

The Consumer Voice in Europe

THE DIGITAL SERVICES ACT PROPOSAL

BEUC position paper



Contact: Maryant Fernández – digital@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45



Co-funded by the European Union

Ref: BEUC-X-2021-032 - 09/04/2021

Why it matters to consumers

Shopping, connecting with friends and family, sharing experiences, watching a series, moving around a city, and looking for and imparting information. These are just some examples of activities that millions of consumers carry out every day. For each one of these activities, there is one or multiple online platforms that facilitate and/or deliver these services. Platforms present numerous benefits but also present even larger challenges for consumer protection and safety. The current legal framework fails to effectively protect consumers online and hold platforms to account. For example, consumer organisations found 66% of 250 products purchased on online marketplaces did not comply with EU laws and technical standards. The Digital Services Act (DSA) can be part of the solution to fix this.

Summary

The Digital Services Act (DSA) proposal is a good starting point, but improvements are needed.

BEUC, the European Consumer Organisation, generally welcomes the DSA proposal, but improvements are needed on several aspects.

Key BEUC recommendations:

- 1. A clear liability regime for marketplaces should be introduced.** Inserting a narrow exception to an overly broad liability exemption as proposed is welcome, but not enough.
- 2. Responsibilities need to be broader in scope and strengthened.** Obligations can be asymmetrical, but basic responsibilities should not only apply to platforms of a certain size (notably the obligations on internal complaint mechanisms, out-of-court dispute settlement, traceability of traders, online advertising or recommender systems). In addition, obligations need to be clear and stronger to change the status quo. Improvements are needed notably on trader traceability, requiring spot-checks on services and products that platforms facilitate offering, behavioural and micro-targeted advertising and recommender systems. Transparency and self- or co-regulation are not enough.
- 3. The DSA needs to be enforced swiftly and in practice.** The country of origin as a jurisdiction principle does not lead to efficient enforcement for consumer and NGO complaints. In those cases, authorities where consumers are affected should be competent. We need to learn from previous experience, e.g., the problems with the cross-border enforcement system of the General Data Protection Regulation (GDPR). The proposed Commission powers against very large platforms could be part of the solution, but a Commission fall-back option in case of inaction of the authority of the Member State of establishment may come too late or not at all, if these provisions do not oblige the Commission to act. Finally, we need to ensure enforcement is efficient, works well with and does not add unnecessary delay to existing enforcement structures in other EU laws.

Table of contents

Introduction	3
Chapter I. General provisions	5
1.1. Objectives	5
1.2. Scope	6
1.3. The DSA in relation to other laws	6
1.4. Definitions and terms used	7
Chapter II. Liability of providers of intermediary services.....	9
2.1. Positive liability provisions for online marketplaces (Article 5.3)	9
2.2. Voluntary own-initiative investigations and legal compliance (Article 6)	12
2.3. No general monitoring (Article 7)	13
2.4. Orders to act against illegal content and provide information (Arts. 8 and 9)	14
Chapter III. Due diligence obligations	15
3.1. Obligations' categorisation	15
3.2. The substance of the provisions	17
<i>Protection against dark patterns needed</i>	17
<i>Single point of contact and Compliance officers (Articles 10 and 32)</i>	18
<i>Legal representative (Article 11)</i>	18
<i>Terms and conditions (Article 12)</i>	18
<i>Transparency reporting (Articles 13, 23, 33)</i>	19
<i>Notice and action and statement of reasons (Articles 14 and 15)</i>	19
<i>Internal complaint-handling & out-of-court dispute settlement (Arts.17-18)</i>	21
<i>Trusted flaggers (Article 19)</i>	23
<i>Measures and protection against misuse (Article 20)</i>	23
<i>Notification of illegal activities to authorities (Article 21)</i>	23
<i>Traceability of traders (Article 22)</i>	24
<i>Online advertising and recommender systems (Articles 24, 29, 30, 36)</i>	25
<i>Risk assessment, mitigation of risks and independent audits (Arts. 26-28)</i>	28
<i>Data access and scrutiny (Article 31)</i>	28
Standards (Article 34).....	29
<i>Codes of conduct and crisis protocols (Articles 35-37)</i>	29
Chapter IV. Implementation, cooperation, sanctions and enforcement	30
Chapter V. Final provisions	33

Introduction

On 15 December 2020, the European Commission launched a **proposal for a Digital Services Act (DSA)**¹. The draft DSA aims to set enforceable rules for online intermediary services, including platforms (like Google, Facebook, Amazon, Alibaba, Booking.com²), but also other companies such as cloud service providers (e.g., Amazon, Dropbox) and telecom companies (e.g., Telefonica, Proximus).

The DSA proposal seeks to partially amend the e-Commerce Directive, which was adopted in 2000³. It also proposes additional obligations for intermediary service providers (online platforms in particular), and reinforced implementation, coordination and enforcement rules.

Why the DSA is needed

As mentioned in our previous position paper⁴, the DSA is needed because **the market reality has changed, new challenges have arisen. Legislators need to catch up to change the status quo.**

When the e-Commerce Directive was adopted in 2000, platforms like Google, Amazon or Booking.com were in their infancies. Many other intermediaries did not even exist. For example, Facebook and Shopify were launched in 2004, and Airbnb in 2008. Instagram, Wish and AliExpress saw the light of day in 2010. The European landscape is witnessing a multiplication of platforms; a proliferation of the collaborative⁵ and gig economy; a diversification of service providers in terms of functions, vertical integration and size; a predominant surveillance business model used for example in content moderation, advertising and for other purposes, which sometimes leads to data exploitation, discrimination, manipulation and disinformation; and a **wide range of illegal activities online**. Furthermore, many consumers do not really understand what a marketplace is and think that they are buying from the platform and not from the seller in question. This is particularly relevant and problematic when sellers with a strong market position or brand provide a marketplace channel on their website or application, which is confused with their direct sales channel (e.g., Fnac).

Consumer associations keep uncovering unsafe and illegal activities online⁶, notably in online marketplaces⁷. These range from the sale of dangerous products⁸ to a market of

¹ Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN>

² All references to companies are meant for illustration purposes only.

³ 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, <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000L0031>

⁴ Making the Digital Services Act work for consumers, BEUC's recommendations, BEUC-X-2020-031, https://www.beuc.eu/publications/beuc-x-2020-031_making_the_digital_services_act_work_for_consumers_-_beucs_recommendations.pdf

⁵ <https://www.ocu.org/consumo-familia/consumo-colaborativo/informe/plataformas-consumo-colaborativo>

⁶ Unsafe and illegal activities online - Research and evidence from BEUC member organisations, https://www.beuc.eu/publications/unsafe_and_illegal_activities_online.pdf (list updated from time to time).

⁷ Is it safe to shop on online marketplaces? Consumer research finds 66% of 250 tested products to be unsafe, BEUC-X-2021-004, February 2021, https://www.beuc.eu/publications/beuc-x-2021-004_is_it_safe_to_shop_on_online_marketplaces.pdf

⁸ E.g., ICRT, BEUC, Test Achats/Test Aankoop, Altroconsumo, Consumentenbond, Forbrugerrådet Tænk, Stiftung Warentest and Which?, Two-thirds of 250 products bought from online marketplaces fail safety tests, consumer groups find, February 2020, <https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html>

See also https://www.beuc.eu/sites/default/files/icrt_product_safety_online_marketplaces.pdf

fake reviews⁹, scam and fraudulent ads¹⁰ and ticket touting victims¹¹. Unfortunately, consumer advocates have not been the only ones coming up with similar or even more alarming results as in some cases the level of non-compliance found is higher¹².

So far, self- and co-regulatory initiatives that have tried to address some of these issues **have failed to effectively protect consumers** and achieve a level-playing field between businesses that try to respect the law and those that neglect it¹³. In fact, failure to comply with voluntary commitments does not lead to legal consequences such as sanctions or consumer redress. This unfortunate reality juxtaposes to consumer expectations: **consumers expect protection¹⁴ and legislative change¹⁵**.

Such EU legal changes in the platform economy will **also benefit businesses that** play by the rules, as the DSA can bring more legal certainty, fix the current uneven playing-field, avoid regulatory silos and fragmentation, and ultimately deliver a fairer and more competitive single market.

Finally, new rules can **help competent authorities** to ensure the law is respected, to better coordinate, supervise and enforce obligations against infringers, and alleviate the burden some currently experience.

The DSA: a good starting point and part of a bigger picture

The DSA proposal was presented together with the crucial Digital Markets Act (DMA)¹⁶. The DMA would allow the Commission to pro-actively tackle unfair behaviour by gatekeepers and make it easier for new entrants to break into digital markets. **Coordination between the DSA and the DMA is needed, as they complement each other.** A strengthened DSA and a DMA could significantly improve the way Europe's digital economy works, give consumers a fairer share of the benefits of digital services and boost consumer protection in the online world.

BEUC considers the DSA proposal as an urgently needed step in the right direction. We appreciate that the European Commission took on board several of the recommendations BEUC¹⁷ and the European Parliament made to protect consumers. BEUC generally welcomes that the DSA proposal applies to companies established inside or outside the EU; obliges non-EU providers to appoint a legal representative that can be

⁹ E.g., Stiftung Warentest, Fake-Bewertungen Wie Verkäufer mit gekauftem Lob Kunden manipulieren, June 2020, <https://www.test.de/Fake-Bewertungen-Wie-Verkaeuer-mit-gekauftem-Lob-Kunden-manipulieren-5401497-0/>

¹⁰ E.g., Which?, Nearly one in 10 have fallen victim to scam adverts on social media or search engines as platforms fail to adequately protect users, November 2020 <https://press.which.co.uk/whichpressreleases/nearly-one-in-10-have-fallen-victim-to-scam-adverts-on-social-media-or-search-engines-as-platforms-fail-to-adequately-protect-users-which-finds/>

¹¹ E.g., L'UFC-Que Choisir dépose plainte, February 2020, <https://www.quechoisir.org/action-ufc-que-choisir-viagogo-l-ufc-que-choisir-depose-plainte-n75959/>

¹² For example, this is the case of [public authorities](#), but also industry actors such as [Toys Industries of Europe](#) (TIE), [the Danish Chamber of Commerce](#) or the [Face-value European Alliance for Ticketing](#) (FEAT).

¹³ This has been the case of the Product Safety Pledge and failure to comply by major signatories like Amazon, eBay and Wish. See, e.g., Which?, Online marketplaces fail to remove banned products – even after consumers report them, December 2020, <https://press.which.co.uk/whichpressreleases/online-marketplaces-fail-to-remove-banned-products-even-after-consumers-report-them-which-finds/>

¹⁴ See, e.g., Vzbv, Grenzenloser Ärger statt bequemer Online-Kauf, November 2020, <https://ssl.vzbv.de/pressemitteilung/grenzenloser-aerger-statt-bequemer-online-kauf>
Sveriges Konsumenter, Privatimportens faror – det här vill vi se hända, December 2020, <https://www.sverigeskonsumenter.se/vara-projekt/privatimportens-faror/slutrapporten/>

¹⁵ E.g., Which?, Online marketplaces and product safety, September 2019, <https://www.which.co.uk/policy/consumers/5234/onlinemarketplaces>

¹⁶ Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN>

¹⁷ Making the Digital Services Act work for consumers, BEUC's recommendations, BEUC-X-2020-031.

held liable for non-compliance; establishes points of contact, compliance officers and more transparency obligations; establishes notice and action procedures with safeguards; partially excludes online marketplaces from the liability exemptions; includes an obligation for marketplaces to trace traders, asks for further rules on advertising; regulates recommender systems (albeit only for some platforms); introduces additional rules for very large platforms, including risk assessments and mitigating measures obligations, independent audits, scrutiny and data access; and provisions that seek to improve consumer redress and current enforcement efforts.

At the same time, we consider **improvements are needed**, notably on the liability of marketplaces, the due diligence obligations and the redress and enforcement mechanisms, to ensure the aims and intentions of the proposal are fully achieved, including on the points above.

BEUC calls on the European Parliament and the Council of the European Union to build on the DSA and DMA proposals put forward by the Commission, in a way to improve the texts and deliver a successful outcome to protect consumers and contribute to a fairer and more competitive digital economy¹⁸.

This BEUC paper consolidates recommendations from 45 consumer organisations from 32 countries¹⁹. To be most useful to policymakers, our paper follows the structure of the DSA legislative proposal as much as possible.

Chapter I. General provisions

1.1. Objectives

The proposal seems to focus on ensuring a single market for digital services and avoiding legal fragmentation (Article 1.2). While laudable, **consumer protection and product safety** are not clearly spelled out in the objectives. This is contrary to Article 169.2 a) of the Treaty on the Functioning of the European Union (TFEU).

BEUC welcomes that the EU Charter of fundamental rights is mentioned not only in Art. 1.2, but also in other provisions. However, the proposal seems to neglect consumer protection. Despite being enshrined as a fundamental principle in Article 38 of the Charter of Fundamental Rights, consumer protection is not mentioned when the proposal refers to some articles of the Charter²⁰.

Similarly, the DSA proposal must have **special protections for children below 18**. Online platforms and in particular social media services which target a young audience need to be designed with the best interests of the child, which is not the case for many platforms.

BEUC recommendation: consumer protection, product safety and the protection of minors must be defined as explicit legal objectives in Article 1.2, building on recital 34.

¹⁸ Digital Markets Act Proposal - Position paper, BEUC-X-2021-031, April 2021, https://www.beuc.eu/publications/beuc-x-2021-030_digital_markets_act_proposal.pdf

¹⁹ <https://www.beuc.eu/beuc-network/our-members>

²⁰ See, in particular Articles 26.1,b), 37.4,e), 41.6; and recitals 3, 41, 57.

1.2. Scope

BEUC welcomes that the DSA scope of application covers intermediary services established outside the EU (Article 1.3). For that, Art. 2.d) and recitals 7 and 8 require these service providers to have a substantial connection with the EU. In BEUC's view, recital 7 is in line with private international law and CJEU case law interpreting it. The key criterion to fall within the territorial scope of the DSA is that providers target their activities towards one or more Member States. While the criteria proposed is not cumulative (which is good), BEUC considers that the criterion to have "a significant number of" EU users is included within the other criterion. Therefore, it can be deleted.

In BEUC's view, foreign intermediary services that target their activities to EU consumers, particularly to offer them services and products, should be covered by the DSA to protect consumers and reach a level playing field. Enforcement against providers and traders not established in the EU is a key aspect to improve under the DSA. We refer to our comments regarding chapters III and IV of the DSA.

Regrettably, non-EU intermediary services would still not be covered by the provisions of the eCommerce Directive. That is because the scope of the e-Commerce Directive (Article 1.1 and recital 58 of the latter) is not amended by the DSA (Article 72).

BEUC recommendations:

- **Policymakers should ensure non-EU companies that target their activities to one or several Member States cannot escape from the scope** (Articles 1.3, 2 d)) **and enforcement of the DSA.**
- **The DSA should also amend Art. 1.1 and recital 58 of the e-commerce Directive** so its rules apply to digital services offered by providers established outside the EU. This can be done by amending Arts. 1 and 72 of the DSA.

1.3. The DSA in relation to other laws

The DSA must be carefully designed to fit into the regulatory landscape of existing and upcoming rules. Article 1.5 and recitals 9-11 of the proposal clarify the DSA will apply without prejudice to other laws, including the e-Commerce Directive, consumer, product safety, privacy and data protection laws.



BEUC recommends ensuring coordination, but there should be no trade-offs or preclusion effects on other laws. It is important to ensure both the DSA and other relevant legislation fix any possible legal loopholes. For example, if policymakers do not get the provisions right, we see a risk for the liability provisions in chapter II to potentially limit how other EU and Member State laws establish positive liability on online marketplaces²¹, including via the Omnibus Directive²² or a possible future reform of the Product Liability Directive. Despite assurances in the explanatory memorandum, it is also unclear how and whether the DSA enforcement structure would affect enforcement and redress mechanisms in other legislation. We explain concrete ways to avoid these types of problems in pages 21, 22 and 30 *et seq.*

²¹ Member States should also use the possibility of recital 23 of Directive (EU) 2019/771 to expand the new conformity rules to platforms which are not direct sellers to consumers. The DSA should not prevent that.

²² 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, Art. 6a, <https://eur-lex.europa.eu/eli/dir/2019/2161/oj>

1.4. Definitions and terms used

Article 2 and the consistent use of terms thereof are crucial because they determine the applicability and the scope of the rules.

BEUC generally welcomes that the Commission uses long-standing definitions, but **recommends more clarity** around some definitions and the use of terms throughout the provisions, including:

- **'recipient of the service' (b)**: while we understand this concept includes both traders and consumers, sometimes the proposal gives the impression it is only referring to business users. In the same vein, this definition is different from Article 2.d) of the e-Commerce Directive. The distinction between traders and consumers on the one hand and recipients of the service on the other should always be clear.
- **'to offer services in the Union' (d)**: as mentioned earlier, and while remaining proportionate, legislators should make sure all relevant companies fall within the scope of the Regulation. The 'substantial connection' criteria cannot become a way for foreign companies to circumvent the Regulation. While the criteria proposed is not cumulative (which is good), BEUC recommends deleting 'a significant number of users in one or more Member States' from Article 2 d) and recital 8 as this criterion would be included within the criterion to target activities to one or several EU Member States. The second criteria ("the targeting of activities towards one or more Member States") is in line with Private International Law and CJEU case law.
- **'illegal content' (g)**: BEUC welcomes this definition²³ as the DSA is not meant to define when content is legal or illegal. Other EU and Member State laws do so. However, the use of this term should be more coherent and consistent throughout the text. Illegal content and 'activities' are sometimes used interchangeably in the articles. Similarly, information should not be treated the same as 'goods' or 'services'.
- **'online platform' (h) and 'dissemination to the public' (i)**: these definitions and related recitals should be assessed carefully to ensure that all relevant companies and their services would be subject to relevant DSA obligations. For example, messaging services like WhatsApp are in principle excluded from the scope of application of the DSA (recital 14). This makes sense to for example ensure encryption is not weakened to moderate content. However, BEUC notes that messaging apps may in the future become sales channels²⁴, in which case some DSA rules (like the traceability of traders under Article 22) should apply to them. Therefore, they should not fully be exempted from the scope of application.
- **'advertisement' (n)**: the definition must include both direct and indirect ways to promote, market or rank information, products or services. In the same vein, BEUC witnesses indirect and direct forms of remuneration. Both should be included. This is important because, for example, some online influencers do hidden marketing of products without revealing that they are paid for it. This is an unfair commercial practice that is commonly used in the areas of health, food supplements and beauty products, but not only limited to them. For example, this is what BEUC and 17 of our member organisations found in relation to TikTok²⁵.

²³ The definition also seems to be consistent with the Commission's Recommendation on measures to effectively tackle illegal content online, <https://digital-strategy.ec.europa.eu/en/library/commission-recommendation-measures-effectively-tackle-illegal-content-online>

²⁴ Some allow this already, like the Chinese app "WeChat". See, e.g., <https://www.marketingtochina.com/wechat-e-commerce-guide/>

See also <https://about.fb.com/news/2020/10/privacy-matters-whatsapp-business-conversations/>

²⁵ <https://www.beuc.eu/tiktok>

- **'recommender system' (o):** the definition should not only be limited to "suggestions" but also ranking and prioritisation techniques. This change would bring the definition in line with recital 62, as recommended by the European Data Protection Supervisor (EDPS)²⁶.
- **'terms and conditions' (q):** the definition is good, but it is important to clarify in a recital that terms and conditions should be in line with applicable EU and Member State laws. This is important because the use of unfair terms by online platforms is unfortunately widespread, despite existing laws and various national judgements on the matter. Recently, following an action brought forward by UFC-Que Choisir, the French Tribunal de Grande Instance ordered Twitter to delete more than 250 abusive clauses²⁷, condemned Google for using 209 unfair or illegal contract clauses²⁸ and found Facebook had 430 abusive or illicit clauses²⁹.

To avoid unclarity, policymakers should resort to the existing **definition of 'online marketplaces'** under the Omnibus Directive, Directive (EU) 2019/2161³⁰, i.e., "a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers"³¹. While the Commission does not use the term 'online marketplace' in the articles shaped for them under the DSA, it seems to largely follow the definition established under the Omnibus Directive.

As BEUC pointed out in the past, we understand that if one intermediary company provides a service that fulfils the criteria to be considered as a marketplace, the rules should fully apply to that part of the business. These would not only include platforms that directly facilitate the selling of goods, but platforms where suppliers can place advertisements (think social media services, e.g., Instagram, TikTok) and platforms which offer comparison, advisory or reputational services (e.g., Booking.com or Yelp).³² This is because they facilitate ("allow") the conclusion of B2C contracts as well. **It is important the DSA is flexible enough to cover those relevant services under the scope of application, to ensure no company would try to circumvent key provisions of the DSA.**

²⁶ https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf

²⁷ <https://www.quechoisir.org/action-ufc-que-choisir-reseaux-sociaux-et-clauses-abusives-l-ufc-que-choisir-obtient-la-suppression-de-centaines-de-clauses-des-conditions-d-utilisation-de-twitter-n57621/>

²⁸ <https://www.quechoisir.org/action-ufc-que-choisir-donnees-personnelles-l-ufc-que-choisir-obtient-la-condamnation-de-google-n63567/>

²⁹ <https://www.quechoisir.org/action-ufc-que-choisir-donnees-personnelles-l-ufc-que-choisir-obtient-la-condamnation-de-facebook-n65523/>

³⁰ 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.

³¹ Article 2.1 n) of the Unfair commercial practices Directive, as amended by Directive 2019/2161, <https://eur-lex.europa.eu/eli/dir/2019/2161/oj>

³² This categorisation is inspired on the European Law Institute's Report "Model Rules on Online Platforms", https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf (article 1).

Chapter II. Liability of providers of intermediary services

BEUC considers there is value in the liability exemptions set forth in the e-Commerce Directive for intermediary service providers other than online marketplaces. Yet, dealing with products and services is not the same as dealing with consumer-generated content. Equally, dealing with commercial transactions leading to the conclusion of distant contracts between a trader and a consumer should not be treated the same as dealing with videos, tweets or content posted by individuals. Therefore, **BEUC welcomes that the European Commission has distinguished liability provisions for marketplaces from those applicable to other types of intermediary services**, e.g., a cloud-service or internet access provided by telecom companies.

BEUC regrets there is no clear liability provision that establishes the consequences for not being compliant with the DSA. Here, public enforcement will not be sufficient.

2.1. Positive liability provisions for online marketplaces (Article 5.3)

While Article 5.3 is a step into the right direction, as the Commission recognised the need to create an exception for online marketplaces to the general liability exemptions, this provision and corresponding recitals would benefit from further clarity and expansion. **BEUC recommends turning article 5.3 into a positive liability framework for online marketplaces.**

More clarity and a positive liability framework needed

Art. 5.3 provides for an **exception** to the liability exemption for online marketplaces. In other words, it stipulates when the liability exemption does not apply. As the same time, while the Commission does not use the term 'online marketplace', it seems to largely follow the definition established under the Omnibus Directive³³. That is, "a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers³⁴". This definition is important because the distinction between social media services, messaging apps and "classic" online marketplaces are increasingly blurred and interlinked.

Also, Art. 5.3 **does not provide for positive liability (recital 17)**. Read in conjunction with recital 17, article 5.3 cannot be read as establishing positive secondary liability on marketplaces for damages, non-performance of the contract or guarantee issues. It just provides that the liability exemption does not apply to online marketplaces under certain circumstances. BEUC considers that this approach is insufficient and **a positive liability framework for online marketplaces at EU level is needed to address the existing problems related to widespread illegal activities in online marketplaces.**

In addition, it is problematic that recital 17 establishes that "the exemptions from liability established in this Regulation should apply in respect of any type of liability as regards any type of illegal content, irrespective of the precise subject matter or nature of those laws." Other laws such as the GDPR³⁵ or Directive 2019/771 (the 'Sales Directive')³⁶ establish

³³ 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.

³⁴ Article 2.1 n) of the Unfair commercial practices Directive, as amended by Directive 2019/2161, <https://eur-lex.europa.eu/eli/dir/2019/2161/oj>

³⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council 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, Article 82.

³⁶ Recital 23.

and/or allow Member States to establish positive liability for certain types of platforms. **Recital 17 must be amended to ensure it does not apply to questions relating to information society services covered by other EU or Member State laws.**

At the same time, the exception in art. 5.3 is quite **narrow**, as we explain below. The DSA should be **clear as to what scenarios this liability would apply to**. In this sense, further clarity is needed.

Firstly, **the "average and reasonably well-informed consumer" limitation should be deleted**. This term is not a suitable benchmark to delineate the availability of protection, particularly when it comes to the online environment and sophisticated use of technologies and interface design in digital services that all consumers are exposed to and often have difficulties with³⁷. It is important to account for digital marketing practices such as practices which target internal and dispositional vulnerabilities of each individual to maximise revenue³⁸. Consumer vulnerability also needs to be reframed due to the use of AI, profiling and algorithmic targeting. Everyone is vulnerable to a great extent in the context of such systems. Thus, the benchmark of the reasonably well-informed consumer is not appropriate in the scenario at stake and would not ensure effective protection.

We need clear liability rules for platforms including for consumer law and product safety violations. Art. 5.3 refers to liability under "consumer protection law". It is unclear what consumer protection law would comprise, for example would it also include product safety legislation? **'Consumer protection law'** is not a defined term, so for the sake of legal certainty, this **should be deleted**, particularly because in Article 1 of the DSA proposal the Commission distinguishes between consumer and product safety laws.

Article 5.3 seems to be focused on **information** issues (e.g., the listing of a product online for sale), but it regrettably does not clearly address product conformity (see also recital 23). If the DSA does not establish positive liability regarding products, we need to ensure Article 5.3 and recital 17 do not have a precluding effect on other laws, notably a possible review of the Product Liability Directive to establish secondary liability under certain circumstances³⁹.

Moreover, if this provision is not turned into a positive liability provision in an improved manner, other EU or Member State laws will need to tailor and shape any liability provisions in light of the DSA, restricting their margin of manoeuvre. Just like the e-Commerce Directive, the DSA could act as a deterrent to establish clear liability in other laws.

A change in the approach to liability is possible

Establishing responsibilities and liability are not mutually exclusive. Responsibilities need to come with liability for non-compliance, in order to make them effective.

³⁷ New research commissioned by BEUC indicates that protection of consumers online should be improved. See https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf

³⁸ See https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf, p. 46 on the reconceptualization of digital vulnerability, p. 108 on dark patterns using personalisation. Some companies engage in morphing, which transforms the interface or parts of it depending on certain conditions and is one of the ways dark patterns operate, e.g., to make certain information or disclosure less visible. Dispositional vulnerabilities of consumers are the potential for vulnerability of a person that can materialise under certain circumstances, e.g., a consumer never looks at certain parts of the interface, or a consumer is often distracted by certain types of visuals or messages.

³⁹ BEUC's position: https://www.beuc.eu/publications/beuc-x-2020-024_product_liability_position_paper.pdf

Establishing liability rules under the DSA and other laws is not mutually exclusive either⁴⁰. Other EU laws should play their share⁴¹. For BEUC it is important that the ongoing review of the General Product Safety Directive (GPSD)⁴² and the possible upcoming review of the Product Liability Directive (PLD)⁴³ will also establish clear and consistent liability rules for online marketplaces. BEUC recommends the following division:

	Type of liability for online marketplaces	Scope
DSA	Secondary civil liability for damages, non-performance of a contract or guarantees	Content, including information about a product or a service.
	Liability for non-compliance	The DSA due diligence obligations
GPSD	Liability for non-compliance of safety obligations	Safety requirements
PLD	Secondary liability for damages for products failing to comply with users' reasonable expectations	Product non-conformity

These instruments are partly overlapping, but not completely. For example, when addressing intermediary services like online marketplaces, we do not only refer to platforms that facilitate the sale of products like Amazon or Alibaba, but also those that offer services (e.g., Booking.com or Airbnb). This is important because while it is necessary to establish liability rules for marketplaces in the 36-year-old Product Liability Directive, these may not cover liability for issues related to service offers.

Online marketplaces should bear subsidiary liability under certain circumstances as they do not merely store information or just connect two (or more) recipients of the service. BEUC proposes a specific liability regime that takes into account the different business models of this type of platforms. Notably, we propose that if a marketplace exerts decisive influence on a trader or a commercial transaction, it should bear greater responsibility.

The role of online marketplaces (and the liability deriving therefrom) must be fully recognised under the DSA. It is important the DSA clarifies when marketplaces can be held liable. This must not, yet again, be postponed to updates of other EU laws. Article 21 of the e-Commerce Directive already had "the attribution of liability" as part of the provisions that merited further analysis and re-examination. We need to address the current offline-online disparity. Brick-and-mortar shops can be held liable when they sell unsafe products. While platforms are not sellers, they should contribute their share of liability and responsibility. We have witnessed how Article 14 of the e-Commerce Directive has prevented other EU laws from establishing clear liability rules for online marketplaces. We cannot afford legal loopholes under the DSA.

BEUC recommendation: Following independent research involving many academics⁴⁴, **BEUC proposes article 5.3 to be amended to ensure online marketplaces and traders can be jointly and severally liable:**

- For non-compliance of their due diligence obligations. For example, if a marketplace fails to demonstrate it verifies traders following Article 22 of the DSA.

⁴⁰ https://www.beuc.eu/publications/beuc-x-2021-004_is_it_safe_to_shop_on_online_marketplaces.pdf

⁴¹ See, for example, Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods.

⁴² https://www.beuc.eu/publications/beuc-x-2020-068_beuc_and_anecs_views_for_a_modern_regulatory_framework_on_product_safety.pdf

⁴³ https://www.beuc.eu/publications/beuc-x-2020-024_product_liability_position_paper.pdf

⁴⁴ https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf

- For damages, when failing to act upon obtaining credible evidence of illegal activities, without incurring into a general duty to monitor the activity of platform users⁴⁵.
- For damages, contract performance and guarantees:
 - 1- for failure to inform consumers about the supplier of the goods or services, in line with Article 4.5 of the Omnibus Directive introducing the new Art. 6a.1,b) of the Consumer Rights Directive and CJEU Wathelet case C-149/15;
 - 2- for providing misleading information, guarantees, or statements;⁴⁶
 - 3- where the platform has a predominant influence over suppliers or the transaction. Such predominant influence or control could be inferred by non-exhaustive and non-cumulative criteria that would be assessed on a case-by-case basis by courts. Following research by the European Law Institute, we would like to suggest the following indicative criteria⁴⁷:
 - a) “The supplier-customer contract is concluded exclusively through facilities provided on the platform;
 - b) The platform operator withholds the identity of the supplier or contact details until after the conclusion of the supplier-customer contract;
 - c) The platform operator exclusively uses payment systems which enable the platform operator to withhold payments made by the customer to the supplier;
 - d) The terms of the supplier-customer contract are essentially determined by the platform operator;
 - e) The price to be paid by the customer is set by the platform operator;
 - f) The marketing is focused on the platform operator and not on suppliers; **or**
 - g) The platform operator promises to monitor the conduct of suppliers and to enforce compliance with its standards beyond what is required by law.”

To be proportionate, marketplaces should enjoy a right to redress towards the party at fault⁴⁸. This is precisely what was done under Article 82 of the General Data Protection Regulation (GDPR). For this, both Article 5.3 and related recitals must be amended. Recital 17 must be deleted or amended to ensure it does not prevent establishing a positive liability regime for online marketplaces and does not hamper existing legislation.

Rights and remedies for consumers

In light of the above, and as long as a hosting service provider is not exempted from liability in line with Article 5.1, the **DSA should establish that consumers can exercise against the intermediary service provider all the rights and remedies that would be available against the trader**, including compensation for damages, repair, replacement, price reduction, contract termination or reimbursement of the price paid⁴⁹. **In addition, specific remedies** for consumers shall be foreseen **in case** the intermediary service provider is in **breach of its own obligations** listed in this Regulation.

2.2. Voluntary own-initiative investigations and legal compliance (Article 6)

BEUC is very sceptical about introducing a “Good Samaritan”-type clause to add more protections to intermediary service providers that adopt “voluntary” actions. This could render enforcement less effective.

⁴⁵ Based on the European Law Institute Model Rules for Online Platforms, article 8.

⁴⁶ *Ibid*, articles 9 and 23.

⁴⁷ European Law Institute Model Rules on Online Platforms, article 20.

⁴⁸ Based on the European Law Institute Model Rules on Online Platforms, article 25.

⁴⁹ This follows the definition of ‘redress measure’ under Article 3.10 of the Representatives Actions Directive, Directive (EU) 2020/1828.

Just because voluntary action is taken, it does not mean platforms will effectively protect consumers. While big online platforms often complain that the current regime penalises those that proactively try to address illegal content, the solution is not to import concepts from the US law⁵⁰ which are not fit-for-purpose in EU law. Article 6 does not fully equate to similar provisions in the United States, but it still adds further protections for platforms.

It is important that platforms are responsible for the consequences of actions they have taken (or not taken). In addition, it is important measures undertaken are proven effective. At the moment, when consumer organisations notify platforms of illegal activities online, a response that consumer organisations often get is that platforms voluntarily put filters and human resources in place, but they did not catch these specific instances – in some cases even after repeatedly flagging the same types of listings year after year. This is, for example, what eBay and Amazon told Which? after the UK consumer group flagged very dangerous child car seats over several years since 2014⁵¹. This is unacceptable. Putting the excuse that “bad actors” will always try to bypass their systems is simply not good enough. Any action taken by platforms must seek to be effective to protect consumers while minimising the risks for other fundamental rights, freedoms and principles under the EU Charter of Fundamental Rights.

Being able to establish subsidiary liability, particularly for marketplaces, is needed as an incentive to ensure the scale of illegal activities on their sites and apps is severely reduced. It is not appropriate for marketplaces to profit from illegal activities on their services. In addition, if policymakers manage to ensure obligations in the DSA are clear and strong, companies will not need to go beyond the law and take (unenforceable) voluntary actions. Democratic institutions should decide what platforms should do. Consumers need further protection, not platforms. In the event that Art. 6 is retained, measures to be taken must be specified, e.g., via the platforms’ terms and conditions. Overall, Art. 6 is very vague, which leads to strong legal uncertainty.

BEUC recommends deleting Article 6 and recital 25 or at least narrowing them down as much as possible, to ensure any voluntary actions taken by intermediary service providers are designed to be effective.

2.3. No general monitoring (Article 7)

BEUC welcomes that the prohibition not to conduct general monitoring can still be found in the DSA. This is particularly important to preserve freedom of expression and the rights to privacy and personal data protection. It is important to protect citizens’ communications and the content they generate. However, Articles 7, 22 and recitals 28 and 50 should not prevent **online marketplaces** from being obliged to conduct **periodic checks on trader accounts and the products and services they facilitate offering**. It is important not to have a one-size-fits-all solution for online marketplaces and other type of platform services. This is essential to avoid the reappearance of illegal listings.

The DSA should impose an obligation on marketplaces to do regular checks on products and services they facilitate offering. This addition would be an added value to Art. 22 (on the traceability of traders). Currently, some online marketplaces claim to undertake those checks voluntarily, but these cannot be verified and failure to comply with those checks does not create any consequences for the platform. Their effectiveness would not be guaranteed. The DSA needs enforceable rules.

⁵⁰ Particularly in section 230(c)(2) of the Communications Decency Act, <https://www.law.cornell.edu/uscode/text/47/230>

⁵¹ <https://www.which.co.uk/news/2019/02/why-are-ebay-and-amazon-still-selling-killer-car-seats/>

Platforms should not need filters in place to comply with such recommendation. They can be done by other means, just like BEUC members do, e.g., conducting visual inspections and mystery shopping exercises. We do not ask for a 24/7 constant monitoring or the monitoring of consumer communications. The 'no general monitoring' obligation on user-generated content or communications and specific checks on products and services can and should coexist.

BEUC recommendation: BEUC advocates to keep the principle that consumers' communications and the content they generate should not be monitored. However, a specific obligation should be inserted for online marketplaces. **Articles 7, 22 and recitals 28 and 50 should be amended to ensure marketplaces are obliged to undertake spot checks.**

2.4. Orders to act against illegal content and provide information (Arts. 8 and 9)

BEUC generally welcomes that the Commission aims to provide more clarity on Member State authorities' possibilities to issue orders to oblige intermediary service providers to act against illegal content and to request information from them. This should indeed not only be exclusive of authorities where companies decide to be established. These orders could be a potential remedy to forum shopping. If the final text is carefully drafted, Articles 8 and 9 have the potential to better protect consumers and ensure that Member State authorities where consumers are affected by the propagation of illegal content can, in principle, act to protect them.

The same way the Commission provides a notice mechanism for consumers and entities (Art. 14 *et seq.*), it is important that independent, competent authorities have the possibility to issue orders (that comply with EU laws and principles, fundamental rights included) so that the concerned company takes adequate action.

BEUC recommends extending Article 8 not only to "specific items of illegal content" but also issues in relation to illegal content in so far as it is in breach of the DSA obligations, e.g., an order to change a recommender system that does not comply with Article 29's non-profiling obligation. For the sake of legal certainty, Articles 8 and 9 should provide a **timeline** to comply with orders that would apply unless there are specific laws at EU or national level that specify a different one (e.g., for a specific type of content). This would be clear by linking these provisions with Article 1.5 of the DSA. If necessary, the timelines could be adapted to the size and resources of companies affected.

Article 9 can be important for example to identify traders that mislead consumers. When it comes to personal data requests from EU citizens, safeguards need to be put in place. Data protection principles must apply.

Finally, it is **essential that legitimate orders are enforceable**. While it would be difficult to harmonise enforcement procedures for orders of different nature, either Articles 8 and 9 or the DSA's enforcement chapter can clarify that Member States shall put in place mechanisms to ensure orders are enforced, respecting fundamental rights and the EU *acquis*, including general principles of EU and international law.

Chapter III. Due diligence obligations

BEUC welcomes that the Commission has put forward a set of obligations and distinguished obligations between different intermediary services. It does make sense to treat hosting service providers differently from mere-conduit providers, as their relationship with content is different. It also makes sense to have additional rules for hosting service providers and online platforms in particular, as they are actors that have generated a lot of concern amongst authorities and consumer organisations, for facilitating illegal activities online without being held accountable or even liable as a last resort.

BEUC recommends clarifying what 'due diligence obligations' would mean in practice. For example, the mere fact that a platform has a compliance team and filters in place to tackle illegal activities online should not mean the platform complies with relevant DSA obligations per se. Regarding the obligations proposed, BEUC recommends improvements regarding their categorisation and in terms of the substance of the obligations themselves.

3.1. Obligations' categorisation

As a general rule, the DSA must ensure that all providers ensure a high level of consumer protection, including product safety. It would be both inappropriate and confusing for consumers to create a two-tier system of consumer protection depending on whether a firm is big or small. For example, if a consumer loses a limb because of a faulty kitchen mixer, it does not matter if that product has been manufactured by Siemens or in a garage by a small company. Just like in the e-commerce Directive, all relevant intermediary services must have the same duty to protect consumers. Against this background, asymmetrical legislation (i.e., targeting certain players) can only be introduced as a means to tackle market-related problems (e.g., in the Digital Markets Act). To be proportionate, some DSA obligations can exclude micro-companies, but these exclusions should not compromise the level of consumer protection afforded. In addition, enforcement measures (e.g., sanctions) can be adapted to the size and user-base of the company.

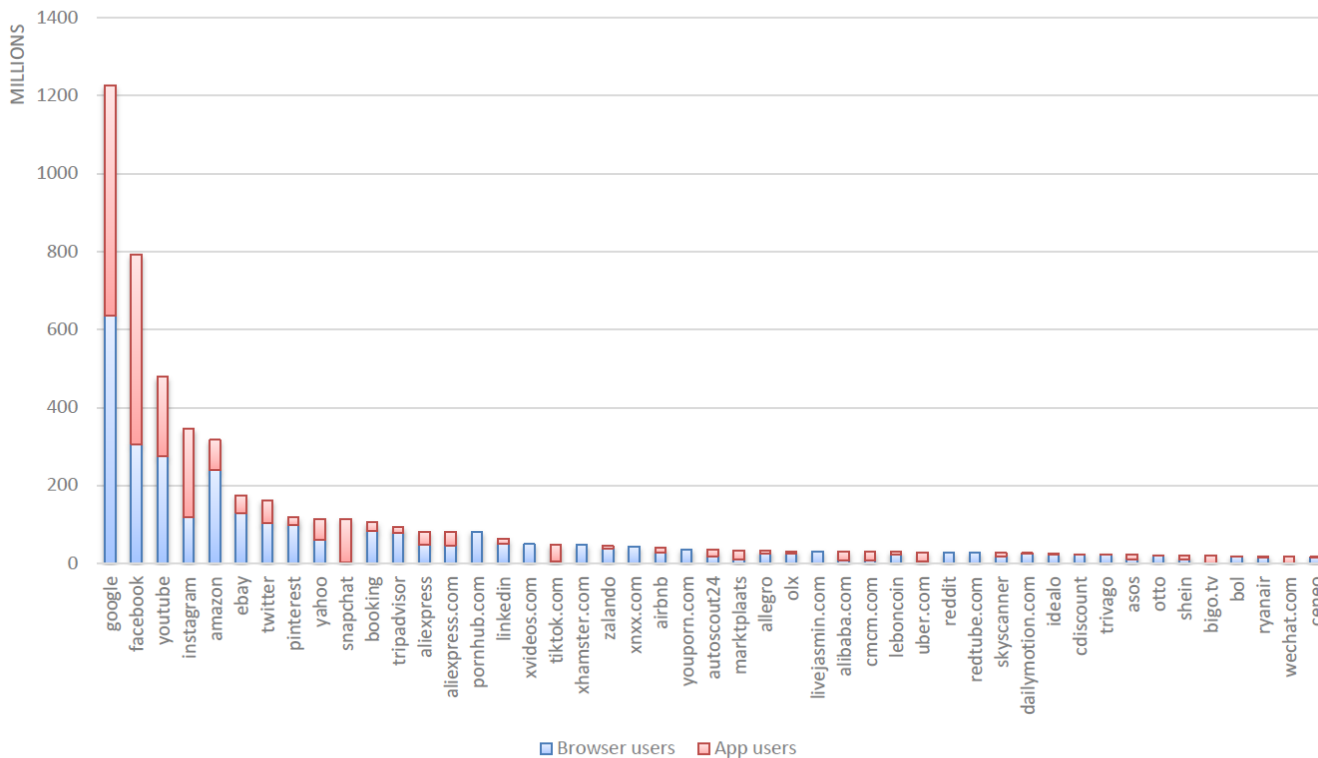
BEUC appreciates the aim of legislators to impose necessary and proportionate measures. When doing such assessment, BEUC questions the exclusion of "small" companies from all platform-related obligations (Article 16). This is particularly important for smaller EU Member States. If barely any obligations apply to their companies, the applicability and added-value of the DSA would be severely affected. Therefore, **BEUC recommends amending Article 16 to ensure this exclusion applies only to justified obligations and to truly small enterprises.** Under the annex to Recommendation 2003/361/EC⁵², a small enterprise is defined as having ≤ 50 employees and an annual turnover and/or balance \leq €10 Million. That is considerable. Similarly, some companies can have a significant user-base and plenty of illegal activities online to take care of and have a team below 50. To the very least, Article 16 should not apply to Articles 17 (internal complaint mechanism), 18 (out-of-court dispute settlement), 22 (traceability of traders), 24 (online advertising) and 29 (recommender systems).

In addition, the **definition of very large online platforms** (Art. 25) needs greater scrutiny. The 45 million average monthly active user threshold is quite high. Only very few companies would fall under these criteria. Considering the fact that the extra due diligence obligations these companies would be subject to would not be that disproportionate, the threshold should be lower. It is also not clear what "active" would mean and it may not be

⁵² <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:EN:PDF>

an appropriate qualitative criterion to indicate whether a platform poses systemic or significant risks. Any loopholes or uncertainties in how this is calculated could be used by companies to try to prevent falling under the scope of the DSA obligations.

Average monthly users in the EU (Similarweb)



According to the graph the Commission included in its impact assessment⁵³, important platforms like Alibaba or Airbnb, with millions of users and significant risks for people, may not fall under the definition of very large platforms. And this data does not seem to calculate 'active' users. In addition, not all services from the platforms covered by the definition may fall under the corresponding obligations.

Furthermore, Article 25 does not make clear what happens if the users of an online platform of a certain size and user-base exceeds 10% of the population in one or several national markets, but does not reach the 45M user threshold in the EU. Despite a company being a huge player in an EU or several EU Member States, Member State action may be impaired. This could have significant consequences for the protection of consumers in those countries where the platform should be considered a very large platform. Therefore, Article 25 should be amended to consider local thresholds.

Similarly, this article should include those companies that are not yet very large online platforms but have an exponential increase and therefore increased risks for consumers. An obvious example of this is TikTok, which was unknown to most Europeans not long ago and has recently become a very popular platform in the EU. We cannot wait until platforms become too big to care.

In addition, considering very large platforms are those that pose the most risks, it is surprising the Commission grants a grace period for the applicability of the rules instead

⁵³ European Commission impact assessment, part 2, p. 65, <https://ec.europa.eu/digital-single-market/en/news/impact-assessment-digital-services-act>

of them becoming applicable in the same way as other DSA provisions. It is unacceptable that for these rules to apply to major players, we would need to first wait to get Digital Service Coordinators appointed (“two months from the date of entry into force of this Regulation”, Art. 38.3), wait for the European Board for Digital Services to be constituted, get a methodology agreed via a delegated act – with an opinion of the Board – (Art. 25.3), then wait for Digital Service Coordinators to build a list and wait for platforms to be notified by them and then wait four months more after the publication of such a list in the Official Journal of the European Union (Art. 25.4). This process is not proportionate and would create unacceptable delays. Time is of the essence. Even digital service coordinators need to be appointed quicker than very large platforms. BEUC urges for Section 4 of Chapter III to apply at the same time as the rest of the Regulation.

In short, Article 25 should also be significantly amended to ensure all relevant companies fall within the DSA responsibilities as quickly and efficiently as possible. Building on the previous considerations, **some obligations should be extended to other services, notably the following ones:**

- Article 16 should not apply to Articles 17 (internal complaint mechanism), 18 (out-of-court dispute settlement), 22 (traceability of traders), 24 (online advertising) and 29 (recommender systems).
- Having an **internal complaint handling mechanism** (Art. 17) should apply to **all hosting service providers**, small ones included. To solve this problem, BEUC suggests including an internal complaint handling mechanism within the notice and action mechanism.
- The obligation to adhere to an **alternative dispute settlement mechanism** (Art. 18) should be applicable to **all platforms, small ones included**. This can actually be beneficial for small businesses to avoid high litigation costs. Article 17 of the e-Commerce Directive already provided for the possibility to provide out-of-court dispute settlement, without distinguishing entities depending on their size.
- The obligation regarding **trader traceability** (Art. 22) should not exclude small companies.
- **Online advertising** (Art. 24) should not exclude small companies.
- The obligations regarding **recommender systems** (Art. 29) should apply to **all platforms**, not just very large ones. This article should be moved to Section 3 of Chapter III.

3.2. The substance of the provisions

The obligations established under the DSA should also be strengthened.

Protection against dark patterns needed

BEUC recommends adding a new article in Section 2 of Chapter III, applicable to all hosting service providers. The first paragraph should make sure that the DSA ensures that hosting service providers do not design their online interfaces and/or parts thereof in a way to engage in so-called ‘dark patterns’⁵⁴. A separate paragraph should bring article 22.7 here, in a modified form (see BEUC comments on Article 22 below).

⁵⁴ Dark patterns can be described as “...features of interface design crafted to trick users into doing things that they might not want to do, but which benefit the business in question”, or in short, nudges that may be against the user’s own interest.” - How Dark Patterns Trick You Online at <https://www.youtube.com/watch?v=kxkrdLI6e6M>

Dark Patterns are built on the concept of “nudging”, identified in behavioural economics and psychology, which describes how users can be steered toward making certain choices by appealing to psychological biases. Rather than making decisions based on rationality, individuals have a tendency to be influenced by a variety of

Single point of contact and Compliance officers (Articles 10 and 32)

BEUC generally welcomes the DSA requires a single point of contact for all intermediary service providers for direct online communications with Member State authorities, the Commission and the Board, as well as trusted flaggers and professional entities “under a specific relationship” with the intermediary (recital 36).

BEUC also welcomes the establishment of compliance officers for very large platforms (which should, nevertheless, already exist). This figure would act similarly as that of a Data Protection Officer (DPO) under the GDPR, which has proven to bring benefits to companies and consumer trust. It is important that the companies provide officers with the necessary powers to conduct their tasks; and that there are protections, so they are not dismissed for trying to ensure compliance with the DSA and applicable laws⁵⁵. Digital Service Coordinators and/or the Commission should be obliged to communicate the names of the compliance officers to the authorities within the Board.

Legal representative (Article 11)

It is good that intermediary service providers not established in the EU need to appoint a legal representative in the Union. BEUC welcomes that the representative needs to be provided with enough resources and powers (Art. 11.2) and that it can be held liable for non-compliance with obligations of the Regulation (Art. 11.3). These are essential elements to ensure the effectiveness of such figure, ultimately ensuring a better enforceability of the law. At the same time, BEUC suggests adding more clarity as to what “necessary powers and resource” will mean in practice. It is important legal representatives have the power to ensure effective and swift compliance with the DSA on behalf of the company represented. **Policymakers should ensure rules are enforceable both against non-EU players that target services at EU consumers, but also against non-EU traders.**

Having a legal representative alone will not fully address current issues with the spread of illegal activities online and how non-EU traders reach consumers. For example, under the Cosmetic Products Regulation a ‘responsible person’ has been mandatory for years⁵⁶. Nonetheless, despite this, BEUC member organisations have been able to purchase all kinds of non-compliant cosmetic products online⁵⁷. Therefore, it is important Article 22 ensures online marketplaces check EU and non-EU traders. See our comments to Article 22 below.

Terms and conditions (Article 12)

BEUC also welcomes more transparency on the terms and conditions of digital services (T&C), including on how intermediary services conduct content moderation and

cognitive biases, often without being aware of it - Deceived by Design - Forbrukerradet, June 2018, <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>

⁵⁵ Inspiration can be drawn from the banking sector.

⁵⁶ Regulation (EC) No 1223/2009 of the European Parliament and of the Council of 30 November 2009 on cosmetic products, Article 4.1.

⁵⁷ For example, 21 of 39 cosmetic products bought by BEUC member, Forbrugerrådet TÆNK via Wish.com did not include the mandatory information such an ingredient list, use instructions or information on the responsible person/company. See <https://kemi.taenk.dk/bliv-groennere/cosmetics-wishcom-fail-comply-eu-legislation>

Consumentenbond likewise found that of 11 make-up sets for children bought on Amazon, Wish.com and AliExpress only 2 products had all required information. For the remaining make-up sets the included information was often incomplete, the ingredient list contained spelling mistakes or the use instructions were in Chinese (literally). 8 products moreover contained lead, a toxic heavy metal, above the legal limit. In one case – a product claiming to be ‘non-toxic’ – the legal limit was exceeded by 475 times. See <https://www.consumentenbond.nl/online-kopen/make-up-sets-voor-kinderen>

any potential restrictions and compliance with fundamental rights. BEUC recommends adding in Article 12 that terms and conditions must **disclose all remedies available, including applicable alternative dispute resolution mechanisms independent from the company.**

In addition, this article should require the provision of **a very short, clear and user-friendly summary of key T&C for consumers**, taking inspiration from Article 102 of the European Electronic Communications Code. This summary should include remedies and redress mechanisms available.

Finally, in line with Article 6.1 d) of the Consumer Rights Directive⁵⁸, it is important that the article also ensures **online marketplaces clearly inform consumers about the fact that consumers enter into contracts with both the marketplace provider and a trader**⁵⁹.

Transparency reporting (Articles 13, 23, 33)

BEUC welcomes that the DSA requires annual transparency reports on all intermediary service providers (Article 13). Because of the importance and the role that online platforms are playing in the digital economy, BEUC also welcomes the additional transparency reporting obligations for platforms (article 23) and very large platforms (Article 33).

BEUC recommends improving Articles 13, 23 and 33 to ensure **reports are written in objective terms** (not as marketing tools) and **follow a consistent methodology**. Competent authorities, researchers and public interest NGOs (consumer organisations included) should have the ability to request raw data, redacting personal data, and prove the statistics conveyed are verifiable. It is important the reports include actions taken for different types of illegal content, not just a few. For instance, we notice that among currently available reports, a lot of focus is put on intellectual property rights notice and takedowns but not so much on product safety or consumer law violations, if at all. Similarly, transparency reports should include statistics on the audience/users that use the company's services.

Reports need to be comprehensive. Amongst the measures taken, online marketplaces must also disclose the due diligence actions taken to ensure only legitimate traders are allowed in their websites, apps or any other type of software, and the spot-checks conducted on services and/or products they facilitate offering – just like consumer organisations do.

Notice and action and statement of reasons (Articles 14 and 15)

BEUC welcomes the DSA will set forth notice and action principles. BEUC recommends the following suggestions to strengthen the text.

Article 14 should **distinguish between notices from companies and notices from individuals**. In addition, **the action taken by platforms should take into account different types of illegal activities**.

BEUC particularly welcomes the Commission clarifies in Art. 14.3 that legitimate notices can give rise to actual knowledge or awareness of a potential illegal activity.

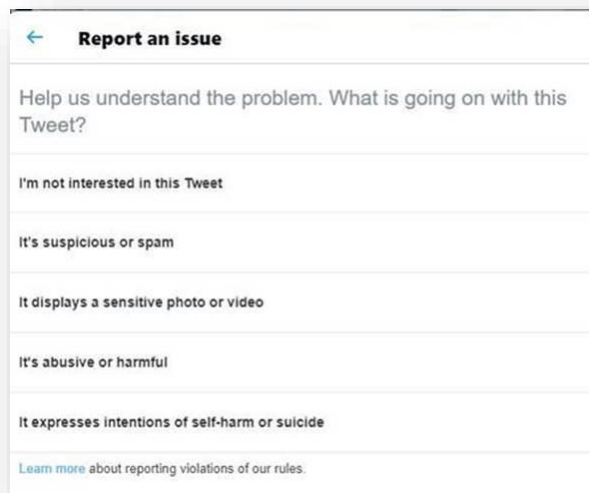
⁵⁸ Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights.

⁵⁹ Loos, M. and Luzak, J., Update the Unfair Contract Terms directive for digital services, Study requested by the JURI Committee, pp. 19-20,
[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU\(2021\)676006_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf)

We welcome the Commission aims to ensure a notice does not automatically lead to liability, but “knowledge” or “awareness”. To trigger liability, hosting service providers would have to fulfil other conditions (under Article 5.1 b), they would have to fail to expeditiously remove or disable access to illegal content). The text could be further clarified so intermediary service providers are obliged to adopt reasonable decisions on removals or disabling access to content. This will counter the incentive to automate removals or blocking upon receiving a mere notification.

From a consumer perspective, it is important that a notice by a consumer or a consumer organisation concerning, for example, the sale of an illegal product, ensures prompt removals and that the notice and action mechanism in the DSA cannot be misused as an excuse for platforms not to act or to claim the notice did not lead to awareness or knowledge of an illegal activity. To preserve freedom of expression and address complex balancing-acts, it may be relevant to differentiate between different types of illegal activities and notices depending on the stakeholder that flags them. A complementary solution is to explicitly have greater safeguards against overremovals (asking for a diligent check and reinforce or connect this with safeguards the Commission has proposed for platforms e.g., safeguards against abusive notifiers, right to reinstate legal content during the appeal process, etc). It is important to assess this provision not only from the perspective of freedom of expression but also from a consumer protection and product safety perspective. Contrary to evidence of overblocking found in the field of copyright, for example, consumer organisations have witnessed the big problem of ‘underremovals’ for consumer or product safety law violations, leading to unhindered proliferation of illegal products on platforms.

We also need to **ensure Article 14 applies when platforms treat notices as terms of service violations**, instead of a violation of the law. Current practice shows platforms have a notice and action mechanism in light of their terms and conditions, not the law, and their scope tends to be rather limited. There should always be clear options to report e.g., consumer and product safety law violations as well. The DSA should and can improve the current situation. See for example Twitter’s notice mechanism⁶⁰:



⁶⁰ Screenshot from 21 January 2021.

Regardless of how the user evaluates the content (illegal content/violation of the platform's T&Cs, even after a further request from the platform), the process must be carried out following the notice and action mechanisms of Article 14 (unless any other law provides for a content-specific mechanism).

In addition, **it is important that the mechanism to provide notices is not hidden and is well integrated in the way companies (notably platforms) present content.** For example, under the new rules a consumer should be able to report a potentially illegal activity while shopping, scrolling on a feed, when seeing an ad on a search engine and after a purchase. For example, when the consumer completes a purchase, the consumer should be informed about remedies available, including where s/he can complain. It should be clear that providing a chatbot⁶¹, a general customer service number or generally any hidden mechanism that needs to be found after several clicks would not meet the requirements of Article 14.

If the notice mechanism is provided according to BEUC recommendations, Article 2 b) should be amended as **providing a URL will not always be needed to determine which content a notifier is referring to.** E.g., if you report a tweet, Twitter knows the location of a tweet. In other platforms like Facebook sometimes you cannot copy-paste a link, so this requirement may be difficult to fulfil. However, a URL may be needed for notices to other types of internet service providers.

In addition, consumer groups have seen that **some platforms provide quite restrictive choices when reporting content (e.g., multiple choice checkboxes)**, which may limit what consumers are actually able to complain about. The DSA must ensure reporting mechanisms are comprehensive.

Ultimately, the **notice mechanism should be user-friendly, comprehensive and not too difficult for consumers to use or find.**

BEUC is supportive of Article 15 (statement of reasons) but considers hosting service providers should also be required to provide a comprehensive and detailed answer as to why they decide not to remove or disable access to illegal content referred to. The decision taken under Article 14.5 must be meaningful.

Internal complaint-handling & out-of-court dispute settlement (Arts.17-18)

BEUC welcomes both articles 17 and 18, but improvements are needed.

As mentioned earlier, it is important **article 17 (internal complaint-handling mechanism) is added to section 2 of Chapter III of the DSA** so its application is not limited to a reduced number of digital service providers.

BEUC notes that there are still insufficient requirements for ensuring the quality and independence of platforms' internal complaint handling mechanism (Art. 17) and Alternative Dispute Resolution (ADR) entities (Art.18). In addition, the relationship between the internal complaint-handling mechanism (Art.17) and the external ADR provider (Art. 18) is unclear. **These mechanisms should be provided as alternatives and this should be clearly stated in the text.**

BEUC would like to make the following recommendations:

⁶¹ A recent survey by Consumentenbond showed 78% of 10 000 consumers surveyed complain that chatbots do not provide full answers to their questions, <https://www.consumentenbond.nl/nieuws/2021/consumenten-niet-tevreden-over-chatbots>

On the one hand, **Art. 17** is insufficient to promote the transparency of the internal complaint handling mechanism. Intermediary service providers need to be obliged to **disclose the rules of procedure**. This has to be done in the terms and conditions (Article 12), but also presented to the consumer clearly when willing to complain. The rules of procedure must provide for an established **deadline to deal with the complaint internally**. This would be a tool for consumers to know that after a certain number of days, if they do not have a response, they can go to the ADR body. With a deadline, platforms will also be more likely to create well-structured and resourced internal procedures.

There should be an **obligation for the platform to clearly signpost the user to an external ADR body**, just like traders need to do it under Article 13 of the Consumer ADR Directive⁶². In other words, the internal complaint handling mechanism should not be seen by consumers as the only alternative to obtain remedies. When proposing the internal complaint mechanism, online platforms should also be required to **inform consumers that, alternatively, they have the possibility to refer their claim to the certified ADR body**.

On the other hand, **the ADR landscape should be easy to understand and to navigate for consumers**. BEUC sees a risk to have too many ADR providers certified nationally. This is important as we faced this problem with the Consumer ADR Directive. The European Commission indeed noted in its evaluation report of September 2018 on the consumer ADR Directive that “the diversity of ADR landscapes makes them difficult to navigate for consumers and traders, in particular in the Member States with a large number of certified ADR entities. Overall, there is less clarity about the ADR entity to which consumers and traders can turn when there is more than one ADR entity per retail sector”⁶³. To make sure that the landscape is clear and easily navigable for consumers, **BEUC recommends having one (or only a few) ADR providers certified at national level**.

Furthermore, **ADR entities must comply with strong quality requirements** ensuring their independence from marketplaces, their autonomy and their impartiality. Compliance with such quality criteria should be **assessed on an on-going basis**.

Requirements falling on ADR entities under the DSA are lower than those established under Directive 2013/11/EU (‘Consumer ADR Directive’)⁶⁴. BEUC recommends adding similar requirements to those set forth under Article 7 of the Consumer ADR Directive. In particular, **ADR entities under the DSA should have an obligation to draw up annual reports** highlighting *inter alia* the number of complaints received, any systematic or recurrent problems, the average time taken to resolve a dispute⁶⁵. When doing so, they should base their analysis on but should not be limited to the information submitted by platforms under Article 23 of the DSA. This is because ADR bodies need to provide their insights in an independent manner. This would be very useful both to address any serious incompliances with the DSA and, if the gaps are identified, for further eventual improvements of the DSA and its enforcement.

Similarly, there should be a **deadline for the ADR providers for processing complaints**. Under Article 8 of the Consumer ADR directive, it is not more than 90 days.

Finally, **BEUC recommends the establishment of a network of ADR entities and they should exchange information**.

⁶² Directive 2013/11/EU on alternative dispute resolution for consumer disputes, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0011>

⁶³ https://ec.europa.eu/info/sites/info/files/com_2019_425_f1_report_from_commission_en_v3_p1_1045545_0.pdf p. 9

⁶⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0011>

⁶⁵ This would mirror Art. 7.2 of the Consumer ADR Directive.

Trusted flaggers (Article 19)

BEUC welcomes that the proposal will bring more legal certainty and accountability to third parties that have a special status as 'trusted flaggers' vis-à-vis platforms. This is not a new concept. **BEUC particularly welcomes that platforms will not be able to designate 'trusted flaggers', but authorities will (Art. 19.3) and the Commission will ensure the list is public and up-to-date (Art. 19.4).** BEUC also welcomes the proposal has **safeguards against abuse (Art. 19.5-7).** However, BEUC considers improvements are needed.

First of all, Article 19.2 should clarify the criteria to be eligible as a 'trusted flagger'. In addition, **the acquisition of such status should not entail an obligation on trusted flaggers to constantly monitor platforms or all types of content.** Platforms should not simply outsource their work to trusted flaggers. Platforms should also take responsibility. For example, consumer groups have repeatedly flagged unsafe products to marketplaces, but this cannot become the modus operandi to keep consumers safe.

BEUC also strongly recommends **including safeguards to ensure platform responsibility is not shifted to third parties.** Trusted flaggers should not be used as a reason to justify a less stringent approach in the liability and responsibilities framework, particularly for those platforms that facilitate the conclusion of product and services contracts between traders and consumers.

At the same time, **the existence of 'trusted flaggers' cannot be an excuse to neglect notifications by organisations that are not (yet) recognised as such or that do not have the capacity to engage in such a role.** In fact, not all NGOs, consumer organisations included, have the resources or interest to engage in such a role, but could nevertheless report illegal activities online to platforms. This should not lead to ineffective removals.

Similarly, **Article 19 must clarify that notifications by consumers need to be treated swiftly and without delay,** in line with Article 14. It would be inappropriate for platforms to argue they are way too busy with notifications from 'trusted flaggers'. The importance of this clarification is shown by a recent Which? investigation, where several marketplaces have failed "to remove banned products – even after consumers report them". In addition, despite notices by trusted organisations, we may risk having the issue of reappearance over and over again. For example, "even when Which? experts have reported dangerous items to online marketplaces in an official capacity and the sites have taken the listings down, they have often reappeared in new listings within days."⁶⁶

Measures and protection against misuse (Article 20)

BEUC is generally supportive of this article, particularly to penalise illegitimate traders that would consistently spread illegal activities online (Art. 20.1). BEUC recommends that platforms devote best efforts to ensure suspended traders cannot re-join until the suspension is lifted. In some cases, the permanent exclusion of traders would be justified.

Notification of illegal activities to authorities (Article 21)

A duty to promptly inform law enforcement or judicial authorities (article 21) should apply not only when the life or safety of individuals is threatened under criminal law, but also

⁶⁶ Which?, Online marketplaces fail to remove banned products – even after consumers report them, Which? finds, December 2020, <https://press.which.co.uk/whichpressreleases/online-marketplaces-fail-to-remove-banned-products-even-after-consumers-report-them-which-finds/>

when online platforms become aware of other illegal activities such as fraudulent and scam ads, the sale of illegal products online.

Traceability of traders (Article 22)

Having a 'know your business user' obligation is a step in the right direction, while preserving consumer anonymity if consumers so wish. It's good the Commission does not limit this to a mere information-collection obligation. It is necessary that the platform verifies the requisites of such traders. In addition, platforms falling under the scope of this article should also conduct random checks on products and services they facilitate offering, just like consumer organisations do⁶⁷. This can contribute to ensure that if a business user uses a consumer account to circumvent these checks, the platform can realise it is in fact dealing with a trader. For that, Articles 22 and 7, and corresponding recitals, need to be amended.

Moreover, Article 22.1 needs to **clarify that online platforms shall only allow legitimate traders in their platforms**. This is important because there are investigations that show that some companies even encourage sellers into their platform that put consumers at risk.⁶⁸ A Which? investigation showed that fraudsters can create scam Facebook and Google ads within hours⁶⁹. Another Which? investigation demonstrated that it only takes a few minutes to list an unsafe children car seat on Amazon Marketplace⁷⁰, despite having flagged this type of product in 2014⁷¹, in 2017⁷², in 2019⁷³, and in 2020 following by a BBC investigation⁷⁴. This is unacceptable.

In addition, platforms covered under this article must verify existing traders, not just new traders (Art. 22.1). In addition to the criteria mentioned in Article 22.1, it is important to ensure platforms covered under the scope **verify that the third-country trader has a European branch or representative**, which is in line with existing legislation (e.g., market surveillance or cosmetics legislation).

Article 22.2 needs to make sure platforms conduct **regular and diligent checks on traders' legitimacy and the information they provide as soon as they receive it**. Relying on self-certification by the trader will not be enough. We welcome that failure to receive correct or complete information shall lead to the suspension of the trader's account. Similarly, this should happen for existing traders. Every concerned platform should verify its existing traders independently from having current suspicions – this can be done over the period of a year after entry into force of the DSA.

⁶⁷ https://www.beuc.eu/publications/unsafe_and_illegal_activities_online.pdf

⁶⁸ <https://www.wsj.com/articles/amazons-heavy-recruitment-of-chinese-sellers-puts-consumers-at-risk-11573489075>

⁶⁹ Fraudsters can create scam Facebook and Google ads within hours, Which? reveals, July 2020, <https://press.which.co.uk/whichpressreleases/fraudsters-can-create-scam-facebook-and-google-ads-within-hours-which-reveals/>

Which?, fake ads; real problems: how easy is it to post scam adverts on Facebook and Google?, July 2020, <https://www.which.co.uk/news/2020/07/fake-ads-real-problems-how-easy-is-it-to-post-scam-adverts-on-google-and-facebook/>

⁷⁰ Dangerous toys and killer car seats listed for sale at online marketplaces like Amazon and eBay, November 2019, <https://www.which.co.uk/news/2019/11/dangerous-toys-and-killer-car-seats-listed-for-sale-at-marketplaces-like-amazon-and-ebay/>

⁷¹ 'Killer car seat' alert issued by Trading Standards, September 2014, <https://www.which.co.uk/news/2014/09/killer-car-seat-alert-issued-by-trading-standards-379870/>

⁷² Watch out for 'killer car seats' on sale this Christmas, December 2017, <https://www.which.co.uk/news/2017/12/watch-out-for-killer-car-seats-on-sale-this-christmas/>

⁷³ <https://www.which.co.uk/news/2019/02/why-are-ebay-and-amazon-still-selling-killer-car-seats/>

⁷⁴ Dangerous child car seats sold via Amazon flagged by BBC Panorama, February 2020, <https://www.which.co.uk/news/2020/02/dangerous-child-car-seats-sold-via-amazon-flagged-by-bbc-panorama/>

Article 22.7 requires platforms to design and organise their websites and apps in a way that traders comply with their pre-contractual information and product safety information requirements. This **is very welcome but should go beyond pre-contractual and information requirements**. Currently, article 22.7 is only meant for platforms to support traders in complying with their obligations. It does not include platforms' compliance with their own obligations.

Platforms should design their websites and applications in a way consumers are not pushed to take certain decisions which are in the benefit of the platform or trader in question and not necessarily in the interest of consumers. The design interface should also ensure traders can easily comply with consumer and product safety laws, not just parts of them (e.g., right of withdrawal, terms and conditions). Likewise, traders that do not fulfil their obligations under consumer and product safety legislation should not be put on the platform or be suspended.

Finally, if platforms **fail to meet the obligations under Article 22, they should be able to be held liable towards consumers because of their non-compliance with this DSA obligation**. If platforms could demonstrate they did verify the trader information, including the traders' EU presence or representation, they should not be held liable for non-compliance of Article 22.

Online advertising and recommender systems (Articles 24, 29, 30, 36)

BEUC welcomes that the proposal provides for transparency obligations on online advertising in online platforms and recommender systems, including for recommender systems to provide an option for consumers not to be profiled. However, we need **stricter rules on online behavioural and micro-targeted advertising and recommender systems beyond transparency** (arts. 24, 29, 30) **and self- or co-regulation** (art. 36).

Online behavioural advertising can be defined as "online advertising that is microtargeted toward individuals or segments of consumers based on their past, current and future behaviour, which is determined based on extensive tracking and profiling"⁷⁵. Online micro-targeted advertising is based on data analysis that is targeted toward groups or individuals.

Improvements suggested:

- **Regarding transparency disclosure:**
 - All relevant parameters to target recipients in online advertising and recommender systems should be included in a meaningful way, not just the 'main' ones. In order for transparency to be useful in any way, consumers should receive **granular information about why they were shown an ad and why content has been directed at them**. This is important because the current "transparency" tools on major platforms provide information that is very general (e.g., "male, 20-45 years old located in Europe"), that is not very telling.
 - Article 24 (applicable to all online platforms) should also cover who finances the advertisement; the categories of data that targeted forms of advertising would use to address and categorise consumers and the data platforms share with advertisers for ad targeting purposes⁷⁶. Similarly, this article should include a requirement to disclose whether the advertisement is a

⁷⁵ This is the definition provided by BEUC's Norwegian member organisation Forbrukerrådet, which BEUC supports, cf. <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf> (page 184).

⁷⁶This follows the recommendation of the EDPS Opinion on the DSA, p. 16, https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf

result of an automated mechanism (such as an ad exchange system) and, if so, the name of the legal person responsible for such mechanism⁷⁷.

- The ad repository (Article 30, applicable to large platforms) shall not only include which users were included, but also the consumers and group of consumers explicitly excluded⁷⁸.
- **BEUC welcomes the requirement for very large platforms to have ad repositories.** Among other issues, they are meant to facilitate research about disinformation (recital 63). Experience from Facebook's ad repository (and others) shows it is often incomplete (not covering commercial ads) and access is partial, **the provisions need to be water-tight to have the right impact**⁷⁹. For example, it is necessary to ensure the ad repositories are comprehensive and cover all forms of marketing towards consumers (e.g., via influencers and/or hashtags).
- BEUC recommends Articles 24 and 29 **disallow cross-device and cross-site combination of data, particularly "off platform"**⁸⁰. This is important to avoid discrimination, the spread of illegal activities or harmful content such as disinformation.
- The obligations should **cover both direct and indirect forms of promoting content.** For example, BEUC found TikTok has gamified advertising by proposing to businesses advert formats such as 'hashtag challenges' and other branded filters, which are particularly appealing to young consumers. In doing so, TikTok contributes to transform users into advertising billboards without them being necessarily aware⁸¹.
- **Special protections for children below 18 must be built** in Article 24. **Behavioural and micro-targeted advertising should not be permitted towards children below 18.** This could complement proposed transparency measures as well as existing data protection and audiovisual media rules. Particularly for children, the Audiovisual Media Services Directive provides certain (but limited) protections). However, these are only applicable to video-sharing platforms and are very limited in scope. The EU cannot accept commercial surveillance on children.
- **Non-profiling by default for both children and adults should be the norm, both for advertising purposes (article 24) and for recommending content (article 29).** Profiling can lead to the spread of illegal content, harmful content (such as disinformation), discrimination and privacy violations. Profiling for both advertising and recommender systems should only be accepted as a **genuine, informed 'opt-in'**⁸², following the requirements of consent and purpose limitation under the GDPR and without engaging into so-called 'dark patterns'^{83 84}.

⁷⁷ *Ibid*, p. 15

⁷⁸ *Ibid*.

⁷⁹ Leerssen, P. & Ausloos, J. & Zarouali, B. & Helberger, N. & de Vreese, C. H. (2019). Platform ad archives: promises and pitfalls. *Internet Policy Review*, 8(4). <https://doi.org/10.14763/2019.4.1421>

⁸⁰ EDPS Opinion on the DSA, p. 16.

⁸¹ https://www.beuc.eu/publications/beuc-x-2021-012_tiktok_without_filters.pdf

⁸² In line with the EDPS Opinion on the DSA, p. 17

⁸³ <https://www.darkpatterns.org/>

⁸⁴ Similar considerations are offered in the findings of the UK Competition and Markets Authority (CMA) in the July 2020 report, more specifically the 'Fairness by design' principle and the right to use a digital service without being profiled, see e.g. UK Competition & Markets Authority, [Online platforms and digital advertising](#), July 2020, 8.90, p. 379; Appendix Y on Fairness by Design. In the context of a data-safe option for using recommender systems (Art. 29 in the draft Digital Services Act), the European Data Protection Supervisor offers that recipients of the service should have the option to make use of a recommender system which is not based on profiling, within the meaning of Article 4(4) of Regulation (EU) 2016/679. The requirement should be to opt-in rather than

Restrictions of psychographic profiling⁸⁵, which involves the use of pervasive tracking technologies⁸⁶ allowing targeting of individuals on the basis of their most intimate personal characteristics, should also be considered.⁸⁷

- **Article 36 should be deleted** as experience proves soft tools of regulation such as codes of conduct are not effective or enforceable.
- Finally, considering the risks at stake, **the introduction of additional restrictions on behavioural and micro-targeted advertising, including a possible phase-out leading to a ban on these forms of advertising, should be considered.** Advertising based on pervasive profiling and/or tracking of consumers within and outside the platform ecosystem deserve stricter rules in particular to stop behavioural advertising targeted at children. Alternative business models that are protective and respectful of consumer rights should be promoted. This builds on demands by the European Parliament, the EDPS and several civil society organisations. As shown by our Norwegian member organisation Forbrukerrådet⁸⁸, consumer harms derived from behavioural and micro-targeted advertising are considerable. These range from financial repercussions⁸⁹, to manipulation⁹⁰, discrimination⁹¹, physical danger⁹², spread of low-quality content and disinformation⁹³, but also potentially harmful content for minors⁹⁴. What is more, a recent survey showed that 68 % of respondents regarded “tracking online activity to tailor advertisements” to be unethical, while only 29 % agreed that providing more data leads to better products and services⁹⁵. In fact, there are questions about the effectiveness of invasive ads, as in some cases they only seem to create value for the middlemen, instead for advertisers⁹⁶.

This policy option would complement – not replace - the GDPR or its enforcement. The DSA and the GDPR have different objectives and their scope is different. The latter regulates how to process personal data and the former would regulate and bring more legal certainty to the advertising models that are allowed. It would

opt-out, making the option not based on profiling the default one ([EDPS Opinion 2021/1, on the Proposal for a Digital Services Act](#), para. 74).

⁸⁵ Post-Cambridge Analytica research shows that extremely fine-grained profiles allow psychographic targeting: designing messages for individuals based on psychological variables such as personality characteristics (extroversion, neuroticism, authoritarianism, etc.), attitudes, and interests, and other psychological information that can be either obtained or inferred. These techniques are referred to as psychographic profiling. For a discussion on different grades of profiling, see Burkell, J. & Regan, P. M. (2019) [Voter preferences, voter manipulation, voter analytics: policy options for less surveillance and more autonomy](#). Internet Policy Review, 8(4). DOI: 10.14763/2019.4.1438.

⁸⁶ In this sense, the European Data Protection Supervisor calls for a phase-out and prohibition of targeted advertising based on data collected through pervasive tracking technologies, combined with restrictions on categories of data which can be processed and disclosed for purposes of targeted advertising. See [EDPS Opinion 2021/1](#), para. 69.

⁸⁷ Under the auspices of the EU Consumer Protection 2.0 project, with co-financing by the Adessium Foundation, BEUC is exploring how consumer law can best safeguard consumers against harms arising from commercial practices in digital markets. The main research study forming the backbone of this project is available at https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf.

⁸⁸ <https://www.forbrukerradet.no/out-of-control/>

⁸⁹ E.g., <https://www.fastcompany.com/90318224/nor-wanted-by-equifax-and-other-credit-bureaus-your-alternative-data>

⁹⁰ E.g., https://www.beuc.eu/publications/beuc-x-2021-012_tiktok_without_filters.pdf

⁹¹ E.g., <https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin>

⁹² E.g., <https://www.independent.co.uk/news/world/africa/egyptian-police-grindr-dating-app-arrest-lgbt-gay-anti-gay-lesbian-homophobia-a7211881.html>

⁹³ E.g., <https://www.buzzfeednews.com/article/craigsilverman/how-a-massive-ad-fraud-scheme-exploited-android-phones-to>

<https://promarket.org/how-the-adtech-market-incentivizes-profit-driven-disinformation/>

⁹⁴ https://www.beuc.eu/publications/beuc-x-2021-012_tiktok_without_filters.pdf

⁹⁵ <https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf>

⁹⁶ See, for example, <https://www.wired.com/story/ad-tech-could-be-the-next-internet-bubble/>

contribute to a fairer society and is not intended to harm small business or to outlaw all forms of advertising, but to promote healthier and more sustainable advertising business models over time that do not harm individuals and society as a whole⁹⁷. In fact, the Dutch broadcaster NPO saw ad revenue increase when it decided to change its advertising scheme to a less invasive one, eliminating unnecessary and non-law-compliant middlemen⁹⁸.

Risk assessment, mitigation of risks and independent audits (Arts. 26-28)

BEUC very much welcomes these provisions as they can be a way to address some of the concerns civil society and policy-makers have identified on major platforms over the years, including the spread of illegal but also harmful content, such as disinformation.

We would advise for these assessments to be **public and written independently in objective terms (not as marketing tools)**. These **companies must be obliged to implement the recommendations of independent auditors validated by authorities. It is important platforms submit the findings of their risk assessment and auditors to authorities**, which, in turn, can assess whether the recommendations are suitable or must be subject to improvement. In this sense, policymakers can draw inspiration from articles 35 and 36 of the GDPR. Authorities must provide clear guidance as to what is expected from these exercises. In addition, the DSA must specify articles 26-28 cannot lead to a presumption of compliance with the DSA or other applicable laws. Otherwise, these tools may risk being ineffective for the aims pursued.

BEUC also recommends expanding the risk assessment list in Art. 26 as it is currently too narrow. Article 26.1 b) **omits referring to consumer protection**. Art. 26.1 b) should not be limited to a small number of articles from the EU Charter of Fundamental Rights. It is important to recall that consumer protection is embedded in Article 38 of the Charter. **Consumer protection should be included**. In addition, Art. 26.1 c) must include **risks of deception or manipulation of consumers**.

Similarly, **Article 26.1 should contain a specific risk assessment for online marketplaces**. Tackling systemic risks that online marketplaces incur when hosting offers selling unsafe products or non-compliant services should be of paramount importance.

BEUC also welcomes **Article 26.2** but considers **the risk assessment must also include any potential infringement of consumer rights by business active on the platforms and the platforms themselves**, including consumer manipulation, unfair subversion or impairment of consumers' autonomy, decision-making, or choice.

Finally, **Article 27** should also include **mitigation measures for online marketplaces, including random checks on the products and services** they facilitate offering or promoting.

Data access and scrutiny (Article 31)

BEUC is **very supportive** of this provision and can suggest further improvements. Platforms must share relevant data with competent authorities and independent researchers, redacting and anonymising personal data, as appropriate.⁹⁹

⁹⁷ See alternative business models that this policy option would promote: <https://dataethics.eu/4-alternatives-to-the-current-creepy-digital-advertising-model/>

⁹⁸ https://www.theregister.com/2020/07/03/stop_tracking_increase_revenue_effectiveness/

⁹⁹ See, for example, European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

Art. 31 should also enable all Digital Services Coordinators (and relevant authorities) to require data, not just the Digital Services Coordinators of the Country of establishment or the Commission. In line with the Opinion of the European Data Protection Supervisor (EDPS)¹⁰⁰, BEUC recommends **extending the scope** of Art. 31 to:

- include data access for research that can **verify the effectiveness of the risk mitigation measures** taken by very large platforms (Article 27).
- Include **vetted researchers from civil society organisations representing the public interest**. These must prove the research is genuinely conducted for public interest purposes and are independent from any corporation or corporate interest, funding included (Art. 31.4).

In any case, as the European Data Protection Supervisor has pointed out, “data protection should not be misappropriated as a means for powerful players to escape transparency and accountability. Researchers operating within ethical governance frameworks should therefore be able to access necessary API and other data, with a valid legal basis and subject to the principle of proportionality and appropriate safeguards”¹⁰¹.

Standards (Article 34)

BEUC and ANEC (the European consumer voice in standardisation) are concerned that Article 34 asks the Commission to support and promote voluntary industry standards. The use of standards in legislation/policy must follow specific rules on the elaboration of technical standards/Harmonised Standards in an inclusive way, according to Regulation (EU) 1025/2012. Consumer organisations contribute to such standardisation process, so we suggest that **article 34 should not promote “voluntary industry standards”, but standards subject to transparent, multistakeholder and inclusive processes**.

Regulation (EU) 1025/2012 also contains provisions on the identification of ICT technical specifications that are not national, European or international standards, but meet the requirements set out in Annex II. We also base our request on the priorities of the Annual Union Work Programme for European standardisation for 2021 (2020/C 437/02)¹⁰² which identifies the European standards and European standardisation deliverables that the Commission intends to request for the year 2021. Priority 20 is about Online Platforms and refers to the Proposal for a Digital Services Act.

Codes of conduct and crisis protocols (Articles 35-37)

BEUC is very sceptical about the inclusion of non-enforceable codes of conduct to tackle illegal activities and content as well as systemic risks under the DSA. These are already possible under Article 16 of the e-Commerce Directive, but that provision has never led to any real added value or effective protection for citizens or consumers.

For the reasons stated earlier, given the big risk and dimension and potential harm for individuals and society, **BEUC recommends to at least delete Article 36**, since the problems with tracking- and profiling-based online advertising will not be solved by soft law.

If Codes of Conduct are included, there should be clear and strong governance and a monitoring system that each code has to be submitted to as well as greater requirements of transparency and inclusiveness. These must *inter alia* include:

¹⁰⁰ EDPS Opinion on the DSA, p. 18, https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf

¹⁰¹ *Ibid.*

¹⁰² https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2020.437.01.0004.01.ENG&toc=OJ%3AC%3A2020%3A437%3ATOC

- A **balanced and transparent composition** They should truly be of a **multi-stakeholder nature**, not only done between the Commission and very large platforms. The Commission must (not 'may') ensure the participation and meaningful inclusion of civil society organisations representing the public interest, including consumer organisations. The Code must take utmost account of the views of civil society organisations. This is important to ensure the Commission is supported by NGOs that want to contribute to protect and respect citizens' rights. To ensure their participation, resources for civil society organisations working for the public interest must be facilitated.
- **Clear and precise consumer protection objectives.**
- A **regular transparent and thorough evaluation.**
- In addition, **reporting and review of the results** should be communicated to the whole Board and be public on a timely manner.
- **Effective and dissuasive sanctions** in case of the intermediary service providers do not respect the commitments made.

Finally, BEUC also strongly recommends introducing a requirement in Articles 35-37 and/or Article 73 to ensure that if the codes **fail to get the expected results, the Commission shall be required to make legislative proposals**. This would complement Art. 37.5 but also recital 68, which establishes that refusals to participate in codes of conduct can determine whether relevant DSA obligations have been infringed.

Chapter IV. Implementation, cooperation, sanctions and enforcement

BEUC welcomes that a substantive part of the DSA has been dedicated to the implementation and enforcement provisions. BEUC would like to suggest the following improvements:

- BEUC welcomes the designation of independent Digital Services Coordinators and the obligation to **cooperate between themselves, but also with other competent authorities** (Article 38). **BEUC also recommends that the Board makes available a list of the competent authority or authorities** designated by Member States.
- BEUC recommends that Article 39.1 is changed to **ensure** Digital Services Coordinators have not only 'adequate' but **all 'necessary' resources, premises and infrastructure to effectively carry out their tasks and powers**¹⁰³. These should include "in-depth technical skills, including data processing and auditing capacities, which would allow for a reliable and thorough oversight and transparency of algorithmic decision-making processes"¹⁰⁴. This is necessary to ensure the exercise of the power conferred under Article 41.1. In the exercise of their tasks, it is important Coordinators and the Board cooperate with and seek advice from relevant authorities for matters outside their competence. For example, if they audit algorithms based on personal data, they should engage with data protection authorities and seek the opinion of the European Data Protection Board (EDPB) in cross-border cases.
- BEUC welcomes Digital Service Coordinators do not only have powers to impose penalties (Art. 42), but also other important powers (Art. 41), such as on-site inspections. BEUC would like to add two more powers. First, **BEUC recommends**

¹⁰³ This draws inspiration from Article 52.4 of the GDPR.

¹⁰⁴ In line with stakeholder requests under the DSA public consultation, cf. <https://ec.europa.eu/digital-single-market/en/news/summary-report-open-public-consultation-digital-services-act-package>

clarifying in Article 41.2 b) that Digital Service coordinators should be able to order platforms to compensate consumers (where needed/relevant). Second, authorities must have the **power to order the “prohibition on the deployment of open content recommendation systems at least until compliance is guaranteed and the [consumer and] fundamental rights of online users are sufficiently protected”¹⁰⁵.**

- **Consumers must have effective (and proportionate) remedies**, including repair, replacement, price reduction, contract termination or reimbursement of the price paid, compensation for material and immaterial damages for breaches of the DSA obligations¹⁰⁶. Specific remedies for consumers shall be foreseen in case the intermediary service provider is in breach of its own obligations listed in this Regulation, for example in case of breach of transparency obligations (notably Articles 12, 24, 29, 30) or of the obligations to “know your business customer” as specified in Article 22 of the proposal. This is also important to render the inclusion of the DSA in the Representative Actions Directive (Article 72 of the DSA proposal) workable in practice. Public enforcement alone will not be sufficient.
- For the sake of legal certainty and effectiveness of enforcement, the **DSA must clarify that when enforcement authorities or networks exercise their powers under other laws, the DSA enforcement network should not interfere and add further delays.** The DSA enforcement structure should intervene in relation to DSA obligations. In any case, it is important that when the DSA Board, the Commission and Digital Service Coordinators address matters dealt with in other laws, they should cooperate and seek advice from other EU enforcement networks, including the Consumer Protection Cooperation (CPC) network and the EDPB.
- In order to **promote joined up and consistent enforcement of the complementary objectives under the DSA and the Digital Markets Act (DMA)**, where information received by the competent enforcement authorities during a DSA investigation is also relevant for gatekeepers’ obligations under the DMA and, vice versa, where information received by the Commission in a DMA investigation is also relevant for gatekeepers’ DSA obligations, there should be a provision in the DSA (and DMA) for the sharing of this information between the European Commission and the Digital Services Coordinators.
- In terms of jurisdiction (**Art. 40**), **BEUC welcomes that Chapter II is excluded.**

As per the applicability to Chapters III and IV, BEUC would rather propose a mixed jurisdiction mechanism, in line with Article 43 (right to lodge a complaint) of the DSA proposal, the e-Commerce Directive (Article 3 and the consumer contracts derogation under the annex) and consumer protections afforded under Private International Law rules, namely under Article 18 of Regulation 1215/2012 of 12 December (“Brussels 1 bis”) which gives consumers the option to sue traders before the court of their domicile.

¹⁰⁵ <https://www.accessnow.org/cms/assets/uploads/2020/10/Access-Nows-Position-on-the-Digital-Services-Act-Package.pdf> - inspired from article 58 of the GDPR.

¹⁰⁶ This is only natural under several Member States tort and/or contractual laws and also under EU laws such as the Unfair Commercial Practices, as amended by Directive (EU) 2019/2161 (Article 11a); or the GDPR (Article 82). An alternative is to use the wording recommended under the European Law Institute Model Rules on Online Platforms, Articles 19-25, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf

While business users may be able to afford expensive foreign lawyers and engage in a foreign language, this is almost impossible for consumers. Such barriers can discourage consumers and consumer organisations representing them. Article 40 could also mean that in the event of a representative action against a platform (Art. 72), the competent authority and courts would be the ones where the platform is located. This puts effective and swift consumer protection and redress at risk.

We have seen the problems of following a country-of-origin principle for jurisdiction under the GDPR, where enforcement is bottlenecked in very few countries. Such principle turns some national authorities into pan-European bodies without sufficient resources or pan-European-law-expertise. A better option is to **make the country of consumers affected the preferred jurisdiction for consumer complaints/issues.**

We commend the proposal tries to address some of the pitfalls of the country-of-origin jurisdiction, notably by creating a **fall-back option for the Commission in case of inaction of the authority of the Member State of establishment under certain circumstances** (Article 45). However, we fear this fall-back option may come too late, or not at all. In fact, under the DSA proposal the Commission reserves the right to exercise its powers, but does not oblige itself to take a decision (cf. Arts. 50.1 and 51.1, 51.2; recitals 96 and 97). This should be changed.

The question then is whether there are sufficient guarantees in the text to make sure that enforcement will work in practice. Even if authorities organised joint investigations (art. 46), consumers and their representatives would still have to rely on the willingness of one Member State authority or the Commission to act (cf. Art. 45.4-7; art. 46; arts. 51 et seq.). It is not only important to complain before the authority where the consumer resides (Art. 43), but that the matter is not resolved by foreign judicial or administrative authorities. In addition, article 43 must ensure that **consumers and organisations representing consumers have a right to get a response from authorities within three months.**

- **BEUC welcomes there is a possibility for enhanced supervision against very large platforms** by the Commission (Arts. 51 et seq.). We suggest improvements, including the following:
 - In case platforms offer commitments (Art. 56) and before the European Commission adopts a decision, it shall seek advice from third parties (notably parties that brought complaints before the authorities), including civil society organisations, consumer organisations included.
 - In Art. 63 platforms and eventually traders (Art. 52.1) are the only ones that have clear rights to be heard and access the file, not consumers or NGOs that would bring a complaint to competent authorities. **Arts. 63 and 52 as well as recital 101 must be clear that other relevant parties must be heard, access the file and be able to get information shared.** This is also a problem encountered in the DMA, which runs contrary to competition law¹⁰⁷.
 - Article 58.1, a) should clearly stipulate that **in case of violations of the DSA obligations, the Commission must act.**
 - The Commission should not have a limitation period for imposing or enforcing the penalties. **Articles 61 and 62 should be deleted.**

¹⁰⁷ Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, Official Journal L 1, 04.01.2003, p.1-25 (Chapter VIII) and its implementing regulation, Commission Regulation (EC) No 773/2004 of 7 April 2004 relating to the conduct of proceedings by the Commission pursuant to Articles 81 and 82 of the EC Treaty, Official Journal L 123, 27.04.2004, p. 18-24 (Chapter V).

- **BEUC welcomes the establishment of an information sharing system (Art. 67) and a European Board for Digital Services (EBDS, Arts. 47-49).** However, we recommend **it should be chaired by an independent authority on a rotatory basis**, not the Commission, **and the EBDS should have its own secretariat to ensure its independence**, just like the European Data Protection Board. Therefore, Articles 48.3 and 4 should be amended accordingly.

Chapter V. Final provisions

Article 71 of the proposal replaces articles 12-15 of the e-Commerce Directive. As mentioned earlier, **the DSA should amend the scope of the e-Commerce Directive to also cover digital service providers established outside the EU.** Otherwise, the provisions of the Directive would still not apply to these entities, leading to unfair competition, an uneven playing-field and leaving consumers potentially exposed to wrongdoings that are not accepted in the EU.

BEUC welcomes article 72 adds the DSA into the annex of the EU Representative Actions Directive¹⁰⁸. This is important, because while the e-commerce Directive is included in such annex already, the DSA does not replace the Directive in its entirety. In order to maximise the potential of the Directive, it is necessary to clarify consumer remedies in the DSA as well as establish the relevant liability provisions. The criteria to represent consumers, foreseen in Article 68, only seem to apply to Articles 17 (internal complaint handling), 18 (ADR) and 19 (Trusted flaggers). To be able to bring a representative action on behalf of consumers (injunction or collective redress action) for an infringement of the DSA, an association should simply need to comply with the criteria for legal standing foreseen in the Representative Actions Directive. **Article 68 should not apply to the representation already regulated under the Representative Actions Directive.**

BEUC welcomes the Commission introduced a requirement to evaluate the DSA (Art. 73). **However**, we consider the frequency of such reports should be shorter than five years. We have seen that the economy can evolve in unexpected ways and EU policymakers must be ready. Just like under the e-Commerce Directive, the Commission should evaluate the rules **every two years**. This will allow the Commission to present evaluation reports relevant for both instruments. BEUC considers that for the evaluation reports, the Board should also be consulted as well as stakeholders, ensuring Multistakeholder diversity (not just consultation with big players, for example). To alleviate the Commission's task, this could be **combined with the additional assessment** proposed on the functioning of the European Board for Digital Services. Finally, BEUC welcomes the Commission opens the possibility to adopt **amendments in the future**, but this **should not only be limited to the functioning of the Board**, where necessary and appropriate. This should include relevant provisions, including on the need to legislate following the failure of self- and co-regulation.

¹⁰⁸ Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC

Finally, **BEUC welcomes** that Article 74 proposes a **swift entry into force** (twenty days after its publication) **and application** (three months after the entry into force). **Any exception to the swift application and enforcement of the DSA should be treated with care.** As mentioned earlier, we recommend amending Article 25.4 which states that the extra obligations for very large online platforms only apply 4 months after the publication of the list designating them as such. BEUC considers it is not justified to further delay the application of the rules to potentially major carriers of risks and illegal activities online.

- END-



This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2021-2027).

The content of this publication represents the views of the author only and it is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.