

## PROTECTION OF MINORS ONLINE

Recommendations of the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv) on the Commissions draft guidelines on protection of minors online under the Digital Services Act (DSA)

3. Juni 2025

### Legal information

**Federation of German Consumer Organisations – Verbraucherzentrale Bundesverband e.V. (vzbv)**

Team Digital and Media  
[digitales@vzbv.de](mailto:digitales@vzbv.de)

Rudi-Dutschke-Straße 17  
10969 Berlin

The Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband e.V.) is registered in the German Lobby Register and the European Transparency Register. You can access the relevant entries [here](#) and [here](#).

# CONTENT

<b>RELEVANCE FOR CONSUMERS</b>	<b>3</b>
<b>INTRODUCTION</b>	<b>4</b>
<b>SUMMARY</b>	<b>4</b>
<b>INDIVIDUAL POINTS IN DETAIL</b>	<b>5</b>
1. Risk Review (5)	5
2. Service Design (6)	5
2.1 Age Assurance (6.1)	5
2.2 Account settings (6.3)	6
2.3 Online interface design and other tools (6.4)	6
2.4 Recommender systems and search features (6.5)	7
2.5 Commercial practices (6.6)	7
2.6 Moderation (6.7)	8
3. Reporting, User support and Tools for Guardians (7)	8

## RELEVANCE FOR CONSUMERS

Children and young people should be able to take advantage of the internet, build communities and express themselves. At the same time, their privacy must be protected and their general safety ensured. In 2025 Verbraucherzentrale Bundesverband e.V. (vzbv) conducted a qualitative study of 18 selected online platforms to analyse the prevalence of "Hyper-Engaging" dark patterns (HEDP). Both social networks and online marketplaces were examined. The results show that all platforms studied make use of HEDP elements, albeit to varying degrees. Particularly striking techniques included infinite scroll, autoplay, gamification, and the exploitation of the "fear of missing out" (FOMO). Minors are a particularly vulnerable target group since they are more susceptible to manipulative design due to their limited experience, cognitive development, and higher emotional responsiveness. Platforms often use mechanisms like streaks, reward badges, and peer comparisons to encourage longer usage, which can foster addictive behaviour in minors. Important information like terms of use, costs, or data collection practices are often hidden or hard to understand, which is especially problematic for younger users. Children may also not be able to distinguish between genuine content and advertising, making them more prone to covert commercial influence. More target group-oriented design and default settings can help to minimise these risks so that underage users can navigate the internet as safely as possible.

# INTRODUCTION

On 13<sup>th</sup> of May 2025, the European Commission published the ‘Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065’ to seek feedback on the guidelines on protection of minors online under the Digital Services Act (DSA). vzbv would like to thank the European Commission for the opportunity to comment on the proposed guidelines.

The guidelines aim to support platforms accessible by minors in ensuring a high level of privacy, safety, and security for children, as required by DSA. The guidelines outline a list of non-exhaustive measures that all platforms, with the exception of micro and small enterprises, can implement to protect minors, using a default approach that is guided by privacy by design.

Minors are a very vulnerable target group that needs special protection in digital environments. With this paper, vzbv provides an initial statement on selected aspects discussed in the proposed guidelines for article 28 of the DSA.

# SUMMARY

Children should be able to enjoy digital spaces without encountering anything harmful. The goal is not to restrict access, but to create digital environments where minors can participate safely, learn confidently, and develop without fear or manipulation. With proper risk evaluation, child-friendly defaults and design, online platforms can uphold their responsibility to younger users. In response to the European Commission’s draft guidelines on protecting minors online, the Federation of German Consumer Organisations (vzbv) suggests the following aspects to be taken into account with regard to the proposed guidelines:

- ✦ Risk classification must move beyond abstract frameworks. While the OECD’s 5Cs typology of risks (Content, Conduct, Contact, Consumer, Cross-cutting) provide a helpful overview, they aren’t sufficient as an orientation for providers of online platforms to assess their services. Platforms need actionable guidance. vzbv calls for the Commission to provide a clear system for evaluating risk levels so platforms can tailor their protective measures accordingly.
- ✦ Age assurance is not a silver bullet. It can be bypassed and misused. vzbv advocates for child-friendly design and features by default. Age assurance should only be used selectively when changing default settings.
- ✦ Digital interfaces should empower, not manipulate young users. Children are especially susceptible to dark patterns and exploitative advertising, which can compromise their safety and decision-making. vzbv strongly supports a ban on manipulative design features and demands simple, accessible tools for deleting personal data and entire accounts.
- ✦ Recommendation algorithms often prioritise content that maximizes engagement. This model can expose children to disturbing, addictive, or extreme content. vzbv argues that such systems should not rely on behavioural tracking at all. Instead,

content recommendations for minors should be based solely on explicit preferences, giving children more agency and control over their digital experience.

- ✦ Children's lack of financial literacy makes them especially vulnerable to unintended or impulsive spending. Reports of minors spending large sums on online games are alarmingly common. vzbv calls for the default deactivation of in-game purchases and clear spending limits.
- ✦ Minors must be shielded from harmful images and video content, while their own shared media must be protected from misuse. vzbv supports stronger moderation measures, such as screenshot blockers and automatic blurring of explicit material.

## INDIVIDUAL POINTS IN DETAIL

### 1. RISK REVIEW (5<sup>1</sup>)

The chapter explains how a provider of an online platform that is accessible to minors can undertake the risk review of its platform to determine which measures to put in place to protect children's safety, privacy and security and suggest considering the 5Cs typology of risks in Annex I which the Organisation for Economic Co-operation and Development (OECD) and researchers have classified. It includes five categories of risks: content, conduct, contact, consumer risks, cross-cutting risks. The typology is useful as a classification of risks that minors may encounter in digital environments but it lacks a clarification about which risks are high, medium or low. Since that is the base for any set of measurements providers of online platforms should undertake to protect the safety, privacy and security of minors, it is important to specify it in the guidelines.

vzbv recommends to the European Commission to introduce an orientation for online platform providers to help them assess the level of risks for minors and put proportionate measures into place.

### 2. SERVICE DESIGN (6)

#### 2.1 Age Assurance (6.1)

The proposed guidelines consider measures restricting access based on the recipient's age to be effective to ensure a high level of privacy, safety and security for minors on online platforms. At the same time, providers shall assess if age assurance based restriction is appropriate. It might be difficult for providers to assess if age assurance is an appropriate solution to protect minors since the proposed guidelines lack a clear classification of risks as already stated above (1. Risk Review (5)) or if other less intrusive measures might be sufficient to protect minor. A risk rating system can help platform providers to assess whether and what type of age protection is appropriate for the respective digital environment. Data protection aspects such as the principle of data minimisation must be taken into account. With regard to checking the age of users, and in particular of minors, systems should be used that do not collect and process any personal data.

It is also important to be aware of the fact that all types of age assurances can potentially be circumvented by minors for example through Virtual Private Network (VPN) clients. The aim should therefore be to make the internet safer for minors and not exclude

---

<sup>1</sup> The numbering refers to the chapters in the commission's draft guideline.

them from digital environments. This is best achieved through child-friendly platform design and default settings. For further details, see the recommendations in chapters 2.2 to 2.5.

vzbv recommends that the Commission develops a rating system that online platform providers can use as a guide when they need to assess whether age assurance is the right solution to protect minors or if less intrusive measures are sufficient.

vzbv recommends that providers of online platforms which address also minors shall implement measures to make their services child-friendly by design and default. Age verification would only come into play if certain functions that might endanger a minor's privacy, safety or security are to be activated.

## 2.2 Account settings (6.3)

vzbv is generally in favour of child-friendly account settings and platform design if online platforms offer their services to minors as already outlined in the previous chapter and supports the Commission's recommendations in chapter Default settings (6.3.1) in principal but advocates for the following adjustments:

The Commission states that online platforms should 'Ensure that minors are not in any way encouraged or enticed to change their settings to lower levels of privacy, safety and security' (430). Instead, minors should not be able to make account settings that might endanger their privacy, safety and security. Age verification would be required to change the settings.

vzbv recommends adding these points to the guidelines:

Ensure that there is no tracking-based advertising to minors. Ensure that the use of communication data and the data of the end devices and the software intended for minors is strictly limited.

## 2.3 Online interface design and other tools (6.4)

Manipulative platform design can be a great risk for users' safety, security and privacy. Since minors are a particularly vulnerable consumer group because of their developmental stage and psychological vulnerabilities, they are more easily manipulated into sharing personal data or making unintended online purchases. Providers of online platforms should therefore completely abandon manipulative design features in their online interface design.

The General Data Protection Regulation (GDPR) establishes the right to be forgotten (Article 17), which allows individuals to request the deletion of their personal data from the internet or from an organisation's systems under certain conditions. It is important that minors can easily make use of this right, as they are particularly vulnerable and data disclosed on the internet can compromise their privacy, safety and security. vzbv supports the Commission's recommendations in principal but advocates for adding the following points:

Avoidance of any manipulative design features, if a provider offers its services to minors.

Implementing an easy to find and use function for deleting your own content and deleting the account as a whole.

## 2.4 Recommender systems and search features (6.5)

Recommender systems and search features curate the content available to minors on online platforms. Children and young people must be protected from content that is harmful to them. Instead of using interaction rates to determine which content is shown to children, preferences stated by minors themselves should be prioritised to protect children's privacy, safety and security. The content for minors should be age-appropriate, differentiated and minors should be enabled to curate their own digital environments. In chapter 'Testing and adaptation of the design and functioning of recommender systems for minors' (6.5.1) the Commission suggests that online platforms should 'Prioritise 'explicit user-provided signals' over 'implicit engagement-based signals' to determine the content displayed and recommended to minors. The selection of such signals should be justified in the best interest of the minor, which will help to ensure that they contribute to a high level of safety and security for minors. For the purposes of the present guidelines, 'explicit user-provided signals' shall be understood as referring to user feedback and interactions that indicate users' explicit preferences, both positive and negative, including the stated and deliberative selection of topics of interest, surveys, reporting (43), and other quality-based signals. For the purposes of the present guidelines, 'implicit engagement-based signals' shall be understood as referring to ambiguous signals that infer user preferences from their activities (browsing behaviour on a platform), such as time spent viewing content and click-through rates' (539-550).

In a different passage the Commission suggest that providers should 'Ensure that recommender systems do not rely on the on-going collection of behavioural data that captures all or most of the minor's activities on the platform, such as watch time and click through rates, and do not rely on the collection of any behavioural data that captures the user's activities off the platform' (535-538). vzbv criticises recommender systems based on any form of user engagement to curate content for children. Engagement-based recommender systems only take into account whether a content is captivating and therefore tend to recommend content that keeps children online for as long as possible. Children are more likely to click on flashy, extreme, or emotionally charged content. If the algorithm of the recommender system learns to prioritise such content, it can distort children's perception or increase anxiety. Even on child-friendly platforms, algorithms can surface content that is not age-appropriate or even harmful, such as dangerous trends, challenges, or subtly violent material. vzbv therefore recommends that online platforms should not be allowed to collect any behavioural data (implicit engagement-based signals):

vzbv recommends to the Commission to suggest that online platforms shouldn't collect any behavioural data of children. Instead, the recommender systems and search features for children should only use explicit user-provided signals to curate content for them.

## 2.5 Commercial practices (6.6)

Minors are particularly vulnerable to impulsive decisions, manipulation, and financial harm. Minors typically do not possess the financial literacy required to make informed purchasing decisions. They may struggle to differentiate between virtual currency and real money or to understand the concept of recurring charges and cumulative costs. This can lead to unintended overspending. Minors are also more prone to impulsive behaviours. This makes them especially vulnerable to emotionally driven or short-sighted spending decisions: minors may unintentionally make large purchases using a parent's

credit card or linked account. Cases of children spending hundreds or even thousands of dollars on apps and games have been widely reported.<sup>23</sup>

vzbv welcomes the Commissions guidelines on commercial practices and recommends adding 'Ensure the restriction of online payments, e.g. by setting standard spending limits for children's accounts and deactivating in-game purchases by default' to protect them from commercial exploitation.

## 2.6 Moderation (6.7)

Minors must be protected from harmful image and video content, for example by making it unrecognisable. At the same time, user-generated image and video content from minors must be protected from misuse. The implementation of technical measures to protect minors against image-based digital violence must be effective without undermining the security and integrity of digital communication. vzbv welcomes the Commissions moderation guidelines and recommends adding the following points. Providers of online platforms should:

Ensure the protection of posted images by minors through screenshot blockers and copy and deep fake protection to reduce the risk that images posted by children and young people are misused and thus removed from their control.

Blurring of private messages with potentially age inappropriate content as well as potentially pornographic or violent images, which can be optionally unblocked by users by clicking on them.

## 3. REPORTING, USER SUPPORT AND TOOLS FOR GUARDIANS (7)

Reporting systems are essential for ensuring user safety, maintaining content quality, and upholding legal and community standards. It empowers users to flag harmful, abusive, or misleading content, enabling online platforms to take timely action and enforce guidelines effectively. This not only helps protect individuals from harassment, scams, and misinformation but also builds trust and accountability within the digital community. Additionally, reporting systems support regulatory compliance, provide valuable data for improving moderation tools, and contribute to a safer, more reliable online environment. vzbv welcomes the Commissions guidelines on user reporting, feedback and complaints and recommends adding following point to the guidelines in chapter User reporting, feedback and complaints (7.1):

The reporting option must be accessible with a maximum of two clicks via links clearly marked 'Check the reported content immediately in accordance with the requirements of the DSA if there are significant and serious dangers.'

<sup>2</sup> Kollwe, J. (2025, March 3). Our eight-year-old daughter spent over £8,500 on the Apple App Store. The Guardian. <https://www.theguardian.com/money/2025/mar/03/our-eight-year-old-daughter-spent-over-8500-on-the-apple-app-store>

<sup>3</sup> BBC News. (2023, May 26). *Ten-year-old girl spends over £2,500 on Roblox game*. BBC. <https://www.bbc.com/news/uk-wales-65659896>