock on to the systemic operators and exchange information with it; systemic operators may not make commercial use of any of the data that is received from third parties during interoperability activities for purposes other than enabling those activities; interoperability obligations should not limit, hinder or delay the ability of intermediaries to patch vulnerabilities;
- ensure that the new *ex ante* mechanism is without prejudice to the application of competition rules, including on self-preferencing and overall vertical integration, and ensure that both policy tools are completely independent.

VIII. SUPERVISION, COOPERATION AND ENFORCEMENT

The DSA should improve supervision and enforcement of the existing rules and strengthen the internal market clause as the cornerstone of the Digital Single Market, by complementing it with a new cooperation mechanism aimed at improving the exchange of information, the cooperation and mutual trust and, upon request, mutual assistance between Member States, in particular between the authorities in the home country where the service provider is established and the authorities in the host country where the provider is offering its services.

The Commission should conduct a thorough impact assessment to assess the most appropriate supervision and enforcement model for the application of the provisions regarding the DSA, while respecting the principles of subsidiarity and proportionality.

In its impact assessment, the Commission should look into existing models, such as the Consumer Protection Cooperation (CPC) Network, the European Regulators Group for Audiovisual Media Services (ERGA), the European Data Protection Board (EDBP) and the European Competition Network (ECN), and consider the adoption of a hybrid system of supervision.

That hybrid system of supervision, based on EU coordination in cooperation with a network of national authorities, should improve the monitoring and application of the DSA, enforce compliance, including enforcing regulatory fines, other sanctions or measures, and should be able to carry out auditing of intermediaries and platforms. It should also settle, where needed, cross-border disputes between the national authorities, address complex cross-border issues, provide advice and guidance and approve Union-wide codes and decisions, and, together with the national authorities, it should be able to launch initiatives and investigations into cross-border issues. The ultimate oversight of the Member States' obligations should remain with the Commission.

The Commission should report to the European Parliament and the Council, and, together with the national authorities, maintain a public 'Platform Scoreboard' with relevant information on the compliance with the DSA. The Commission should facilitate and support the creation and maintenance of a European research repository tool to facilitate the sharing of data with public institutions, researchers, NGOs and universities for research purposes.

The DSA should also introduce new enforcement elements into Article 16 of the E-Commerce Directive as regards self-regulation.