The Consumer Voice in Europe

# BETTER SAFE THAN SORRY

## BEUC position paper on how to keep children safe online in the EU

**Contact:** **Mykyta Sobko and 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-2025-014 – 17/02/2025

## Why it matters to consumers

In the EU, 97% of young people[1] use the internet daily, primarily for social networking, yet they are insufficiently safe online.[2] While the internet serves as a platform for socialising, community-building and self-expression, children are highly vulnerable to privacy-invasive, addictive and manipulative designs which are usually driven by commercial practices. With growing evidence of the detrimental effects on children's mental health and development, it is primordial for the EU to vigorously enforce its digital rulebook and tackle pending issues to protect children and adults alike in the digital sphere to create a safe environment by design and by default.

## BEUC key recommendations to better protect minors online

1. **Establish safe by default and by design settings:** ensure all traders automatically set minors' accounts to private, turn off engagement-based recommender systems by default, disable tracking mechanisms (e.g. non-essential cookies, pixels, and location techniques), restrict the possibility for payments and sensitive features like microphones and cameras after each session.

2. **Tackle the harms stemming from surveillance advertising:** introduce a horizontal prohibition on advertising to minors that is based on tracking across all sectors and traders, building on Article 28 of the Digital Services Act, which currently applies only to online platforms.

3. **Address addictive and manipulative design**: prohibit online features that exploit children's vulnerabilities for commercial profit, such as amplification of toxic content, infinite scrolling and autoplay, across all traders. The upcoming Digital Fairness Act (DFA) should include an open list of banned practices, focusing on preventing digital addiction and promoting safe user engagement.

4. **Fill gaps in the regulation of influencer marketing, harmful advertising and other commercial communication:** introduce EU-wide rules for influencer marketing, including mandatory disclosure of commercial content and bans on promoting harmful and unsuitable products and services to children. Guarantee these measures extend to all advertising and marketing activities children are exposed to, instead of those explicitly targeted at them. Businesses must find operational solutions that effectively protect children online.

5. **Enforce existing legislation to ensure that it truly delivers for consumers on the ground and triggers compliance by companies:** ensure effective enforcement of EU laws, such as the Unfair Commercial Practices Directive (UCPD), the DSA, the General Data Protection Regulation (GDPR), the ePrivacy Directive and the AI Act, to safeguard children's online privacy and safety. When enforcing the rules, authorities should carefully consider the vulnerabilities and specificities of children and cooperate with each other to ensure effective, deterrent and rights-protective enforcement.

[1] European Commission, EU Strategy for the rights of the child, 2021.
[2] Eurostat, Young-people – digital world, 2014-2023.

# Table of Contents

## 1. Introduction – protecting children online starts with protecting us all

As societies become increasingly digitalised, children[3] are deeply immersed in online environments that shape their development and behaviours from an early age, normalising both the advantages and drawbacks of internet use. With **85% of those under 23 using social media for up to seven hours daily**,[4] it is clear that the digital sphere plays a significant role in their lives.

While **79% of EU citizens consider digital technologies as vital for the future**, **only 50% believe digital rights are well protected**, and even **fewer find the digital space safe for kids**.[5]

This position paper underscores the importance of upholding children's rights in the digital world by advocating for safer, rights-preserving online spaces.

Despite existing EU laws addressing some of these issues, gaps remain. Consumers expect better: **three out of four want the EU to do more while less than one in ten (8%) feel that enough is being done to protect children.**[6]

In this paper, we focus on key areas affecting children's online protection, such as addressing dark patterns, combating digital addiction, enhancing privacy protections, and regulating gaming, influencer marketing and surveillance advertising. This paper also highlights the importance of robust enforcement mechanisms and draws attention to the risks linked to age assurance methods.

The safer the whole online ecosystem is, the better it will be for children and all consumers. Internet safety and digital fairness need to benefit everyone. We would need fewer tailored protections if we had a safer online ecosystem and that is why it is important future legislation, notably the upcoming Digital Fairness Act, protects us all.[7] For the purposes of this paper, we would like to refer to particular points that refer to child protection.

## 2. Towards a safer and rights-protective internet for kids

It is commonly acknowledged that children are confronted with several risks and challenges when online. **Children, among the most vulnerable and impressionable groups in society, spend a significant amount of time online, making them particularly susceptible to harms and external influences. These include addiction, exposure to harmful content, exploitative practices and advertisements that negatively impact their health, as well as their parents' wallets.** All of these issues extend across different online services including video games, messaging apps, social media, web streaming platforms or retail business-to-client (B2C) shops.

Protecting children online is an important responsibility of parents, educators, teachers and caregivers. But **companies have a significant role to play too.** In a state of digital asymmetry and vulnerability,[8] purported solutions such as parental control tools are often ineffective and can be easily circumvented by children. Furthermore, parents themselves can be manipulated by digital services in similar ways, making it difficult for them to effectively monitor and manage their children's online activities.

[3] 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.
[4] Henna Maria Virkunnen, Commissioner-designate hearing at the European Parliament verbatim report, 12/11/2024.
[5] Eurobarometer, The digital decade, June 2023.
[6] BEUC, Consumer survey results on the fairness of the online environment, 20/09/2023.
[7] BEUC, Towards European Digital Fairness, 20/02/2023.
[8] *Ibid*.

Many online harms children experience stem from an underlying business model designed to maximise user engagement and data collection. Tracking and profiling children are economically very valuable activities, since they allow consumer relationships to be built from a very early age. The collected data is used to track and profile users to offer them targeted advertising and content recommendations, which can be more invasive than other forms of advertising and other commercial communications.

Such practices have led to widespread dissatisfaction among consumers across the EU.

**70% of consumers are worried about how their personal data is used and shared.[9]**
**37% of consumers feel that companies are aware of their vulnerabilities and exploit them for commercial gain.[10]**

Trade-offs between commercial interests and children's safety, privacy and security must be avoided. **Online service providers should pursue their commercial interests only to the extent that their practices align with the law protecting children's online rights and interests, as a Dutch court recently ruled.**[11] The best way to make this happen is to create an internet that is safe and rights-protective for everyone, so kids are better protected and there is less need for tailored approaches. In reality, however, this is far from the case.

### 2.1. Safe by default and by design: a rights-preserving digital space

Evidence has uncovered that many harmful industry practices affecting children in the digital world are not accidental but deliberate choices guided by business decisions. This includes default settings that are often designed in ways that do not serve the best interests of children. Research consistently shows that consumers tend to stick with pre-configured options. This highlights the critical role of default settings in protecting children and promoting fairness and choice.[12]

**Currently, the strategic design of digital consumer environments and default settings deepens the imbalance between consumers and businesses, and makes consumers digitally vulnerable.** This issue becomes even more urgent when it comes to children, who are often introduced to digital services through default settings that they have no role in selecting.

**Current consumer protection laws, with the exception of the Unfair Commercial Practices Directive (UCPD), lack child-specific provisions to properly address these shortcomings.**

While the UCPD recognises children as vulnerable consumers and prohibits direct exhortations to children to purchase products, more comprehensive safeguards are needed to create a more rights-preserving digital space, as suggested by the Commission.[13] For example, in the case of video games, this could include setting default spending limits for child accounts and disabling in-game purchases by default. More broadly, online platforms could enhance protections by automatically setting minors' accounts to private.

[9] European Commission, Questions and Answers on the Digital Fairness Fitness Check, 03/10/2024.
[10] *Ibid*.
[11] This was upheld by the Amsterdam District Court in a recent decision against TikTok, where TikTok was found responsible for violating the privacy of more than 1.5 million Dutch children on a large scale. See Consumentenbond, *Stichting Take Back Your Privacy in hoger beroep in TikTok-zaak*, 18/10/2023.
[12] BEUC, An effective choice screen under the Digital Markets Act, 19/10/2024.
[13] European Commission, Commission Staff Working Document 'Fitness Check of EU consumer law on digital fairness', 03/10/2024.

### Game Over Action - Consumers fight for fairer in-game purchases

In September 2024, BEUC and 22 of its member organisations from 17 countries filed a complaint[14] to the European Commission and the network of consumer protection Authorities (CPC-Network) to denounce several deceptive practices by leading video game companies[15] marketing popular games and affecting millions of European consumers, including children.

Among our findings, we highlighted the lack of professional diligence by traders to better protect children and teenagers from unwanted and unfair in-game purchases as all in-game purchases are "on" by default.

Unfortunately, there are numerous examples of massive in-game and in-app spending. They show the limits of existing voluntary safeguards and the need for stricter rules in the Digital Fairness Act to ensure that consumers, and even more so, children who are playing video games widely, are protected by default and by design.

Concretely, EU consumer law[16] should require the deactivation of in-game payment mechanisms "by default". Consumers should have a choice to activate in-game purchases ('opt-in'). The holder of the means of payment (cards or others) should receive a notification and be required to validate each in-game or in-app transaction. Finally, when installing the game or app, consumers should be obliged to define a 'password' to avoid unwanted transactions.

Default settings are critical in shaping consumers' and children's online experiences. Deceptive practices that involve multiple steps or subtle nudges to change default settings undermine individuals' ability to control their choices and exacerbate digital vulnerabilities. **Efforts that solely focus on restricting children's access to the internet**, without addressing the design and features of online services, **offer only a band-aid solution that incentivises children to go online without any safeguards in place.** A crucial step forward is implementing **safe by default and by design settings,** protecting the safety, privacy, and security of children.

### 2.2. Age assurance

Age assurance is an umbrella term for various methods used to determine a user's age, whether exact or approximate. **If not done well, these methods can raise concerns, including a potential 'chilling effect' on consumers' online activity, as they require all users to verify their age through various, yet often questionable, means.**[17]

For instance, document-based age verification methods, such as the EU Digital Identity Wallet, have raised concerns.[18] There is a **high risk of exclusion,**[19] not just for children but also for adults without access to digital identification. This is particularly worrisome, as even in highly digitised countries like Norway (an EEA member), approximately 7% of the population lack access to or do not use electronic ID.[20]

Tools that rely on profiling consumers' online activity are particularly concerning, as they can legitimise highly problematic commercial surveillance practices.[21] This, in turn, amplifies existing risks to privacy and leads to harmful economic, social, and personal consequences. Age estimation methods based on

[14] BEUC, Game Over, September 2024.
[15] Activision Blizzard, Electronic Arts, Epic Games, Mojang Studios, Roblox Corporation, Supercell and Ubisoft.
[16] BEUC, Monetising Play, 12/09/2024.
[17] EDRi, Online age verification and children's rights, 04/10/2023.
[18] Biometric Update, Cryptographers warn about EUDI wallet privacy, December 2024 [accessed on 12/02/2025.
[19] EDRi, Online age verification and children's rights, 04/10/2023.
[20] Norwegian Consumer Council, Commercial exploitation of children and adolescents online, November 2024.
[21] *Ibid.*

biometric data analysis are equally concerning. These methods are prone to error, with built-in margins of 2-4 years, and may reflect discriminatory biases present in the training datasets.[22] And again, they are fundamentally incompatible with the high standards of privacy and security required, given the particularly sensitive nature of biometric data.

Age assessment methods also raise concerns related to cybersecurity, the risk of data breaches[23] and the ease of circumvention. These factors highlight that **age assurance solutions alone will not improve child protection or create a safer online space**. Without safety-by-default-and-by-design measures, age assessment systems risk exposing children to unsafe online environments and even excluding adults.[24]

The reality, however, is that **deploying age assurance tools is unavoidable and needed in certain cases**. Therefore, it is crucial that their use is proportionate to the associated risks and appropriate to achieve the intended goal, such as restricting access to gambling platforms or online marketplaces that sell alcohol.

### 2.3. Limited choice screens due to age restrictions: the Apple case

In the pursuit of stronger child protection, some companies have claimed to **introduce measures to protect children, but this has, in some cases, led companies to infringe on their legal obligations**, as seen for example with Apple under the Digital Markets Act (DMA).

Apple's proposed browser choice screen, designed to comply with Article 6(3) DMA, does not work in version iOS 18.2 if parental controls are enabled.[25] By rating all third-party browsers as "17+" on its App Store, Apple effectively prevents users from downloading alternative browsers. This practice locks users into using Safari, the pre-installed browser, and keeps them within the Apple ecosystem. Apple is not the only company claiming it cannot comply with DMA obligations due to challenges in verifying whether other email providers offer parental supervision options. However, this approach prioritises the company's own interests over implementing effective solutions that protect children while preserving consumer choice.

## BEUC RECOMMENDATIONS

**1** Establish safe by default and by design settings and ensure online platforms automatically set minors' accounts to private by default.

**Age verification methods alone are not sufficient to tackle the harms children are facing online. If implemented, they must *always* be effective and accompanied by age-appropriate design measures**, as detailed below:

**2**

- Age verification must be proportionate, risk-based, and necessary to address specific harms. Any disproportionate application risks excluding both children and adults from accessing the internet.
- Verification mechanisms must comply with the GDPR and provide only a simple yes or no answer regarding age eligibility.

[22] EDRi, Online age verification and children's rights, 04/10/2023.
[23] TrustCloud, The AU10TIX case: millions of records exposed in a security breach affecting major apps, 10/07/2024 [accessed on 12/02/2025].
[24] For example, adults not having access to an electronic ID solution when mandated may be excluded. See more at Norwegian Consumer Council, Commercial exploitation of children and adolescents online, November 2024.
[25] Open Web Advocacy, 'iOS age restriction blocks all browsers except Safari, breaks choice screen', 15/11/2024 [accessed on 12/02/2025].

- Tools must be state-of-the-art,[26] cybersecure, untraceable, utilise 'zero-knowledge proof', *i.e.* revealing only whether a user meets the age threshold without disclosing additional information.

- Given the significant privacy and security risks they pose, **methods based on profiling or biometric data are inherently unsuitable.**[27]

**3** Regulators should be vigilant to **ensure that companies do not circumvent their obligations in other areas when purportedly implementing measures to protect children online**.

## 3. How to tackle the harms that children face online

### 3.1. Digital addiction

**Digital addiction is a major concern, particularly for children, as it impacts their mental and physical well-being.** It refers to the excessive use of digital products and services, driven by design features that encourage prolonged engagement for commercial profit. These features include autoplay videos, infinite scrolling, push notifications, and tools like 'likes,' 'streaks,'[28] and ephemeral content like live streams and stories.[29] Given the broad spectrum of addictive designs and features in online services, their impact on consumers can vary in nature and severity, but the effects are consistently harmful.

**83% of consumers** reported spending more time on social media than they initially intended.[30]

The European Commission's Digital Fairness Fitness Check report[31] has concluded **addictive design can lead to time loss, attention capture, mental harms like anxiety and depression,[32] obsessive-compulsive behaviours such as compulsive buying, and physical harms including sleep deprivation, sedentary behaviour and potential early neurodegeneration**.

A recent European Parliament resolution also concluded that minors are particularly susceptible to those harms[33]. At the same time, evidence also suggests that the moods of young people are directly affected by social media 'likes'. According to the European Commission's 2023 Communication on Mental Health,[34] the mental well-being of younger generations is deteriorating, with suicide being the leading cause of death among young people (15-19 years old)[35] after road accidents. The Communication calls for a comprehensive approach to mental health across policies that acknowledges the role of commercial factors, such as pressure from aggressive marketing, as determinants of health.

[26] BEUC, Towards a safer, more private and secure internet for children in online platforms, 30/09/2024.
[27] *Ibid.*
[28] A streak refers to a continuous series of interactions or exchanges between individuals, maintained by engaging with one another at least once daily over consecutive days
[29] BEUC, Towards a safer, more private and secure internet for children in online platforms, 30/09/2024.
[30] BEUC, Connected but unfairly treated, September 2023.
[31] European Commission, Commission Staff Working Document 'Fitness Check of EU consumer law on digital fairness', 03/10/2024.
[32] Notably, this is due to the promotion of unhealthy and unrealistic body images and/or behaviours that can harm health in the short, medium, and long term.
[33] European Parliament, Addictive design of online services and consumer protection in the EU single market, 12/12/2023.
[34] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economics and Social Committee and the Committee of the Regions on a comprehensive approach to mental health, 07.06.2023.
[35] European Commission, Commission Staff Working Document 'Fitness Check of EU consumer law on digital fairness', 03/10/2024.

In the EU, the annual value of lost mental health in children and young people is estimated at 50 billion euros.[36]

Addictive design has severe consequences, not only on children's physical and mental health, but also on the EU economy, highlighting the need for a strong prohibition of tools, functionalities and features that contribute to such effects. This issue should be addressed in the upcoming Digital Fairness Act (DFA), which could complement the general principle of fairness by design. It could include an open list of prohibited practices that can be updated to stay relevant in the future covering all traders. **The DFA presents a pivotal opportunity for the EU to tackle digital addiction by providing a clear definition and identifying features that fall under this scope**. Prescriptive rules are essential, as they minimise ambiguity, ensuring compliance by default and promoting effective enforcement of violations.

The Commission must also focus on enforcing existing legislation, such as the due diligence obligations of the DSA for Very Large Online Platforms (VLOPs) and Services (VLOSEs), to address addictive design and protect children's mental health. **Through guidelines, information requests, and proceedings, the Commission should ensure platforms mitigate risks to minors from their services' design and functionality.** Effective enforcement, as seen in the removal of the TikTok Lite Rewards Program[37], benefits both adults and children. The Commission's ongoing investigation into TEMU's potential DSA violations,[38] including addictive design,[39] is a positive step forward in the right direction.

### 3.1.1. Recommender Systems and Amplification of Toxic Content – the TikTok case

Addictive design manifests itself in algorithmic recommender systems that prioritise emotive and extreme content to maximise user engagement. For instance, evidence uncovered **that TikTok exploits profiling to push users into harmful "rabbit holes" of toxic content.** While the same concerns exist for other platforms,[40] internal documents from TikTok reveal that the platform knowingly exposes users to harmful filter bubbles, such as "SadTok" or "PainHub," which promote self-harm, eating disorders and other mental health harms. This is particularly worrisome, as the platform's primary audience consists of children (even under the age of 13) and teenagers,[41] who are particularly vulnerable to such content.[42]

Some trends are outrightly dangerous to children's health, such as the paracetamol challenge. Several authorities, particularly the Belgian Poison Control Centre, have issued warnings about the risk of paracetamol overdose among teenagers, parents, schools and caregivers.[43] The tragic case of British teenager Molly Russell,[44] whose suicide was linked by a coroner to exposure to harmful online content, underscores the devastating real-world consequences of such design practice. This is particularly worrying in the context of Big Tech phasing out third-party fact-checking programs,[45] as the US undergoes a leadership transition.

**Despite community guidelines prohibiting harmful content, TikTok's content moderation frequently fails to remove it completely, leaving such content accessible, although less visible.[46]** Research indicates that the platform's hyper-personalised algorithms not only amplify harmful content but also worsen users' mental health. For example, employees testing TikTok's algorithms reported adverse mood

[36] European Commission, Better Together: Co-creating the Future of Mental Health, 13/05/2024.
[37] European Commission, "The Commission strengthens consumer protection online with new guidelines on the Unfair Commercial Practices Directive," Press release, 17 July 2024.
[38] BEUC, Taming Temu, 2024.
[39] European Commission, Commission opens formal proceedings against Temu under the Digital Services Act, 31/10/2024.
[40] The Wall Street Journal, Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show, 14/09/2021 [accessed on 12/02/2025].
[41] BEUC, TikTok without filters, 2021.
[42] NPR, TikTok executives know about app's effect on teens, lawsuit documents allege, 11/10/2024 [accessed on 12/02/2025].
[43] The Brussels Times, TikTok paracetamol challenge triggers overdose warning in Belgium, 20/01/2025 [accessed on 12/02/2025].
[44] Judiciary of England and Wales, Prevention of Future Deaths Report: Molly Russell (2022-0315), 13/10/2022 [accessed on 12/02/2025].
[45] Politico, "Mark Zuckerberg goes full Elon Musk, dumps Facebook fact-checker," 02/01/2025 [accessed on 12/02/2025].
[46] NPR, TikTok executives know about app's effect on teens, lawsuit documents allege, 11/10/2024 [accessed on 12/02/2025].

changes and increased feelings of sadness after exposure to harmful material. Such practices clearly show that safety and mental health risks are being consciously overlooked to improve user engagement and to maximise profit at any price, as rightly affirmed by the Italian Competition Regulator, which fined TikTok under the UCPD.[47]

These harmful effects are exacerbated by the platform's addictive design, which includes features that encourage dependency. **TikTok's primary audience spends excessive time on the platform, often at the expense of sleep, physical activity and real-life interactions.** Unredacted documents from a US lawsuit brought by several attorney generals found that "safeguards, like the screen time nudges, were meant to have limited effect on actual screen time, and indeed, appeared to have a "negligible impact."

**After 5–6 hours on the platform, nearly 1 in 2 videos were mental health-related and potentially harmful – approximately ten times the volume shown to accounts with no expressed interest in mental health.[48]**

**Mitigation tools deployed by TikTok, such as time limits or "break" videos, have had minimal impact, reducing average usage by just 1.5 minutes per day – from 108.5 to 107 minutes.[49]**

A Kentucky lawsuit filed the following statement: "TikTok measured the success of the tool, however, not by whether it actually reduced the time teens spent on the platform to address this harm, but by three unrelated 'success metrics,' the first of which was 'improving public trust in the TikTok platform via media coverage'".[50] Moreover, internal company research showed that "the younger the user, the better the performance".[51]

Given the significant role of default settings and the influence of recommender systems on digital addiction and excessive screen time, the EU must adopt changes[52] that require engagement-based recommender systems to be turned off by default.[53] Instead, **algorithms should prioritise content quality and relevance, promoting consumer choice over commercial interests**. This, for example, can be achieved by giving children and their parents more control over the content that algorithms show them by providing their preferences.[54] **Empowering children, with meaningful and effective control over their online experience represents a crucial step toward creating a safer, more rights-preserving digital environment.**

### 3.2. Personal data protection and privacy issues

Consumers have long faced unfair and unlawful processing of personal data, which is then used for surveillance advertising.[55] **Minors, who predominantly use social media,[56] are particularly vulnerable to such privacy abuses, including profiling**. For example, Meta, which has targeted younger users, described children aged 8-12 as a "valuable but untapped audience," according to internal documents from 2021. WhatsApp invalidly claimed a legitimate interest in processing the personal data of minors, such as their whereabouts.[57] Moreover, the Hungarian Data Protection Authority recently fined a controller for unlawfully processing large amounts of minors' personal data for surveillance advertisement.[58]

[47] Italian Competition Authority, TikTok sanctioned for an unfair commercial practice, 14/03/2024 [accessed on 12/02/2025].
[48] Amnesty International, TikTok risks pushing children towards harmful content, 15/11/2023 [accessed on 12/02/2025].
[49] NPR, TikTok executives know about app's effect on teens, lawsuit documents allege, 11/10/2024 [accessed on 12/02/2025].
[50] LPM, "AG Coleman Sues TikTok, Says Internal Documents Show Company Knowingly Addicted KY Youth," News article, 9 October 2024 [accessed on 12/02/2025]. .
[51] LAist, "States Probed TikTok for Years. Here Are the Documents the App Tried to Keep Secret," News article, [accessed on 12/02/2025].
[52] BEUC, The Digital Services Act proposal, 09/04/2021.
[53] This would go beyond Article 38 of the DSA for VLOPs and VLOSEs as the latter only requires the option to have a recommender system not based on profiling.
[54] Panoptykon Foundation & People vs Bigtech, Safety-by-default, 05/03/2024 [accessed on 12/02/2025].
[55] Forbrukerrådet, Time to Ban Surveillance-Based Advertising, June 2021.
[56] Eurostat, Eurostat News: Over 90% of young people in the EU use social media, 14/07/2023.
[57] European Data Protection Board, Urgent Binding Decision 01/2021, 13/04/2021.
[58] Hungarian National Authority for Data Protection and Freedom of Information, Decision on the Processing of Minors' Personal Data for Market Research and Direct Marketing Purposes, February 2022 [accessed on 12/02/2025].

The data collected from users on digital platforms or other services like video games[59] is often utilised for surveillance advertising.[60] **While the DSA prohibits profiling-based advertising targeting children, the provision's effectiveness relies heavily on prompt and timely enforcement.** On top of that, there is no assurance that minors' collected data is deleted to prevent its use for surveillance-based advertising once they become of age[61] or to ensure it is not exploited to train AI systems. However, **surveillance advertising toward minors does not end with the DSA**. As highlighted in the Digital Fairness Fitness Check report,[62] many online services, such as B2C retail websites and especially video games that do not constitute intermediary platforms, fall outside of its scope.

### 3.3. Influencer marketing and hidden advertising

Problems arise also with so-called **hidden advertising**, especially in the case of social media and influencer marketing.

73% of consumers have encountered promotions by influencers and 53% report buying products or services recommended by them.[63]

44% of consumers have seen influencers promoting scams or dangerous products.[64]

Only 20% of influencers systematically indicated the commercial nature of the content shared.[65]

While almost half of the respondents, especially those in younger age groups, noticed that the content they were viewing seemed to be a paid promotion or advertisement, 38% of children between 6-12 do not recognise commercial influencer content as constituting advertising.[66]

The high prevalence of **influencer marketing is particularly concerning given the difficulty for consumers, especially kids, to recognise its commercial nature, even when disclaimers are used**. This is further complicated by the parasocial relationships many influencers cultivate, presenting themselves as friends or older siblings. With countries like France already adopting laws to address this issue, there is an urgent need for a unified approach within the EU to prevent regulatory fragmentation.

**Issues with misleading marketing to children also extend to the promotion of unsuitable products and services**. Children are particularly targeted by unhealthy food ads,[67] a practice linked to rising childhood obesity rates, as highlighted by the World Health Organisation.[68] The lack of EU-binding rules to curb unhealthy food marketing to children, which was instead tackled by soft self-regulatory and co-regulatory measures under the Audiovisual Media Services Directive (AVMSD), has left young audiences highly exposed to such advertising. Similarly, the marketing of dietary supplements, such as muscle-building products, exploits body-image pressures and encourages unnecessary spending on ineffective or

[59] Bird&Bird, Programmatic advertising: it's in the game, 30/03/2023 [accessed on 12/02/2025].
[60] BEUC blog, Why it's time to ban surveillance ads, 15/11/2021.
[61] BEUC, Towards a safer, more private and secure internet for children in online platforms, 30/09/2024.
[62] European Commission, Questions and Answers on the Digital Fairness Fitness Check, 03/10/2024.
[63] BEUC, From influence to responsibility, Time to regulate influencer marketing, 07/07/2023.
[64] *Ibid*.
[65] European Commission, Commission Staff Working Document 'Fitness Check of EU consumer law on digital fairness', 03/10/2024.
[66] Danish Competition and Consumer Authority, Consumers Benefit from visually salient standardised commercial disclosures on social media, June 2021 [accessed on 12/02/2025].
[67] BEUC, Children massively targeted by unhealthy food ads: consumer groups' snapshot exposes blatant need for binding EU rules, 27/09/2021.
[68] *Ibid*.

potentially harmful items.[69] **It is evident that self-regulation falls short on protecting children from exposure to harmful marketing practices, particularly online.**

These gaps show that many harmful commercial practices, that children face online, remain unaddressed under the current EU digital rulebook. **The DFA presents an opportunity to address all harmful commercial B2C practices, including advertising,[70] across all traders.**

Finally, **it is also important to acknowledge that influencer marketing can be detrimental to minors' mental health by fostering unrealistic expectations, including about consumer consumption, thereby contributing to stress and anxiety** as rightly recognised in the Commission's Digital Fairness Fitness Check report.[71] These observations should inform any upcoming legislation on the matter.

### 3.4. Dark patterns

The term 'dark patterns' is commonly used to refer to the manipulation of consumers through the way in which online interfaces are being designed, structured or operated. The most widely used dark patterns were hidden information/false hierarchy, preselection, nagging, difficult cancellations and forced registration.[72]

97% of the most popular websites and apps used by EU consumers deployed at least one dark pattern.[73]

**Unfortunately, EU law does not comprehensively address dark patterns.** Instead, it tackles them through various legal frameworks, each with a specific focus. The most significant legal basis is the UCPD which applies horizontally to all B2C relations.

- The UCPD includes a general prohibition on misleading and aggressive commercial practices, but these prohibitions are formulated in very general terms which is why they provide little clarity as to whether and to what extent dark patterns are prohibited.

- The UCPD Annex contains a list of commercial practices that are prohibited, but unfortunately, this list covers only a few dark patterns, such as bait-and-switch tactics (Item 6) and false countdown timers (Item 7).

Beyond the UCPD, several other EU laws contain provisions addressing dark patterns, but either the scope of these laws is limited, or they only cover a few dark patterns.[74]

While these various EU laws address dark patterns**, a more unified and comprehensive approach is needed under the Digital Fairness Act.** As a safety net, consumer law can ensure full protection for

[69] Forbrukerrådet, One in Two Young People Use Muscle-Building Dietary Supplements, 17/10/2021.
[70] European Commission, Commission Staff Working Document 'Fitness Check of EU consumer law on digital fairness', 03/10/2024.
[71] *Ibid.*
[72] *Ibid*
[73] European Commission, Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. https://op.europa.eu/s/xrpf, page 6, 2022.
[74] The Consumer Rights Directive prohibits the use of pre-ticked boxes if they result in additional costs for consumers.
The GDPR addresses dark patterns in relation to the processing of personal data under the principles of fairness (Art 5.1a GDPR), data protection by design and by default (Art 25.1 GDPR) but also on how the requirements of consent are respected.
The DSA bans dark patterns, but its scope is limited to online platforms.
The DMA only applies to designated gatekeepers in the digital market.
The Data Act bans dark patterns in connection to data sharing of connected products.
The AI Act prohibits certain manipulative practices that can cause people significant harm.
The Directive on financial services contracts concluded at a distance prohibits the use of dark patterns when concluding contracts for such services.

consumers, especially children, across all sectors.[75] It should be completed with effective and proper enforcement to help tackle these practices.

## BEUC RECOMMENDATIONS

**1** The Commission should ambitiously **enforce Articles 34 and 35 of the DSA** against VLOPs and VLOSEs to tackle addictive design.

**2** The Commission should **use the guidelines of Article 28(4) DSA to provide an open list of practices that lead to digital addiction and are very likely to infringe Article 28(1) DSA**, referring to the safety, privacy and security of minors.

**3** **Engagement-based recommender systems should be turned off by default.** To safeguard children's autonomy, engagement-based recommender systems should be disabled by default. Children should be empowered to opt into these systems, ensuring they have control over their data and online experience in line with GDPR requirements.

**4** **Recommender systems should be optimised for quality and content relevance**. This can be achieved by incorporating simple, user-friendly curation and feedback mechanisms that enable consumers to influence the content they receive, thereby improving usability and accessibility.[76]

**5** **Tracking features** (e.g. non-essential cookies, pixels, and location techniques) **on minors' accounts should be disabled by default**, with sensitive functions such as cameras and microphones automatically turned off after each session.

**6** **Children should have an easy and accessible way to delete their digital footprint**, such as through a dedicated 'erase' button.

**7** **Regarding children's privacy in electronic communications,** there should be strict limits on the use of their communications data, as well as the terminal equipment and software designed for them. Notably, children's communications data should never be used for targeted advertising purposes. Also, children should not be targeted by websites with content for kids using profiling and behavioural marketing techniques.

**8** The Commission and national competent authorities should ensure **the prompt and effective enforcement of Article 28(2) of the DSA**.

[75] For a detailed discussion on how dark patterns should be addressed by enforcement authorities and the EU legislator, see BEUC, "Dark patterns" and the EU consumer law acquis, 2022.
[76] People vs Big Tech, Prototyping User Empowerment – Towards DSA-compliant Recommender Systems, 2024 [accessed on 12/02/2025].

**9** **Revise the AVMSD and the UCPD to implement a comprehensive ban on unhealthy food marketing to minors**. This ban should apply to all advertising and commercial communication channels, based on children's exposure to them rather than surveillance-based communication and advertising. The prohibition should also **extend to other unsuitable products and services for children**, such as alcohol, gambling, medical products and procedures.

**10**

**Fill the enforcement gap in regulating influencer marketing** by introducing:[77]

- **EU-wide disclosure rules:** unified and prominent advertising displays across online platforms to help influencers and creators transparently indicate when their content contains or constitutes commercial communication, making it understandable for both adults and children (one single wording etc.).
- **A clear definition of "influencer marketing" and a harmonised definition of "user-generated content" in the UCPD**. Any content shared by a creator in exchange for consideration should qualify as commercial intent and be **subject to mandatory disclosure requirements**.
- **Transparency requirements** should ensure clarity about the entities funding promoted content, aligning with DSA Article 26(2).
- **A joint liability regime among influencers, agencies, and traders** to ensure accountability throughout the influencer value chain[78], unless the influencer is a minor, in which case the liability should be shared with their legal representative. If the influencer is a minor, liability should rest with their legal representative.
- **Prohibition of influencer marketing campaigns for certain types of products** which pose particular risks for consumers, including children (aesthetic surgery, nicotine, unhealthy food to children, alcohol gambling, risky financial products etc.).

**11**

The Commission should update consumer law through the upcoming Digital Fairness Act (DFA) by:

- Introducing **a horizontal prohibition on dark patterns**, reinforced by **an anti-circumvention clause,** in the UCPD. Additional examples should be added to the Annex blacklist to enhance enforcement.
- Establishing **a reversal of the burden of proof as a horizontal measure to address digital asymmetry**, imbalances of knowledge and power between consumers and businesses. Additionally, introducing a requirement for fairness by design is essential to ensure consumers are genuinely protected.
- Creating an **open list of prohibited addictive design practices**, regularly updated to remain future-proof. This would ensure that traders beyond platforms are covered, filling gaps left by the DSA, with the DFA acting as a safety net.

[77] BEUC, "From Influence to Responsibility: Time to Regulate Influencer Marketing", 07/07/2023.
[78] BEUC, "From Influence to Responsibility: Time to Regulate Influencer Marketing", 07/07/2023.

- Introducing a **horizontal ban on advertising based on surveillance targeting minors in consumer law**, expanding beyond Article 28 of the DSA, which currently applies only to online platforms.

## 4. For a safer and fairer gaming experience

### Key figures on the gaming sector

More than half of EU consumers regularly play video games. Among children aged 11 to 14, that number is as high as 84%.[79] Ensuring a safe online environment in video games should be a top priority.

The majority of children (64%) spend an average of between €1 and €20 per month on games. However, there are notable instances of significant overspending by children (and consumers in general). The average monthly spend has increased from €33 in 2020 to €39 this year.[80]

The video games industry is one of the largest entertainment sectors in the world. Historically, it generated revenue primarily from the sale of video games, but in recent years, **in-game purchases have become an increasingly significant revenue stream**. Despite this growth, **the video game sector has largely evaded regulatory scrutiny**. Its business models are often complex or novel, and many authorities and policymakers still consider video games a niche market.

While the current EU consumer law acquis is fully applicable to the gaming sector,[81] **European legislation also has clear limitations in the gaming sector that need to be corrected via the upcoming Digital Fairness Act**.

## BEUC RECOMMENDATIONS

**1** Video game companies must be **prohibited from using deceptive design practices to exploit consumers of any age**. When engaging with video games, companies must ensure that their designs and operations do not manipulate consumer decisions to their detriment.

**2** **All in-game purchases should be priced in real-world currency**.

[79] Consumentenbond, Veilig online opgroeien: Ons pleidooi voor veilig online opgroeien, 2024.
[80] IPSOS, "In-Game Purchases in European Markets", 2023 [accessed on 12/02/2025].
[81] See BEUC Game Over Action, were on 12 September 2024, BEUC and member organisations from 17 countries denounced to EU authorities the unfair practices of leading video game companies, behind games such as Fortnite, EA Sports FC 24, Minecraft and Clash of Clans. Our analysis concludes that traders breach EU consumer protection laws.

**3** **Games likely to be accessed by minors must not:**

- **Offer loot boxes**[82] or other randomised content in exchange for real money.
- Include **"pay-to-win" mechanisms**.

**4** Consumers should have the option to **choose the exact amount of in-game currency they wish to purchase**. Additionally, the owner of the payment method must be notified before any in-game transactions are made.

**5** **Consumers should be able to play video games without having their economic behaviour influenced algorithmically**. The most privacy-protective mode should be activated "by default".

## 5. Delivering on the ground

Enforcement is essential to protecting children's rights in the digital world. While parents, educators and care-holders have an important role to play, the burden should not be on them only, as traders have very important responsibilities to ensure a safe digital environment for children. When applying rules, authorities should consider the behavioural vulnerabilities and specificities of children who, because of their age and lack of experience may fall prey of illegal practices more easily than adults. **Enforcement of relevant EU legislation should** therefore **be tailored to the specific needs of children as target groups,** as it is for instance currently the case with the UCPD.

Effective enforcement should be timely to have a concrete impact. Delays in enforcement, such as BEUC's six-year unresolved GDPR complaint against Google's location tracking, undermine protections and have significant consequences for children's well-being and development. In addition, effective enforcement requires **ambitious and robust procedures across all applicable legal frameworks**, including personal data protection, consumer law, online platforms, markets, and audiovisual media services. A key element in upholding children's rights is **the cooperation between different enforcement authorities.** This cooperation between authorities took place in the past[83] and should be strengthened in the future to ensure that children's protection is addressed in a consistent and coherent manner across sectors.

[82] Loot boxes are 'mystery packages' of digital content in video games which consumers purchase with real money. Loot boxes give gamers advantages or items to use in the game. However, they are randomised, meaning that consumers have no way of knowing what they contain until they have paid for them.

[83] See, for example, the 2022 conclusions from the group of volunteers among representatives from national consumer and data protection authorities, facilitated by the European Commission and the EDPB, on Advertising Towards Children.

## BEUC RECOMMENDATIONS

**1** Ensure the **prompt and effective enforcement of existing EU laws**, such as the GDPR, the ePrivacy Directive, the DSA and the UCPD, to provide a higher level of protection to children.

**2** **The authorities should adapt their benchmark when reviewing illegal practices and carefully consider the needs and vulnerabilities of children.**

**3** **Cross-sectoral and cross-border cooperation of enforcement authorities is necessary to uphold children's rights online**. This should also come in the form of coordinated actions, including the exchange of expertise, evidence and resources to support national authorities in their investigations.

**4** Authorities should **leverage platforms' own data to assess the effectiveness of measures implemented to mitigate harms**, ensuring these measures are not only present but actively used and achieving their intended outcomes.

**5** In case of a complaint being sent to the wrong authority, authorities should **redirect complaints rather than return them to the child or the person representing them**, encouraging swifter resolution and minimising barriers.

**6** **Future legislative proposals and revisions should include prescriptive**, on top of principle-based, **provisions to enable regulators to act decisively**. One-stop-shop enforcement structures, such as that under the GDPR, should be avoided to ensure prompt case handling across jurisdictions.

**7** The Commission should emphasise **the revision of the CPC Network Regulation to address its shortcomings and enhance its role in tackling widespread infringements**. This includes granting the Commission enforcement powers to handle EU-wide violations, similar to its role under the DSA and DMA, and clarifying the *ne bis in idem* principle to ensure legal certainty and encourage action on cross-border violations.

**8** Co-legislators must ensure that **the GDPR cross-border enforcement Regulation**[84] currently in trilogues, **delivers for consumers, drives compliance and creates a level playing field between all SMEs and multinationals**.

[84] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules for the enforcement of Regulation (EU) 2016/679, 2023.

## 6. Conclusion

Decision makers must prioritise protecting children online by adopting a proactive, rights-respecting approach to digital regulation. This includes making the internet safe by design and by default with private, secure settings and targeted measures addressing harmful practices without relying solely on age verification tools, which can carry significant risks. Bridging gaps in existing laws, such as data protection, consumer, and media regulations, is essential, to address issues like addictive design and influencer marketing. Rigorous enforcement of these laws, coupled with cross-border and cross-sectoral cooperation, is essential to protecting children's rights in a digital landscape where business interests often take precedence over safety.

-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.*