The Consumer Voice in Europe

TOWARDS A SAFER, MORE PRIVATE AND SECURE INTERNET FOR CHILDREN IN ONLINE PLATFORMS

BEUC's input to the European Commission's call for evidence under Article 28(1) of the Digital Services Act

Contact: Maria Merkou – 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-2024-074 - 30/09/2024

Why it matters to consumers

As one in three online users in the world are children,[1] the need for the EU to build a safe, secure and private online experience for them is urgent. Children should be able to enjoy the benefits of the internet, build communities and express themselves. However, some online platforms have exposed them to a series of risks. With deceptive and manipulative practices, addictive design features and engagement-based recommender systems being the norm, children cannot enjoy the online world without harm or risk. The forthcoming European Commission guidelines to assist online platform providers to comply with their obligation to ensure a high level of privacy, safety, and security for minors, as required by Article 28(1) of the Digital Services Act (DSA), present a unique opportunity to ensure a safer, more secure and private internet for the most vulnerable of consumers.

Summary

BEUC welcomes the opportunity to contribute to the call for evidence[2] launched by the Commission to support drafting guidelines under Article 28(1) of the DSA to assist online platform providers to better protect children online.

BEUC recommendations:

- The guidelines must bring additional clarity to both regulators and online platforms on which practices are likely to infringe the law, leaving no room for circumvention by companies.
- Age verification tools cannot replace age-appropriate design and key features to protect children by default and by design. Such tools must always provide a high level of cybersecurity, privacy, personal data protection and anonymity when deployed.
- The guidelines must not consider current practices of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines as 'good' or 'best' practices' as they can be significantly improved to deliver safety, security and privacy to minors online - instead the guidelines must be informed by the best scientific evidence on how to effectively address online harms to minors.
- The guidelines must ensure that Article 28(1) DSA is read and applied in conjunction with the rest of the DSA provisions and relevant EU legislation including children-specific provisions, such as the General Data Protection Regulation (GDPR), the Audio Visual Media Services Directive (AVMSD) and EU consumer law such as the Unfair Commercial Practices Directive (UCPD), the Consumer Rights Directive (CRD) and the Unfair Contract Terms Directive (UCTD), the General Product Safety Regulation and the revised Toy Safety Regulation.

[1] For the purposes of this paper a child is considered to be every human being below the age of eighteen years-old, as defined by the United Nations Convention on the Rights of the Child, article 1. The terms 'minors' and 'children' are thus used interchangeably.

[2] Available here, accessed 12/09/2024: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines_en

- The guidelines must encourage structured dialogue and cooperation between different enforcement authorities supervising legislation pertaining to children's rights online when enforcing Article 28(1) of the DSA.
- The guidelines must require engagement and interaction-driven algorithmic recommender systems to be off by default in accounts set up or used by minors. Algorithms must prioritise quality, guardians' and children's feedback and explicit signals when ranking content.
- The guidelines must provide an open list of measures for online platforms to tackle addictive design. Such measures must for example preclude features such as the default autoplay of videos, default 'infinite scrolling', 'push notifications', 'streaks', 'pull-to-refresh' page reload, the '...is typing' functionality, 'read-receipt notifications', and popularity metrics such as 'likes and dislikes'.
- By default, minors' accounts must be private and not open to the public. Any features tracking minor's accounts must be turned off.
- The guidelines must provide a strict interpretation regarding advertising and any other commercial communication to children and clarify that children's data cannot be used for commercial purposes by online platforms.
- Participation in relevant codes of conduct must not lead to a presumption of compliance.

1. Introduction

While consumers enjoy the benefits of the online experience in many aspects of their lives, the increasing risks and harms associated with online platforms led to the introduction of recent EU legislation. As our lives increasingly shift to the digital sphere, children are directly affected by this transformation.

The EU's Digital Services Act (DSA)[3] explicitly acknowledges children's vulnerabilities online, obliging online platforms to implement a high level of privacy, safety and security for minors.[4] With the exception of some examples in recital 71, the DSA does not prescribe exactly how to achieve this obligation. The DSA provides that the Commission may draft guidelines to assist providers of online platforms in the application of this provision[5]. These guidelines present a unique opportunity to pave the way for a safer online experience for children, by requiring online platforms to be more accountable and responsible towards minors.

In light of the above, BEUC welcomes the opportunity to provide input for the elaboration of these guidelines.

2. Time to take action for children online - clear guidance for regulators and online platforms is needed to minimise circumvention

Children and adults alike are exposed to the highly abusive practices of some online platforms whose business model is based on the exploitation of people's personal data.[6] To maximise revenue, online platforms ranging from social media to online marketplaces

[3] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).
[4] *Ibid*, article 28 (1).
[5] *Ibid*, article 28(4).
[6] See for example https://www.beuc.eu/blog/children-are-vulnerable-consumers-and-need-more-protection-on-tiktok/.

design their services so as to prompt user engagement through the implementation of addictive features. These vary from profiling minors to target them with hyper-personalised content and engagement-based algorithms, to use of gaming and gambling features, using consumers' personal data for advertising, and using data to train their artificial intelligence (AI) systems.[7] All these methods seriously threaten children's privacy by turning the internet into an environment they cannot enjoy without risk. As mentioned in BEUC's 2023 survey report on the fairness of the digital environment, children are one of the most vulnerable and influenceable groups in society, as they spend a large amount of time in online environments.[8] In this data-driven ecosystem, children's privacy, safety and security are constantly sacrificed to drive profit and economic value for online platforms' shareholders. As research has shown that children feel exposed while using online services,[9] it is time to take action.

To effectively protect children online, we need to build on lessons learnt and stop online platforms from continuing to use substandard and deceptive practices. As online platforms like TikTok or Instagram, which are extremely popular amongst children in EU countries,[10] are notorious for not complying with their obligations under EU data protection[11] and consumer law[12], the Commission must seize this opportunity by providing clear examples to companies of professional diligence practices that effectively respect children's rights online and those likely to infringe their obligations.

The following examples can help to illustrate online platforms' lack of diligence and compliance, both before and after the entry into force of the DSA. Especially in the case of the current practices of Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs), many of these companies falsely claim to be compliant with EU legislation while there are good reasons to suspect that they are infringing their obligations. TEMU's terms of use for instance require that consumers demonstrate they are above 18 years old,[13] while a BEUC complaint under the DSA from May 2024 illustrates that the online marketplace's services were accessible to minors at the time the complaint was launched, as no appropriate steps were taken to ensure their services were age appropriate. At the time of the complaint, TEMU had not implemented any meaningful or effective measures to keep

Very Large Online Platforms and Search Engines are notorious for repeatedly and persistently infringing consumer and personal data protection laws. Their current practices are far from being considered 'good practices' without prior independent audits.

[7] The Irish Data Protection Commission decisions against BigTech companies Meta, and X requiring them to stop training their AI systems using users' personal data followed complaints launched with national Data Protection Authorities by civil society organisations such as noyb and BEUC members Forbrukerrådet, OCU, TestAchats, Altroconsumo.
[8] BEUC digital fairness survey report, no 35.
[9] https://www.amnesty.org/en/documents/POL40/7349/2023/en/; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN.
[10] Available here, last accessed 06/09/2024: https://www.statista.com/statistics/1337425/tiktok-users-age-group-germany/#:~:text=The%20most%20TikTok%20users%20in,that%20they%20used%20the%20platform.
[11] Available here, last accessed 06/09/2024:https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok.
[12] The CPC Network launched a formal dialogue with TikTok on the basis of a BEUC external alert, available here, last accessed 06/09/2024: https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/social-media-and-search-engines_en#tiktok; Italian Competition Authority: TikTok sanctioned for an unfair commercial practice, available here, accessed 04/09/2024: https://en.agcm.it/en/media/press-releases/2024/3/PS12543.
[13] TEMU, Terms of Use, available here, and last consulted on 11/09/2024: https://www.temu.com/terms-of-use.html?refer_page_name=digital-services-act-help&refer_page_id=19327_1726060238113_11ynjq4imo&refer_page_sn=19327&_x_sessn_id=lz8h3dddtm.

minors off the platform, showcasing that such claims to be compliant can be unjustified and misleading.[14]

TikTok is another example where in the past BEUC and its members revealed the platform's failure to comply with consumer and data protection legislation pertaining to children's rights online. Following BEUC's external alert[15] to the Consumer Protection Cooperation Network (CPC) about the platform's illegal practices, the commitments and modifications made by TikTok to bring its services into compliance with EU consumer law, were deemed by BEUC to be insufficient .[16] In a second letter to the CPC Network authorities, BEUC highlighted persistent infringements of children's rights, including breaches of data protection requirements.[17] For example, regarding consent, BEUC discovered that TikTok's data processing relies on 'dark patterns', using ambiguous clauses that leave consumers unable to clearly understand what they are actually consenting to.[18]

The guidelines must explicitly preclude the use of such manipulative practices as benchmarks, as this would expose children to additional harm. Instead, the guidelines must require compliance measures to be independently evaluated by auditors, regulators and the Commission's services. The guidelines must follow the good example of the Digital Markets Act (DMA) as regards choice screens. To demonstrate effective compliance as required by Article 8 of the DMA), it is essential for gatekeepers to test each of their end user interface designs on actual consumers in relation to the terms of the relevant DMA obligation and the DMA's anticircumvention provision prior to the roll-out of the user interfaces to make sure that consumers understand the choice that they are being asked to make and to ensure that their choices are freely given, specific, informed and unambiguous. The user interface designs should also be subject to prior consultation. The testing results and data on the choices made by end users following roll-out should be provided to the Commission and relevant third parties for analysis of compliance.[19]

BEUC acknowledges that the Commission cannot introduce strict normative rules by means of guidelines. However, BEUC urges the Commission to use this opportunity to provide examples of practices and features implemented by online platforms that are likely to be in breach of the law pending proper investigation and assessment by regulators and the Commission. This would ensure more predictability and send the signal to online platforms that authorities and the Commission will closely scrutinise the measures they put in place and take all appropriate steps to ensure compliance with the law.

BEUC Recommendations:

- The guidelines must bring additional clarity to both regulators and online platforms on which practices are likely to infringe the law, leaving no room for circumvention.
- Existing practices of VLOPs and VLOSEs must not be considered *a priori* as sufficient to protect the safety, security and privacy of minors online.

[14] BEUC complaint against TEMU under the DSA, https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-046_Temu_Why_the_fast-growing_online_marketplace_fails_to_comply_with_the_DSA.pdf.
[15] See BEUC report, TikTok without filters : a consumer law analysis of TikTok's policies and practices, published together with our external alert on February 2021.
[16] Letter from BEUC to the European Commission: BEUC's assessment of the implementation of TikTok commitments following the CPC-Network coordinated action. Ref.: BEUC-L-2022-299/UPA/SBE/rs 14, December 2022.
[17] https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-019_Holding_TikTok_accountable_a%20reality_check.pdf
[18] Marta Cantero Gamito, & Hans-W. Micklitz, Report assessing the Consumer Protection Cooperation Network in the protection of consumers and children on Tiktok, available here, last accessed 06/09/2024: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-018_Assessing_CPC_Network_in_the_protection_of_consumers_and_children_on_TikTok-Report.pdf.
[19] Available here, accessed 25/09/2024: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-062_Summary-non-compliance-reports-gatekeepers.pdf.

3. Children's protection online is a multi-layered issue – interplay with other provisions and other EU legislation

To ensure the approach taken is aligned with the rest of EU law, resulting in the highest level of safety, privacy and security possible for minors, the guidelines for compliance with Article 28(1) should not be considered in a vacuum. As mentioned above, the DSA is not the first piece of EU legislation to address children's rights online. Consumer and data protection laws, such as the GDPR, the UCPD, the CRD and the Audio-Visual Media Services Directive (AVMSD)[20] already include provisions stressing that children should be afforded specific protection due to vulnerabilities linked to their young age. Similarly, the General Product Safety Regulation (GPSR)[21] and the current proposal for a Toy Safety Regulation (TSR)[22] include provisions relevant for the online sale of products and toys.

In addition, the DSA includes a series of provisions specifically aimed at better protecting minors on online platforms. For example, the DSA requires that terms and conditions of all platforms directed at minors should be easily understandable for children,[23] and establishes a blanket prohibition of presenting targeted advertising that is based on their profiling.[24] Moreover, the DSA imposes additional requirements on VLOPs and VLOSEs, obliging them to embed mitigating measures for negative effects on minors.[25] Other relevant non-children-specific DSA provisions foresee that users must have transparent choices about recommender systems[26] and prohibit online platforms from designing, organising or operating their online interfaces in a way that deceives or manipulates consumers.[27]

Against that backdrop, it is important to ensure the guidelines take due account of the DSA as a whole and the aforementioned EU laws protecting children and their rights. To ensure alignment with the GDPR principles of privacy by default and privacy by design[28] in particular, it is essential that the guidelines' approach is proactive, focusing on integrated and default features and measures. Moreover, the Commission must clarify the interlinks between the different EU laws applicable on that matter, following the example of the Commission guidance issued on the UCPD[29] and CRD.[30]

To this end, we encourage the Commission to engage with different enforcement authorities and networks responsible for supervising other key laws[31] such as the GDPR, the ePrivacy Directive, the AVMSD, the DSA and consumer legislation such as the UCPD,

[20] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.
[21] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA relevance).
[22] The Toy Safety Regulation proposal is currently under discussion: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the safety of toys and repealing Directive 2009/48/EC COM/2023/462 final.
[23] DSA, Article 14(3).
[24] *Ibid*, Article 28 (2).
[25] *Ibid*, Article 34 and 35.
[26] *Ibid*, Article 27.
[27] *Ibid*, Article 25.
[28] GDPR, Article 25.
[29] Available here, accessed 12/09/2024:https://eur lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52021XC1229(05).
[30] Available here, accessed 12/09/2024: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021XC1229%2804%29&qid=1640961745514.
[31] Available here, accessed 12/09/2024: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-135_Strengthening_the_coordinated_enforcement_of_consumer_protection_rules.pdf.

the UCTD,[32] and the CRD before publishing the guidelines.[33] Commission guidelines on consumer law, such as guidance issued on the UCPD and CRD should be cross-referenced, as they provide highly relevant sections on social-media and influencer marketing. As the European Data Protection Board (EDPB) is currently working towards developing guidelines on children's data[34] it is important to cross-reference this work and build on the input and guidance provided when drafting the Article 28(1) guidelines.

Finally, cooperation and exchange of information should be encouraged when handling cases of suspected infringements of children's online protection rules, to ensure that complaints falling between the gaps of different legal frameworks are duly handled by the relevant authorities. This is essential to ensure that complaints are handled effectively and promptly and take account of the fact that children are faced with the impact of such practices at a crucial time in their development.

BEUC Recommendations:

- Ensure that compliance with Article 28(1) is assessed in conjunction with compliance with the rest of the DSA provisions and other EU laws including the GDPR, the UCPD, the CRD, the AVMSD and applicable legislation on product and toy safety.
- Encourage the Commission to integrate the views and cross-reference any other regulatory document from regulators in charge of supervising and enforcing other related legislation.
- The Commission guidelines must encourage structured dialogue and cooperation between different enforcement authorities and networks supervising legislation relevant to the topic to ensure comprehensive and deterrent enforcement of applicable laws. This is important to ensure compliance, help platforms to comply in a consistent manner and enhance small players' competitiveness.

4. Safe, private and secure by default – how to make online platforms safer

The best interests of the child[35] should be the guiding principle in designing an age-appropriate online sphere that respects their rights. This means that the children's interests should always prevail over commercial interests. According to the United Nations Convention on the Rights of the Child,[36] these rights include children's right to privacy and freedom from economic exploitation, the highest attainable standard of health, the right to access information, the right to associate with others and to engage in play and recreational activities. All these rights should be reflected in the Article 28 guidelines, along with the principles of EU legislation on privacy, consumer protection and audio-visual media services as mentioned in the previous section.

[32] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
[33] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance.
[34] Available here, accessed 12/09/2024: https://www.edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf.
[35] EU Charter of Fundamental Rights, article 24(2).
[36] Available here, accessed 06/09/2024: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

4.1. Age verification is insufficient to make the internet safe

Upholding children's rights online is a multi-faceted issue requiring a thought-through approach. Any measures taken must be appropriate and proportionate to the risk in question, and be guided by the best interests of children, who are a diverse group with different needs. Bearing this in mind, it is essential to build an online sphere that is safe, secure and private by design and by default. If these measures are horizontally implemented, the need to apply specific protections online for minors, by first verifying their age, would be superfluous to a large extent.

These are important considerations to keep in mind while considering online age verification solutions to ensure minors' safety, security and privacy online. When drafting these guidelines, the Commission should be mindful of the fact that age verification mechanisms may lead to undesirable consequences with exclusionary and discriminatory effects,[37] while at the same time, there is evidence showing that imposing restrictions on a certain age group does not necessarily ensure better protection.

This was demonstrated by BEUC's in-house research on TikTok 2021, leading to an external alert under the Consumer Protection Cooperation Network Regulation. Research showed that at the time the complaint was launched, TikTok's algorithms exposed children and teenagers to potentially illegal content, which was not in line with TikTok's own Community Guidelines while also infringing the UCPD and AVMSD.[38] Amnesty International has also conducted research showing that accounts set up as minors' accounts on TikTok are exposed to potentially harmful content on the platform,[39] demonstrating clearly that age-gating is no panacea to the problems minors encounter on online platforms.

Regardless of whether one is above or below the age limit, age restrictions alone do not adequately protect children from abusive and manipulative practices online. Children deserve a digital environment that respects their rights and empowers them. They need stronger protection when accessing online platforms to achieve this, while additional measures are needed to meet their, and their guardians', expectations. Therefore, age-verification should be considered to be merely a tool in the toolbox rather than a silver bullet to address the risks children face online. Prioritising age verification as a solution should not come at the expense of making the internet safe, secure and private by design and by default.

To reflect these points, the guidelines must underscore that the deployment of age verification as a measure should be proportionate to the risks and appropriate to achieve the goal intended, as would be the case when attempting to, for example, access gambling platforms and online marketplaces selling alcohol. At the same time, if applied, age verification solutions need to guarantee consumers' anonymity, personal data protection and security, confidentiality and privacy, by being cybersecure, untraceable, using 'zero-knowledge proof' and not giving out any information about the user except for whether they are above the age threshold or not.[40] In that sense, age verification tools based on profiling or using biometric data are by default not a suitable solution.

[37] Available here, accessed 12/09/2024:https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf.
[38] Available here, accessed 12/09/2024: https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-012_tiktok_without_filters.pdf.
[39] Available here, accessed 12/09/2024: https://www.amnesty.org/en/documents/POL40/7350/2023/en/.
[40] Available here, accessed 12/09/2024:https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf.

In addition, compliance with Article 28(1) of the DSA must be ensured in full compliance with recital 71 of the DSA, the GDPR and the ePrivacy Directive[41] , including the principles of data protection by design and by default, purpose limitation and data minimisation. This is important to ensure that the potential use of age verification tools does not pose additional data protection and security risks. Obligations imposed on gatekeepers by the Digital Markets Act (DMA), such as the prohibition to cross-use personal data between services, including for advertising, without consent[42] must also be respected. Unless these criteria are satisfied, any age verification tools could be considered privacy-invasive and abusive to minors' privacy and therefore not respect Article 28(1) of the DSA.

BEUC Recommendations:

- The design, features and functionalities of online platforms must be safe, private and secure by default. Age verification is no panacea and should not replace age-appropriate design and features.

4.2. The importance of defaults and compliance by design

Default settings are inextricably linked to consumer protection and consumer choice. Research on default settings conducted with regard to the DMA clearly shows that consumers tend to stick to their default settings.[43] BEUC research on effective choice screen design also shows that choice screens are a valuable tool to promote consumer choice and the contestability and fairness objectives of the DMA.[44] These observations are clearly applicable to frameworks beyond the DMA and underline the importance of default settings.

At the same time BEUC's work on digital fairness has highlighted that default settings and the design of digital consumer environments and choices are two of the factors that make consumers vulnerable online.[45] This translates into consumers' susceptibility to the exploitation of differences in power in the trader-consumer relationship. This condition is aggravated by individualised and other behavioural techniques for influencing consumer behaviour. As children expect and require greater protection online, the concept of digital vulnerability underlines the role that default settings play in protecting children's rights online.

Default settings have a heightened importance concerning children's experience online, as deceptive practices requiring a series of steps or circumvention tactics nudging users to change their defaults, make it increasingly hard to exercise control over one's feed. For these reasons, the guidelines must stress the importance of default settings to better protect children online.

Children's accounts must be private by default - geolocation and other tracking features must be off by default

In line with the GDPR and other applicable law, to ensure that children's online experience is private, and their personal data is respected, minors' accounts should be set up to be

[41] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[42] DMA, Article 5(2).
[43] Available here, accessed 25/09/2024: https://techcrunch.com/2021/12/14/europes-final-push-on-the-digital-markets-act-must-include-default-settings/.
[44] Available here, accessed 25/09/2024: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-131_An_effective_choice_screen_under_the_DMA.pdf.
[45] Available here, accessed 12/09/2024:https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf.

private by default while any existing tracking features, such as third-party cookies, tracking pixels and geolocation should be turned off by default. The same goes for features like access to microphones and cameras, which if used should be turned off after each session. Options to chat and call with other accounts should be limited to known contacts to avoid unwanted and potentially dangerous exchanges. Online platforms must be required to demonstrate their design is compliant with these prerequisites.

BEUC Recommendations

- By default, minors' accounts should be private and not accessible to the public.
- Any features tracking minor's accounts should be turned off by default.

Children's right to be forgotten must be easy to exercise

To ensure a high level of privacy, it is important that children's digital footprint and presence on online platforms can be easily erased, in line with the GDPR's 'right to be forgotten'.[46] Moreover, the content of minors should not be indexed by search engines without the authorisation of the parent or guardian of the child. Furthermore, it should not be possible for third parties to capture or share such images or content. This is particularly important given that digital content may outlive the purpose and circumstances under which it was created and be used for different purposes to the detriment of the user, for example as part of a hiring process when screening candidates.

BEUC Recommendations:

- It must be easy for children to erase their digital footprint and content.

Engagement-driven recommender systems profiling children must be turned off by default.

In an online world where profit is driven by engagement, users of online platforms fall victim to manipulative deceptive features and practices and children are no exception. To generate profit, dominant platforms drive user engagement by deploying content recommender systems that keep children scrolling and clicking for as long as possible. Instead of prioritising relevant or high-quality content, these algorithms give a higher rank to content that will keep engagement high, such as emotive and extreme content. [47] Although content moderation is not a primary focus of this paper, it is worth noting how potentially harmful content is intertwined with engagement-based recommender systems, which entail addictive design features. In this regard, it is important that online platforms take a holistic approach to content moderation and recommender systems to meet their obligations under Article 28(1) of the DSA. This holistic approach should both incorporate transparent and accountable use of digital and human support elements, in order to handle the growing quantity of content and products on platforms in a responsible manner. To further support a safe online experience for minors, the guidelines should recommend there should be a sufficient number of moderators that can effectively support consumers from a specific country and region.

[46] GDPR, Article 17.
[47] Panoptykon Foundation & People vs Bigtech, Safety-by-default, available here, last accessed 06/09/2024: https://panoptykon.org/sites/default/files/2024-03/panoptykon_peoplevsbigtech_safe-by-default_briefing_03032024.pdf.

While the DSA requires platforms to provide alternative recommender system solutions that are not based on profiling,[48] this should be the default for all, as the choice architecture chosen by some providers may render this provision ineffective. This is also what the Italian Competition Authority argued in their decision against TikTok on the basis of the UCPD.[49] This becomes particularly important for minors' accounts, but the issue is not only limited to children.[50] Algorithms should prioritise quality and content relevance, following explicit user input signals and feedback,[51] that are children-friendly and easy to use. To ensure the maximum effectiveness of this measure it is important that children are not nudged to change their settings by deceptive features, as covered by the DSA[52], the UCPD, other relevant laws such as the DMA and the GDPR. It should be clear that switching to surveillance-based recommender systems is subject to their consent as per the GDPR,[53] and not based on the company's legitimate interest if the children are not in the legal age to provide their consent. Surveys indicate that consumers do not feel in full control of the online content they are shown and the decisions they make online,[54] and children share the same sentiment and feel exposed in the digital sphere.[55] Therefore, they should be protected by design and by default.

The impact that engagement-based algorithms have on children can lead to the so-called 'rabbit-hole' effect, which in turn can aggravate existing mental health issues, such as anxiety. Excessive engagement with online platforms taps into children's emotions such as social belonging and the fear of missing out, initiating a vicious cycle where children may end up feeling left out and stressed, leading back to excessive online platform engagement.[56] The emerging trend of 'digital minimalism' and its rising popularity amongst Generation Z points a finger at the need to limit the use of tech and screen time for mental health reasons.[57] These emotions are not only triggered by exposure to harmful content online but feed off children's need for validation and social inclusion. In our assessment, this demonstrates that attention-seeking recommender systems can have negative effects on children.

Finally, these algorithms feed off users' behavioural data to provide each one of them with tailored and hyper-personalised content. Such practices are fundamentally incompatible with the GDPR principles such as fair processing, transparency or data minimisation[58], and violate children's right to privacy and informational self-determination.

[48] DSA, Article 27(3).
[49] Italian Competition Authority: TikTok sanctioned for an unfair commercial practice, available here, accessed 04/09/2024: https://en.agcm.it/en/media/press-releases/2024/3/PS12543.
[50] Irish Council of Civil Liberties, Joint submission on the draft Online Safety Code, available here, accessed 25/09/2024:https://www.iccl.ie/wp-content/uploads/2024/01/submission-60-civil-society-organisations-Coimisiun-na-Mean_OSC-Consultation-Response.pdf.
[51] Panoptykon Foundation & People vs Bigtech, Safety-by-default, available here, last accessed 06/09/2024: https://panoptykon.org/sites/default/files/2024-03/panoptykon_peoplevsbigtech_safe-by-default_briefing_03032024.pdf.
[52] DSA, Article 25.
[53] GDPR, article 4(11).
[54] Available here, accessed 06/09/2024: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-113_Fairness_of_the_digital_environment_survey_results.pdf.
[55] https://www.amnesty.org/en/documents/POL40/7349/2023/en/; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN.
[56] Giulia Fioravanti et al, Fear of missing out and social networking sites use and abuse: A meta-analysis, Computers in Human Behavior, Volume 122, September 2021, 106839, available here, last accessed 06/09/2024: https://www.sciencedirect.com/science/article/abs/pii/S074756322100162X.
[57] https://www.techworm.net/2024/08/gen-z-digital-minimalism-cut-screen-time-mental-health.html.
[58] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), article 5(1)(b)-(c).

BEUC Recommendations:

- Engagement and interaction-based algorithmic recommender systems should be off by default in accounts set up by minors. Instead, online platforms should prioritise quality, children's feedback and explicit signals when ranking content.

Online platforms should not incorporate addictive design features.

The ongoing debate regarding the impact of addictive design features on the mental health of minors has gained considerable traction, leading the President of the European Commission to announce an EU-wide inquiry into the broader impact of social media on well-being.[59] While evidence remains inconclusive, recent studies show small but significant associations and suggestions that higher levels of screen media use might be associated with more behavioural problems.[60] Also the European Parliament has made significant progress in this regard mentioning in its resolution on the addictive design of online services and consumer protection in the EU single market[61] the growing consensus among academics that phenomena such as social media addiction exist, and the impact that platforms' design to keep users hooked can have on children and us all, demanding additional legislative measures. While the DSA cannot tackle all relevant aspects due to its limited scope to some providers and as it is a horizontal piece of legislation, we recommend the guidelines nevertheless address the issue of addictive design to ensure compliance with Article 28 of the DSA.

To ensure the highest level of security, privacy and safety for children online the Commission should pay due consideration to the abovementioned facts and suggest sufficient measures for online platforms to tackle addictive design. Attention-seeking features, such as the default autoplay of videos, default 'infinite scrolling', 'push notifications', 'streaks', 'pull-to-refresh' page reload, '...is typing', 'read-receipt notifications', 'like and dislike' and other functionalities having a similar effect should be turned off by default in order to provide a high level of safety. Such elements, if embedded in the design of the platform, should be a clear indication that the online platform's design does not ensure a high level of safety and is infringing the DSA. These elements should be reflected in the Commission guidelines on compliance with Article 28 of the DSA, leading to actionable steps by online platforms. Safe online platform services should add friction elements to content experiences (e.g. it would be good to test whether indicating time limits for watching content or surfing for products when opening the platform could have positive impacts against minors' addiction, without such measures leading to further tracking users or using that information for other purposes.

BEUC Recommendations:

- The guidelines must provide an open list of measures for online platforms to tackle addictive design. Features such as the default autoplay of videos, default 'infinite scrolling', 'push notifications', 'streaks', 'pull-to-refresh' page reload, the '...is typing'

[59] Political Guidelines for 2024-2029, Ursula von der Leyen, Candidate for the European Commission President, available here, accessed 04/09/2024: https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf.

[60] Rachel Eirich Brae Anne McArthur, Ciana Anhorn, et al, Association of Screen Time With Internalizing and Externalizing Behavior Problems in Children 12 Years or Younger: A Systematic Review and Meta-analysis, *JAMA Psychiatry.* 2022;79(5):393-405, available here, accessed 06/09/2024: https://jamanetwork.com/journals/jamapsychiatry/fullarticle/2790338.

[61] IMCO 2023/2043 (INI) Report on addictive design of online services and consumer protection in the EU single market, available here, accessed on 04/09/2024: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_EN.html.

functionality, 'read-receipt notifications', and popularity metrics such as 'likes and dislikes should be indicators of addictive design.

Commercial communication and advertising

While the DSA prohibits advertising targeted at children based on profiling,[62] this provision will only be effective if it is enforced in practice. For example, if there is no proof as to whether minors' data collected is also deleted, it could be later used to target users with surveillance-based advertising once they become of age, despite being illegal.

As regards commercial practices and advertising, there are alternative ways of targeting children with commercial content besides traditional forms of advertising. This is particularly evident in the case of influencers whose content is indirectly promoting or placing products or services. The problem is highlighted in a recent study from the Danish Competition and Consumer Authority showing that 38% of children between 6-12 do not recognise commercial influencer content as constituting advertising.[63] The line between 'content' and 'advertising' is getting increasingly blurry[64], not only because of content mis-labelling but also due to the increasing popularity of 'challenges' that gamify advertising to further engage users, as has been the case with the promotion of unhealthy food to children.[65] Although this goes beyond the scope of the DSA provisions these are some of the reasons why BEUC is advocating an online ban on the marketing of unhealthy food products, including on food company websites and social media accounts.[66]

The risks that such practices pose for children have been stressed in BEUC's position paper on influencer marketing,[67] which calls for an update to Annex I of the Unfair Commercial Practices Directive (UCPD),[68] and the prohibition of several practices to protect consumers in risky sectors or that exploit children's vulnerabilities. The establishment of harmonised displays and standards for advertising across online platforms is also linked to Articles 26 and 44 of the DSA, requiring digital platforms to provide their users (influencers/content creators) with functionalities to declare whether the content they provide constitutes or contains commercial communication. This is essential to ensure that children can identify in a 'clear and unambiguous manner and in real time, including through prominent markings', whether the content they are viewing constitutes advertising or not.[69]

At the same time, children appear to fall victims of 'implicit' targeting. A recent Financial Times story revealed that Meta and Google concluded a secret ads deal to indirectly target teenagers as part of a 'wider and unknown' audience in the United States.[70] As such evidence surfaces and considering these companies operate globally, the Commission should use this opportunity to state that this type of practice would not ensure the high level of protection required under Article 28 of the DSA.

---

[62] DSA, Article 28(2).
[63] Available here, last accessed 06/09/2024: https://en.kfst.dk/media/z3lmycgw/20210617-consumers-benefit-from-visually-salient-standardized-commercial-disclosures-on-social-media.pdf.
[64] Available here, last accessed 06/09/2024:https://www.theverge.com/2015/11/20/9768350/google-ads-search-results-ofcom.
[65] Available here, accessed 12/09/2024: https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-084_food_marketing_to_children_needs_rules_with_teeth.pdf.
[66] Ibid.
[67] Available here, last accessed 06/09/2024: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-093_From_influence_to_responsibility_Time_to_regulate_influencer-marketing.pdf.
[68] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance).
[69] Available here, accessed 12/09/2024: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-093_From_influence_to_responsibility_Time_to_regulate_influencer-marketing.pdf.
[70] Available here, accessed 12/09/2024: https://www.ft.com/content/b3bb80f4-4e01-4ce6-8358-f4f8638790f8.

As stressed in previous sections, the regulation of advertising and commercial communications is a cross-cutting topic touched upon by a multitude of EU legislation. This includes laws specific to consumer and personal data protection, as well as online platform regulation. To ensure their applicability and proper enforcement, these rules should be strictly interpreted. These guidelines are an opportunity for the Commission to clarify these interlinks and to provide online platforms with an interpretation that does not leave any room for circumvention. In the light of the recent story on Meta and Google's secret ads deal to indirectly target teenagers as part of a 'wider and unknown' audience,[71] it is paramount that the Commission remains vigilant and shows zero tolerance to such phenomena in Europe.

BEUC Recommendations:

- The Commission must provide a strict interpretation regarding advertising and other commercial communications towards children. This is particularly relevant vis-à-vis Article 28(2) of the DSA prohibiting targeted advertising to children.
- Children's data should not be used for online platforms' commercial purposes.

Codes of Conduct

Recital 71 of the DSA mentions that providers of online platforms may participate in relevant codes of conduct, as one of the measures they can take to protect minors. While adherence to appropriate codes of conduct can contribute to compliance with measures necessary, it cannot be considered as a presumption of compliance. Online platforms need to have regular review mechanisms in place and be able to demonstrate their compliance at any given time.

BEUC Recommendations:

- The guidelines should clarify that participation in codes of conduct should not lead to a presumption of compliance with the provisions of Article 28(1) DSA.

5. Conclusion

The guidelines the European Commission is drafting to assist online platform providers to comply with the requirements of Article 28(1) of the DSA present a unique opportunity for the Commission to address many of the risks and harms that children are confronted with when accessing the internet. To ensure that online platforms are held to a standard that ensures the privacy, safety and security of minors online, these guidelines must clarify what constitutes both good practices and examples of practices that may be considered unlawful. The guidelines will also contribute to consistent and coherent implementation of the obligations laid down by Article 28(1) of the DSA across the EU by all concerned regulatory authorities.

Age verification tools by themselves are not sufficient to address a multi-faceted issue and must always be complemented with additional measures that provide a safe, secure and private experience online. Against that backdrop, the guidelines must prescribe that the required level of privacy, security and safety for children can primarily be achieved by online platforms implementing default settings and designs that ensure compliance with these requirements. Tracking features and engagement-based recommender systems that

[71] Available here, accessed 12/09/2024: https://www.ft.com/content/b3bb80f4-4e01-4ce6-8358-f4f8638790f8.

trap children's attention should be off by default, along with addictive design features and functionalities. Insofar as commercial practices and advertising are concerned, the guidelines must give clear examples and guidance of practices that infringe Article 28(1) of the DSA, with due consideration given to the interplay of this provision with the rest of the DSA as well as other relevant EU laws, including the GDPR, the ePrivacy Directive, the UCPD, the CRD, the AVMSD and EU product and toy safety legislation. Finally, to ensure the guidelines are not considered in a vacuum, the Commission must encourage the structured cooperation of different enforcement authorities and networks responsible for monitoring legislation that covers relevant associated requirements.

- END -

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.