



Verbraucherzentrale
Bundesverband

Protection of minors on social media platforms

Evaluating the implementation of Article 28 of the Digital Services Act (DSA) and the European Commission's Guidelines on the Protection of Minors

19 June 2026

Content

I. Relevance for consumers	3
II. Executive summary	4
III. Methodology.....	5
IV. Results.....	5
1. Registration and age requirements.....	5
2. Platform-provided protections for minors.....	6
3. Contact Options	7
4. Location sharing	11
5. Technical protection measures: content displayed	14
6. Time limits/limitation of the duration of use.....	16
7. In-app purchases.....	19
8. Personalised advertising	22
9. Manipulative and potentially addictive design elements.....	27
9.1 Autoplay, Infinite Scroll und Pull-to-Refresh	27
9.2 Push notifications	27
9.3 Manipulative requests to access sensitive features	29
9.4 Gamification and reward systems.....	32
10. Algorithmic recommender systems	35
11. Account deletion	42
V. Political demands	46
Imprint	48

I. Relevance for consumers

Many children and adolescents use digital services every day to connect with others, express themselves creatively and participate in the digital world. But unfortunately, the reality is also that online platforms, in particular, incorporate design features in their business models geared towards maximizing usage time and data exploitation. Manipulative design mechanisms such as infinite scrolling, autoplay, and algorithmic amplification pose high risks to mental health because they can be addictive. This is associated with habit-forming engagement loops, loss of control and the neglect of other activities as well as social contacts.¹ A representative survey conducted by the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband, vzbv) in 2025 clearly shows that a large proportion of consumers surveyed (93 percent) see shortcomings in the protection of minors online in at least one area: 65 percent of respondents criticize a lack of age controls, 54 percent complain about inadequate content filters, and 51 percent see too little commitment on the part of platforms to protect underage users². These results are not surprising given the default settings and design features of large platforms. An investigation by vzbv from January 2025 about dark patterns on online marketplaces and social media platforms³ also concluded that manipulative designs such as autoplay, infinite scrolling and aggressive push notifications were used across all evaluated platforms, even after the Digital Services Act (DSA) had come into force. A similar picture emerged in a vzbv evaluation of unfair practices and manipulative design elements in online games published in March 2025⁴. All games examined used manipulative designs, such as immediate purchase prompts that were displayed as soon as the app was opened. In addition, all gaming platforms examined employed in-transparent pricing information and displayed prices exclusively or partially in in-game currencies. Further studies show that platform designs aimed at maximising users' attention can impair adolescents' well-being by providing a continuous stream of stimuli, thereby negatively affecting sleep, concentration and psychological well-being⁵. These results illustrate a great need for action.

¹ See para. 69 l) of the European Commission's Guidelines. Accordingly, providers of online platforms accessible to minors should ensure that minors are not exposed to manipulative design techniques that can lead to excessive, impulsive or unwanted spending or addictive behaviours.

² Representative online survey (October 2025), conducted by Eye Square on behalf of vzbv. Sample: 1,000 internet users aged 16 and over. Statistical margin of error: max. ± 3 percentage points.

³ Verbraucherzentrale Bundesverband e.V. (Federation of German Consumer Organisations): Manipulative designs on online marketplaces and social media platforms. Evaluating the implementation of Article 25 of the Digital Services Act (DSA), January 2025, [online] https://www.vzbv.de/sites/default/files/2025-11/25-01-15_MB-Report_Manipulative_designs.pdf.

⁴ Verbraucherzentrale Bundesverband e.V. (Federation of German Consumer Organisations): Unfair practices and manipulative designs in online games and on gaming platforms. A field study, March 2025, [online] https://www.vzbv.de/sites/default/files/2025-04/25-03-11_Paper_vzbv_Manipulative_design_unfair_practices_online_games.pdf.

⁵ Baumgartner, Susanne E.: The Effects of Digital Media and Media Multitasking on Attention Problems and Sleep, In Handbook of Adolescent Digital Media Use and Mental Health, eds. Jacqueline Nesi, Eva H. Telzer, and Mitchell J. Prinstein. Cambridge: Cambridge University Press, June 2022; Petrie-Flom Center (Harvard Law School): Addictive Algorithms and the Digital Fairness Act: A New Chapter in EU Public Health Policy?, August 2025; Poles, A.: Impact of Social Media Usage on Attention Spans. Psychology, 16, 760-772, June 2025.

II. Executive summary

The study shows that the platforms examined do not comply sufficiently with their obligations to protect minors. In vzbv's view, the five platforms examined – Facebook, Instagram, Snapchat, TikTok and YouTube – violate the provisions of Art. 28 of the DSA. In addition, the design of the platforms frequently stands in direct contradiction to the European Commission's guidelines for the protection of minors.

Although all social networks examined restrict the visibility of user profiles, user-generated content and contact options for minors, profiles can still be easily found. Combined with providers' sometimes aggressive prompts to share phone book contacts, this can result in large numbers of people being able to contact minors.

While location sharing is not enabled by default on any of the five platforms examined, in four cases underage users can grant location access themselves. Snapchat, in particular, attempts to persuade users to grant access by sending repeated prompts.

All five platforms examined make use of manipulative design features. In addition to manipulative prompts, these include potentially addictive design elements such as autoplay, infinite scroll and pull-to-refresh. The study also found that rewards and gamification elements are used to keep users engaged with the platform for longer, increasing both the interactions with the platform and usage time.

Some of the platforms examined provide conflicting information regarding personalised advertising, so that it remains unclear based on what criteria adverts are displayed. With some providers, deleting a user account is a very complicated process and sometimes made even more difficult by manipulative design features.

All the apps examined display personalised content feeds on their home screens, based on algorithmic recommender systems. Although the DSA requires platforms to provide easily accessible options and feed alternatives that do not rely on profiling, vzbv found that minors face various obstacles and restrictions in this regard. For example, options without profiling are not always clearly labelled or cannot always be set as a permanent default. In addition, long click paths, hard-to-find settings, and other manipulative design techniques may deter minors from using non-personalised feeds.

III. Methodology

vzbv examined five selected social media platforms to assess how providers implement the DSA's requirements on the protection of minors online.

The sample consisted of Facebook, Instagram, Snapchat, TikTok and YouTube, as these five – out of a total of eight social media providers designated by the European Commission as 'Very Large Online Platforms' – account for the largest number of active users in Germany.⁶

The investigation examined compliance with Article 28 of the DSA (Online Protection of Minors)⁷ as well as with the European Commission's Guidelines on the Protection of Minors under the DSA⁸.

For the study, test accounts were created for fictitious 13-year-old users. The assessment focused on the registration procedures, age requirements, default account settings and interface design.

vzbv evaluated the platforms between March 13 and June 1 2026 using a previously developed categorisation framework based on the relevant legal requirements.

IV. Results

1. Registration and age requirements

According to the terms and conditions of the providers, four of the five platforms examined require a minimum age of 13 years for their use (with the exception of YouTube).

It is not possible to register on any of these four platforms if the user is younger than the specified age.

YouTube is a special case in terms of its minimum age, which is 16 years. However, with the consent of a parent or guardian, children and adolescents of all ages can use YouTube. In this case, it is necessary to link the account to a parent's (Google) account.

For the registration of the test accounts, fictitious dates of birth for 13-year-olds were used. None of the five platforms examined carried out any verification of the age provided.

⁶ The list of platforms designated by the European Commission as VLOPs is available online at: <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>. The DSA obliges all providers of very large online platforms to publish the number of monthly users of their services (Average Monthly Active Recipients) in the EU. Cf. the information provided by the providers in their respective DSA transparency reports to the European Commission: <https://digital-strategy.ec.europa.eu/en/policies/dsa-brings-transparency>

⁷ Cf. [Reference to the DSA full text](#)

⁸ Cf. <https://eur-lex.europa.eu/eli/C/2025/5519>

2. Platform-provided protections for minors

Child accounts and other platform-provided protections for minors are sometimes presented by platforms as tools to protect children and adolescents. These features are meant to provide age-appropriate content, restrict communication and give parents greater oversight and control options. From vzbv's perspective, however, such accounts do not provide sufficient protection against the key risks of digital environments, as they address neither manipulative platform designs nor algorithmic recommendation mechanisms that promote excessive use.

All five platforms examined offered limited privacy, content and communication settings that were predetermined based on the user's reported age.

In some cases, the platform-provided protections also allow a parent to adjust and manage the settings of a minor's account. For example, Instagram automatically assigned the test account of a 13-year-old user to a "teen account" with the option to activate "parental supervision".

Example TikTok

TikTok, for example, offers "Family Pairing" which allows parents to manage settings such as screen time and messaging permissions for a minor's account, among others things. "Family Pairing" is optional for the account of a minor. To activate it, both accounts must be linked and assigned the respective role of parent and teenager (see Fig. 1). This can be done via a QR code or an invitation.

Strikingly, in the test, it also seemed to be possible to set the account of the 13-year-old user as the parent of another account (see Fig. 2).⁹ Thus, children and teenagers could possibly circumvent safety features.

⁹ When activating accompanied mode, the TikTok app asks whether you are a parent or a teenager. With the underage test profile, it was possible to select "parent" here. However, the subsequent steps leading up to the actual linking of the two profiles could not be verified / conducted in this test.

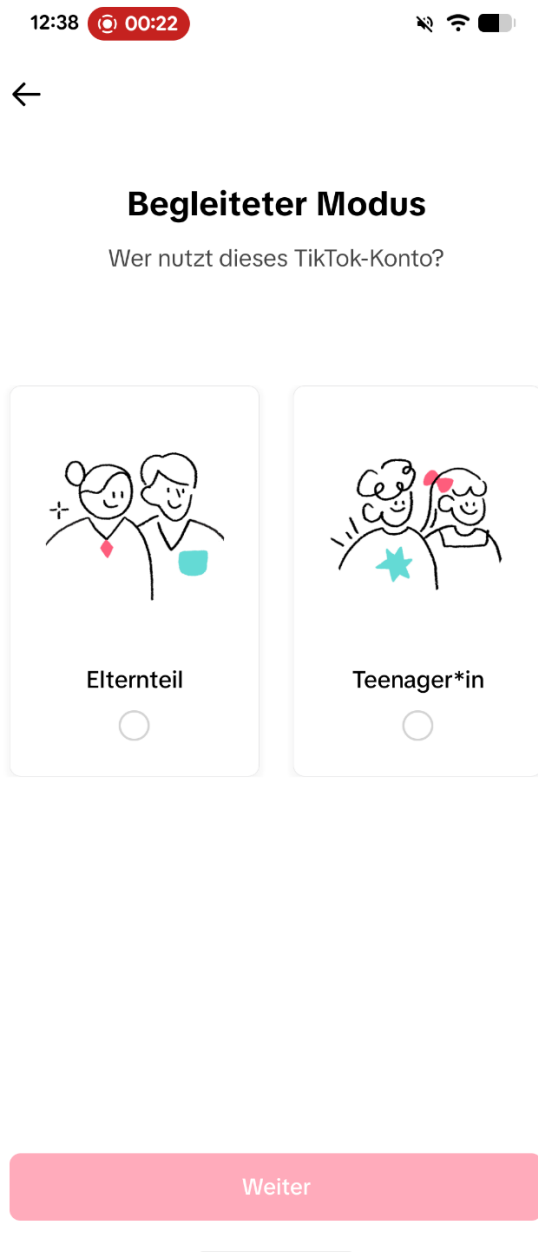


Figure 1: When activating Family Pairing, TikTok asks if you are a parent or a teenager.

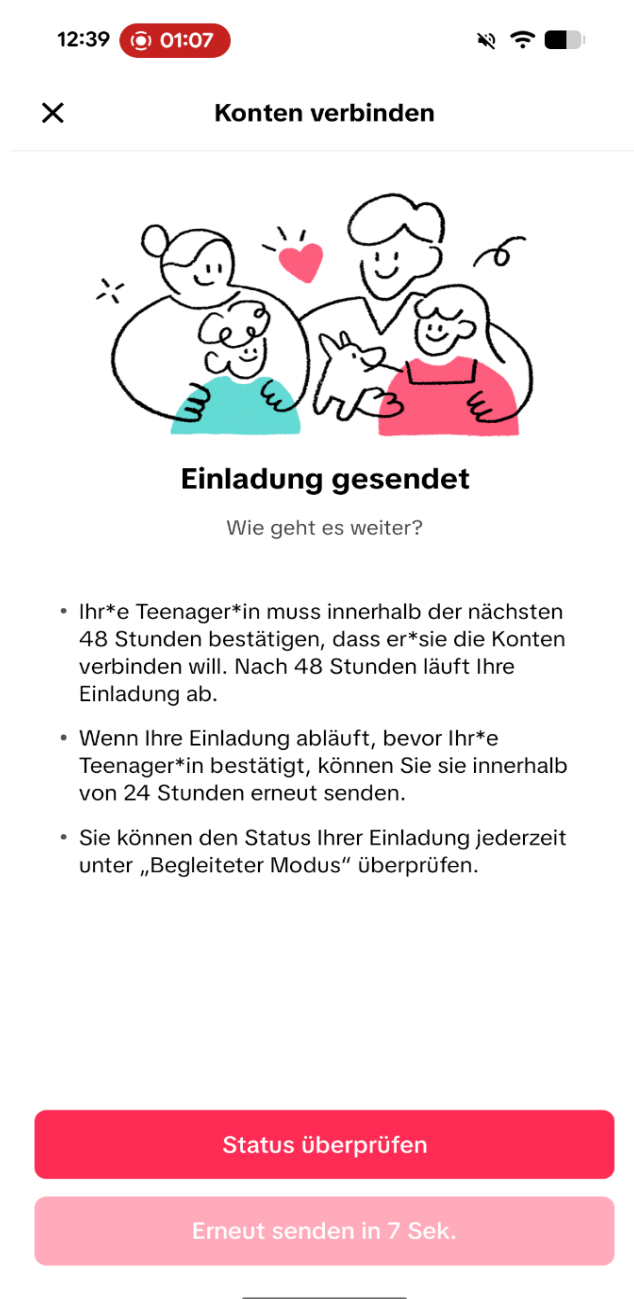


Figure 2: On TikTok, it was possible to select the role of a parent in the underage test profile.

3. Contact Options

The possibility of strangers being able to make direct contact with minors is a key risk for grooming, harassment and sexualised violence. Children and adolescents are particularly vulnerable in this regard, as they often do not yet have the experience or awareness of what information they should disclose and what risks are involved.

On all platforms examined, contact options for minors are restricted by default. However, they can be changed afterwards, for example on Instagram or TikTok. Since the platforms do not display a warning or offer a temporary change to this default setting, vzbv finds that they do not comply with the relevant requirements of the European Commission's guidelines. They suggest the above-

mentioned measures when minors "opt into features that put their privacy, safety or security at risk" by changing default settings¹⁰.

In addition, some platforms specifically ask users to grant access to their phone contacts so that they can find friends or other contacts on the platform (see Chapter 9).

Example TikTok

On TikTok, the default setting allows only approved users to follow a minor's profile and view their posts (see Fig. 3). However, minors can change this setting afterwards. Similarly, posts by minors can only be commented on by verified friends (see Fig. 4). This setting cannot be changed.

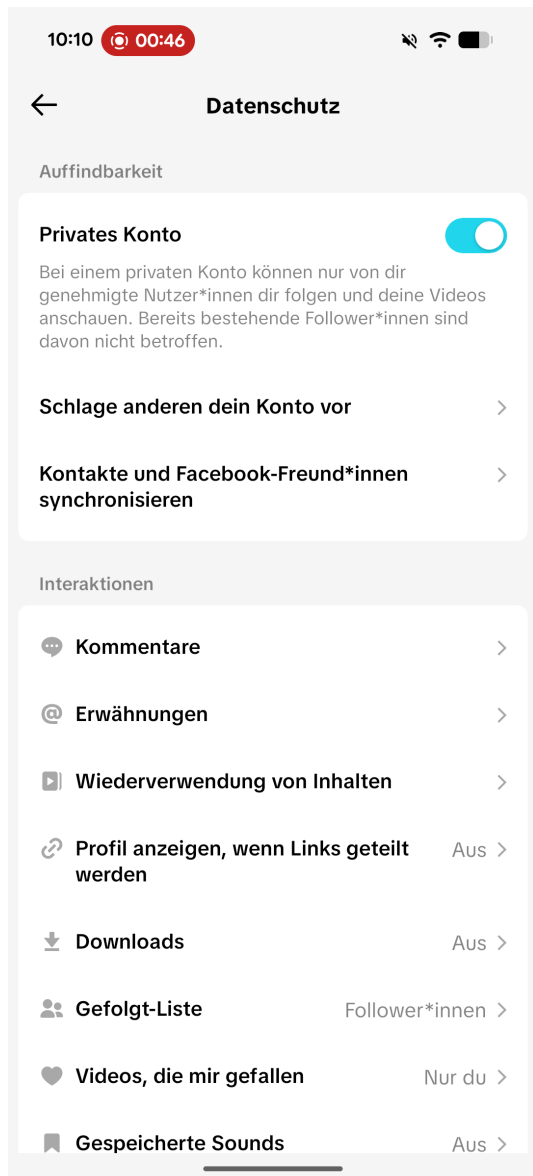


Figure 3: Only approved users can follow the underage TikTok profile.

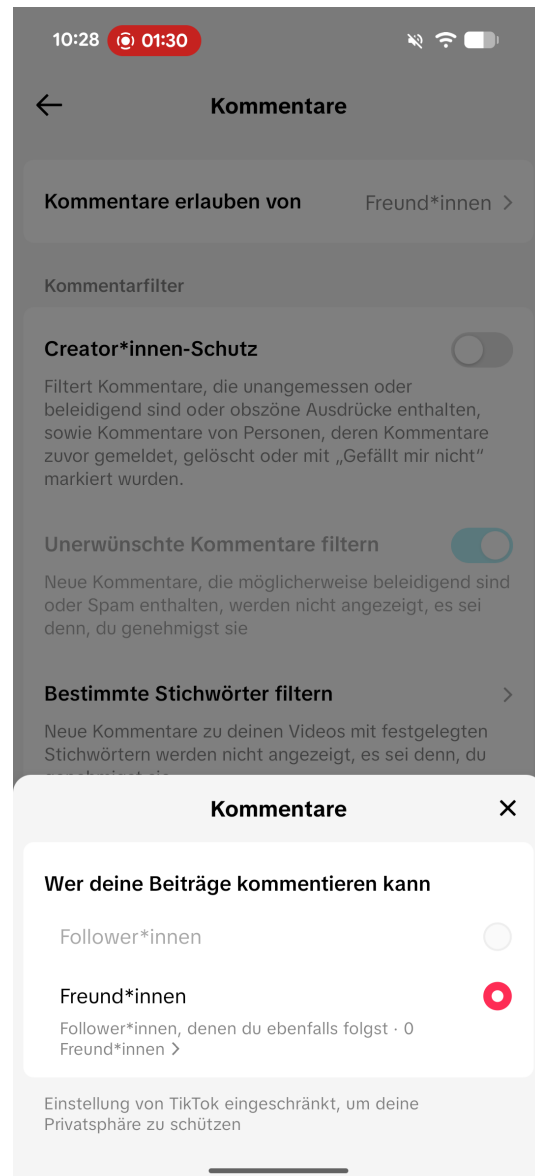


Figure 4: Only friends can comment on posts on TikTok. The Followers option is greyed out.

¹⁰ European Commission, Guidelines on measures to ensure a high level of privacy, safety and security of minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065, paragraph 58: <https://eur-lex.europa.eu/eli/C/2025/5519>

Who minors can communicate with on the platform by default usually depends on the child protection measures implemented by the provider¹¹ (see Chapter 2).

In some cases, however, the fact that profiles can be found via the search function (with some profile information visible, such as the name and profile picture) means that unknown adults can send friend requests to minors and subsequently exchange messages with them.

On four out of five platforms tested, underage users were able to grant access to their microphone and camera, meaning that they could also exchange (or post) images or voice messages (with the exception of YouTube¹²). In some cases, the platforms also request minors to grant access (see Chapter 9).

Example Instagram

Even when using a Teen Account, Instagram allows underage users to share their phone contacts without parental consent. Instagram repeatedly prompts users to do so (see Fig. 5).

In addition, the "Automatically confirm anyone you follow" feature can be enabled, which means that people you follow can automatically follow your (in this case: private) account back without any confirmation being required.

In vzbv's view, underage users can easily lose track of their followers this way. The combination of repeated prompts to share their contact list and the auto-confirmation feature (without prior verification) can lead to a large number of followers, which undermines the default "private" setting of the account.

¹¹ For example, the default settings for the "teen account" on Instagram prevent people you don't already know from sending you message requests.

¹² In theory, permission can be granted via the smartphone's app permissions. However, in the case of the test account, there was no way to use the camera or microphone within the app.

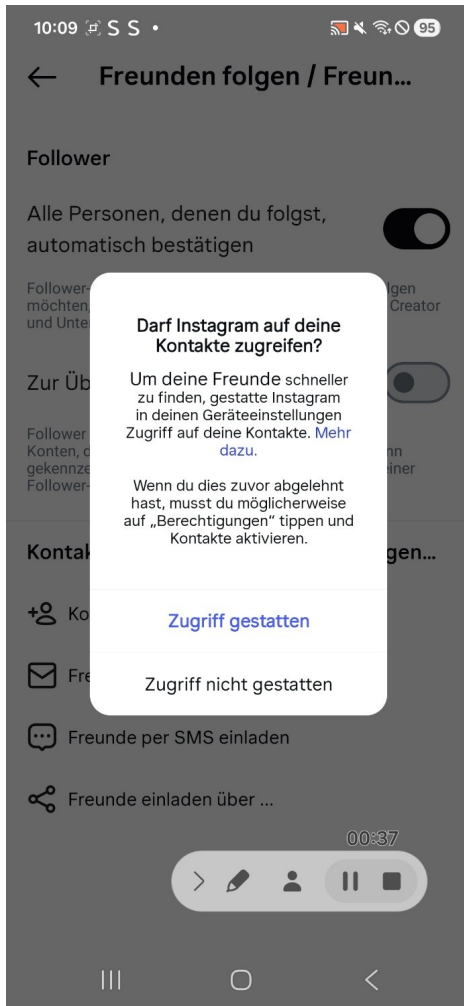


Figure 5: Instagram requests access to contacts stored in the user's phone book. In the background, the "automatically confirm anyone you follow" option can be enabled: people a user follows can automatically follow them back.

Example Facebook

On Facebook, the underage test profile can be found by all Facebook users via the platform's internal search function, and by default, anyone can send it a friend request (see Figs. 6 and 7).

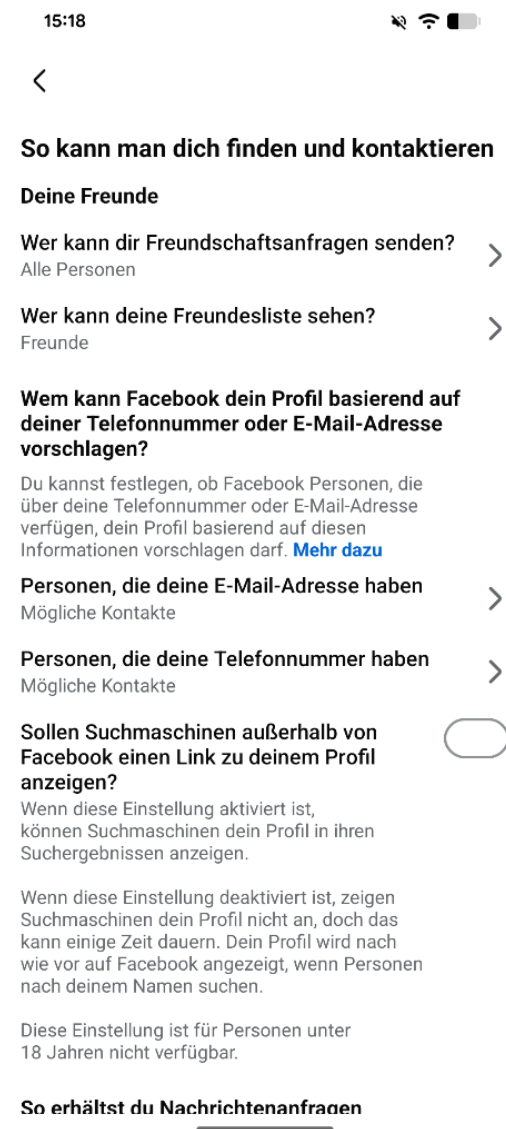


Figure 6: By default, everyone on Facebook can send friend requests.

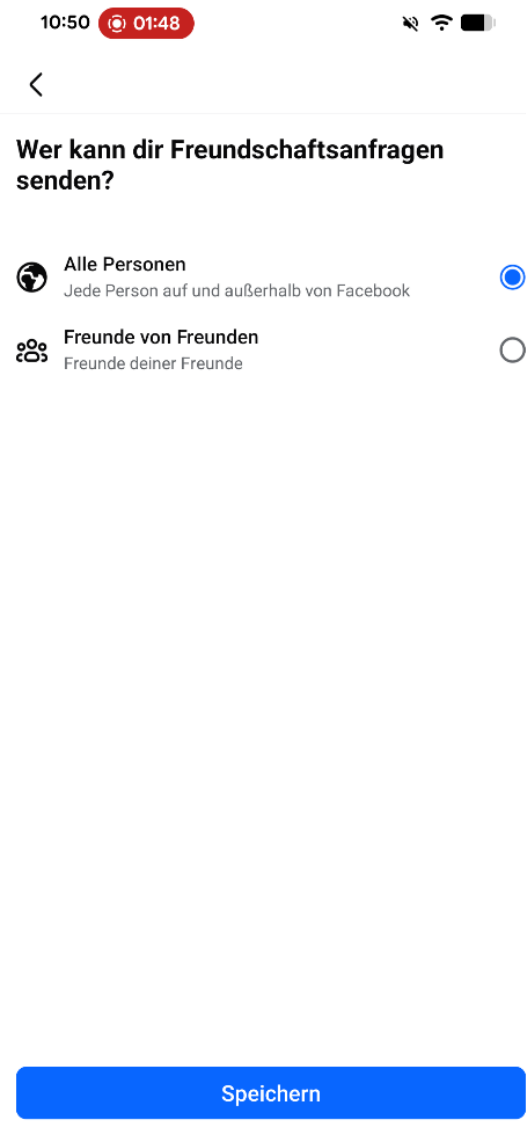


Figure 7: By default, everyone on Facebook can send friend requests.

4. Location sharing

In vzbv's view, the automatic sharing of location data can pose a significant threat to the safety of children and young people. Location information enables third parties to track physical whereabouts, which can lead to surveillance, stalking, or targeted abuse. Children and adolescents often lack the experience or awareness of the risks involved in sharing location data and are, therefore, particularly vulnerable.

None of the five platforms examined has location sharing enabled by default. In four out of five cases, however, location sharing can be enabled by underage users (with the exception of YouTube). However, in these cases, when minors choose to reduce their level of protection, the providers do not consistently implement the measures proposed by the European Commission (such as warning messages or the option of temporary sharing).

Example Snapchat

With recurring prompts and eye-catching buttons, Snapchat attempts to encourage underage users to share their location as extensively as possible (see Fig. 8). A number of granular setting options are available to users. For some of these, the more permissive option is preset or actively promoted (see Fig. 9).

Thus, Snapchat effectively encourages minors to change their settings to a lower level of privacy, security and protection. vzbv considers this to be inconsistent with the guidelines of the European Commission.

One of Snapchat's main features¹³ is the Snap Map, an interactive map that shows the real-time locations of friends and allows users to discover public posts associated with specific places.

By default, users' location is not shared on Snapchat. However, location sharing can be enabled via the app's settings.¹⁴ When changing this setting, the operating system offers several options¹⁵, including when the location should be shared: "When using the app", "Only this time" or "Do not allow". If a user taps "Only this time", Snapchat opens a new pop-up in which the provider asks them to change location access to "Always allow". Snapchat justifies this on the grounds of an improved user experience.

Elsewhere it says: "Every step counts. Update location settings to get the most out of Footsteps and other features such as sharing with friends."

If the location is enabled, it is shared with Snapchat. Options such as "Share Live Location" (with friends) remain disabled (to enable this, "Always Allow" would need to be selected for location sharing) and "Ghost Mode" is enabled. This means that friends cannot see the location. If this mode is disabled, the location is shared with friends.

In the settings in the Map section, options such as "Friends can see your home", "Save new Footsteps as 'My Location' updates on the map" or "Friends can receive notifications about my last trip" are enabled by default. This suggests that as soon as a user's location is shared, these options are also enabled.

¹³ Displayed on the far left of the main controller on the screen.

¹⁴ In the settings under "Show my location" there is a yellow (eye-catching) button: "Activate" ("Activate your location so that friends can see your Bitmoji on the SnapMap"). If users tap it, a pop-up appears in which they can select "Allow" ("Allow" is more prominent than the "Do not allow" button).

¹⁵ There are also the options "Use exact device location" or "Approximate". The former is set by default.

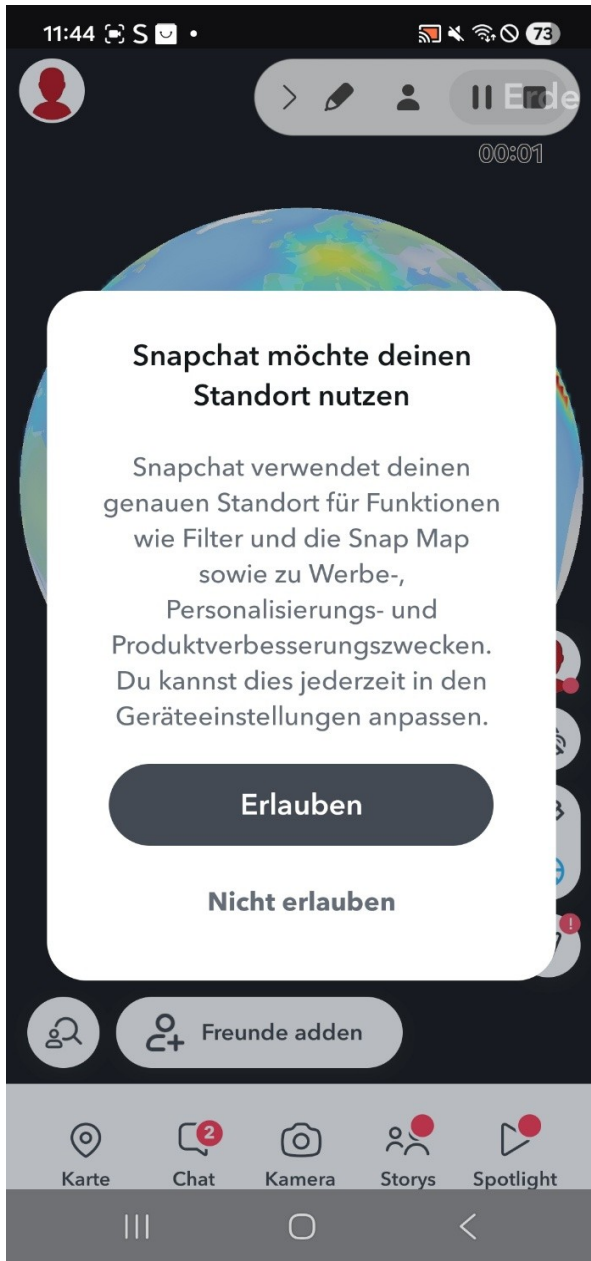


Figure 8: Snapchat requests location sharing.

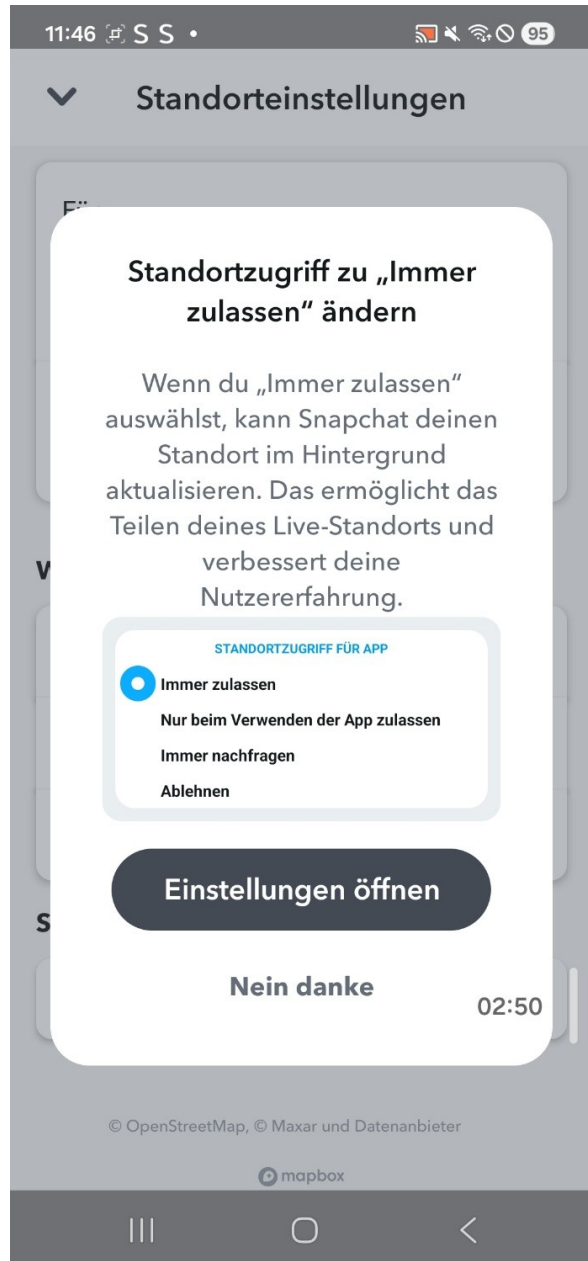


Figure 9: Snapchat is trying to get users to "always" allow location sharing.

5. Technical protection measures: content displayed

Children and adolescents can unintentionally come across problematic content on online platforms, which, in vzbv's view, could seriously harm their mental and physical health. Platform providers can counteract this by using appropriate technical solutions that reduce the risk of potentially harmful content being displayed or recommended to underage users.

For example, the platforms examined sometimes rely on technical protection measures to filter out content that is unsuitable for minors.

Example TikTok

TikTok includes a so-called "restricted mode", which restricts content "that may not be appropriate for all audiences" (see Fig. 10).

In the test, however, this mode was disabled by default. This raises the question of why this is the case for a minor's account and who this mode is actually intended for.

Also striking: If a user would like to activate the restricted mode as a 13-year-old, TikTok even asks for a reason (see Fig. 11).

In vzbv's view, this runs counter to the European Commission's guidelines on default account settings. The guidelines call on providers to activate the highest level of data protection, security and safeguards for minors' accounts through default settings.

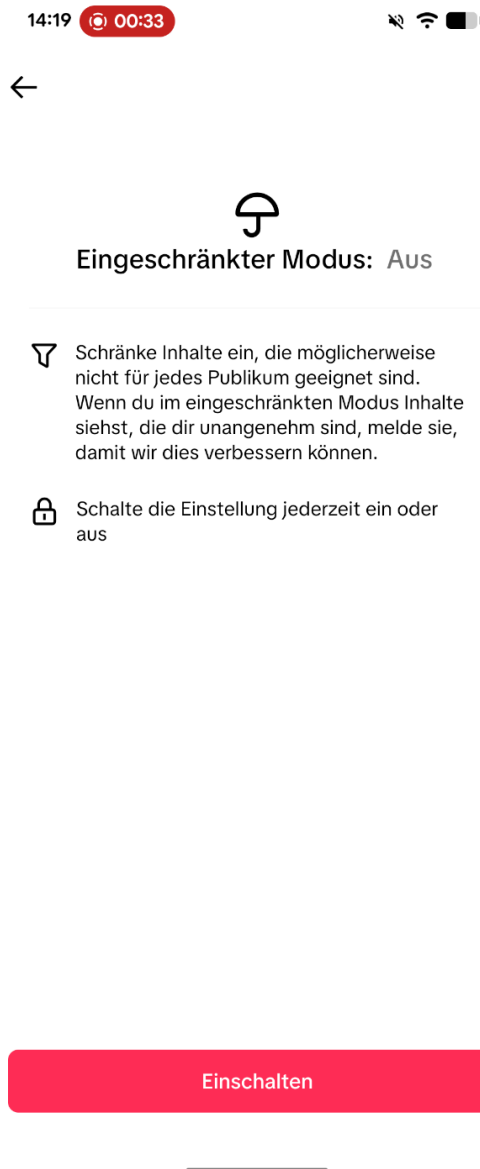


Figure 10: On TikTok, restricted mode is switched off by default.

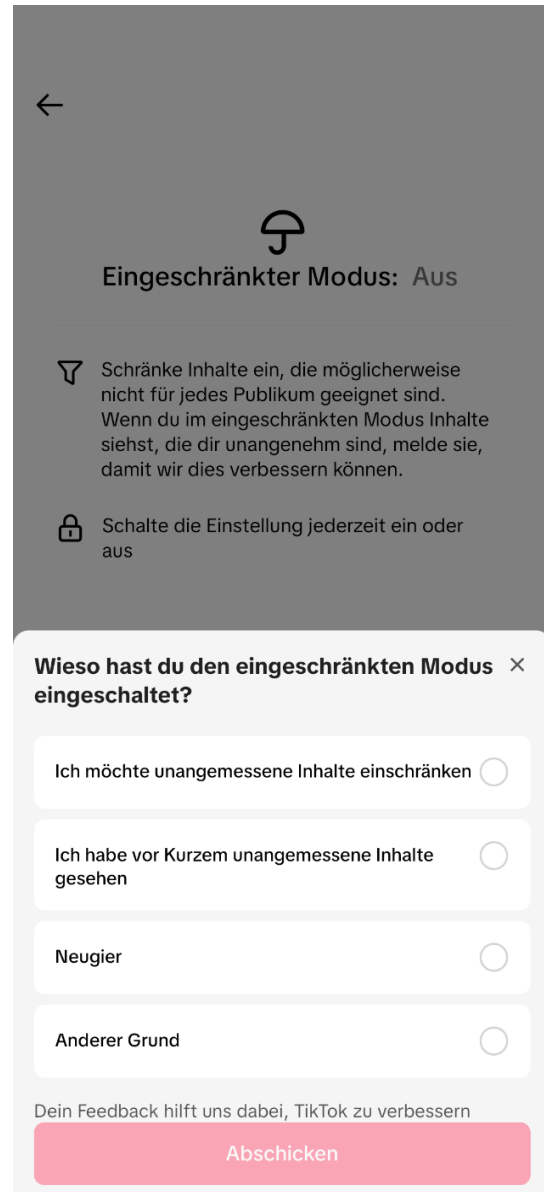


Figure 11: If a user enables restricted mode on TikTok, it asks for a reason.

6. Time limits/limitation of the duration of use

Built-in time management tools can help children and teens develop a better sense of how much time they spend on online platforms. They should be tailored to the needs of minors and help them to reduce the amount of time they spend online.

On four of the five platforms examined, time limits for app usage are set by default (see Figs. 12 and 13). However, such reminders can sometimes simply be ignored or dismissed (see Fig. 14).

Example Facebook

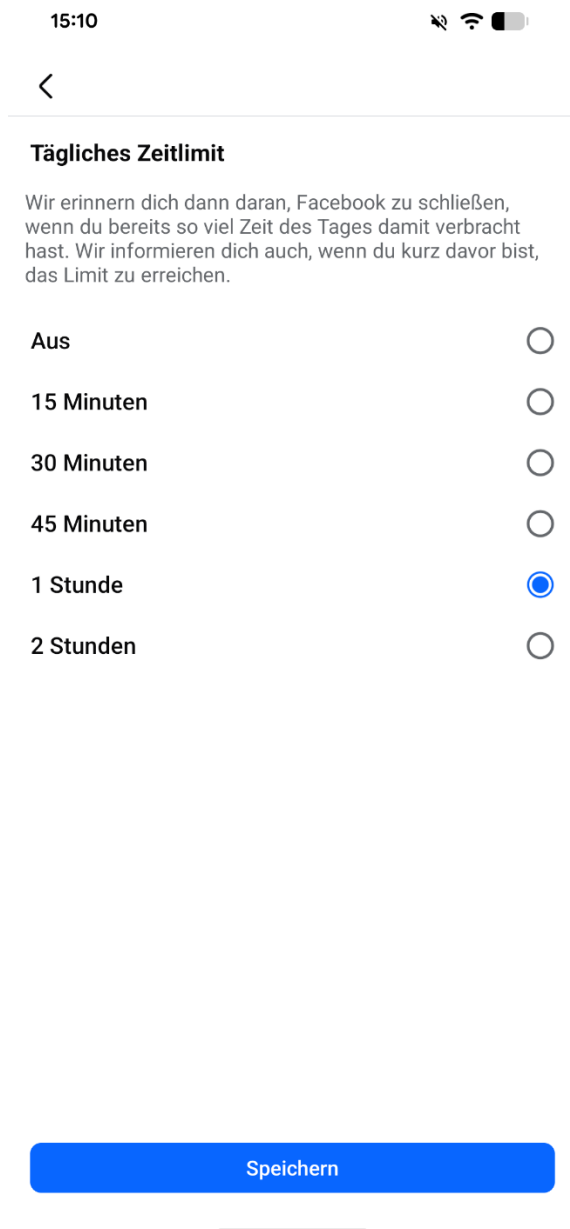


Figure 12: Facebook has a default daily time limit of one hour.

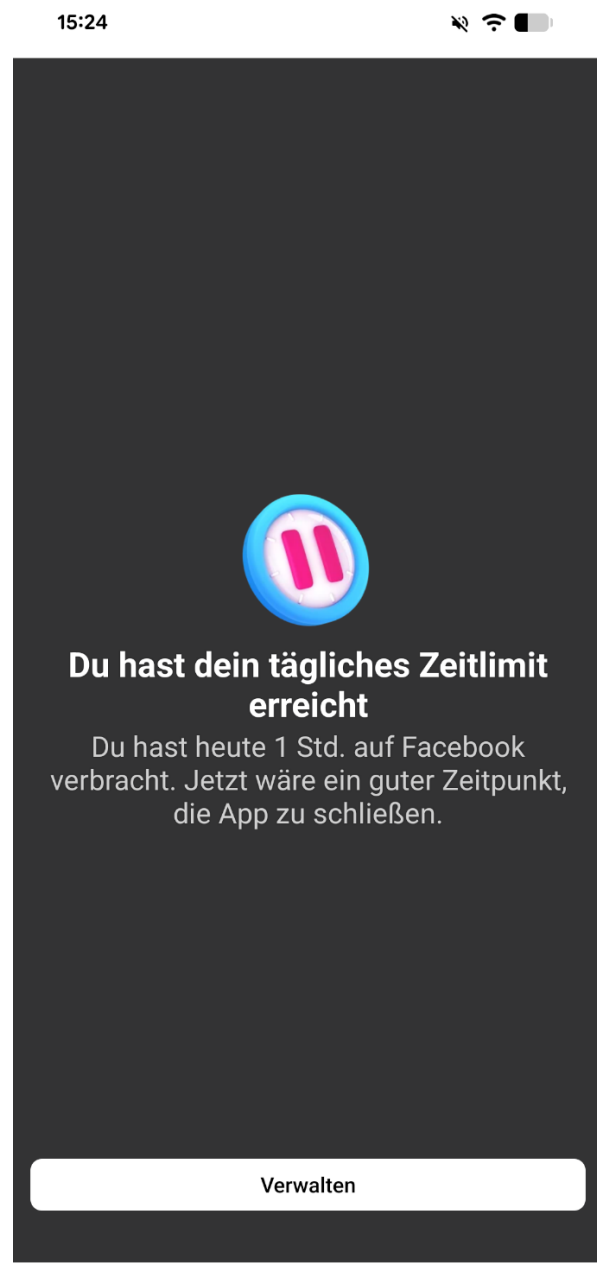


Figure 13: Facebook displays a notification after reaching the daily time limit.

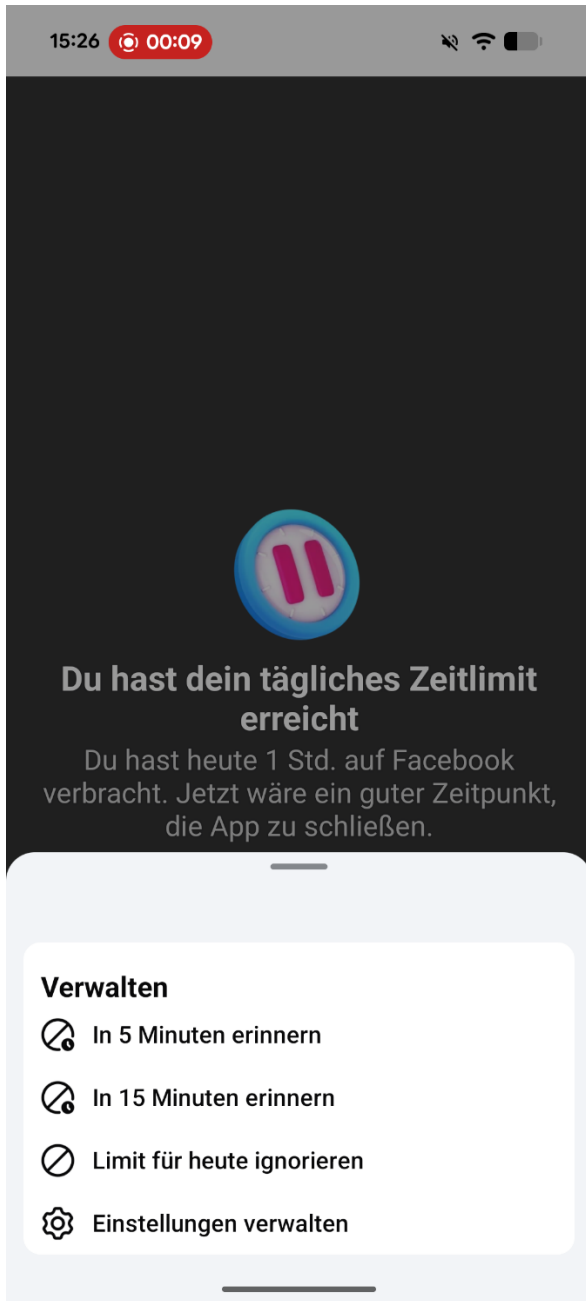


Figure 14: The option "Ignore limit for today" can be used to close the message from Facebook.

Likewise, the apps examined sometimes have pre-set bedtime reminders or notification breaks during certain times of the day.

One striking feature on YouTube is that bedtime for teenagers apparently ends as early as 5.00 am (see Fig. 15). On Facebook, it ends at 7.00 am (see Fig. 16).

In vzbv's view, the existing time management tools do not adequately meet the guidelines, as they are easy to circumvent and do not effectively limit usage time.¹⁶

¹⁶ See para. 61 of the European Commission's guidelines.

Examples: YouTube and Facebook

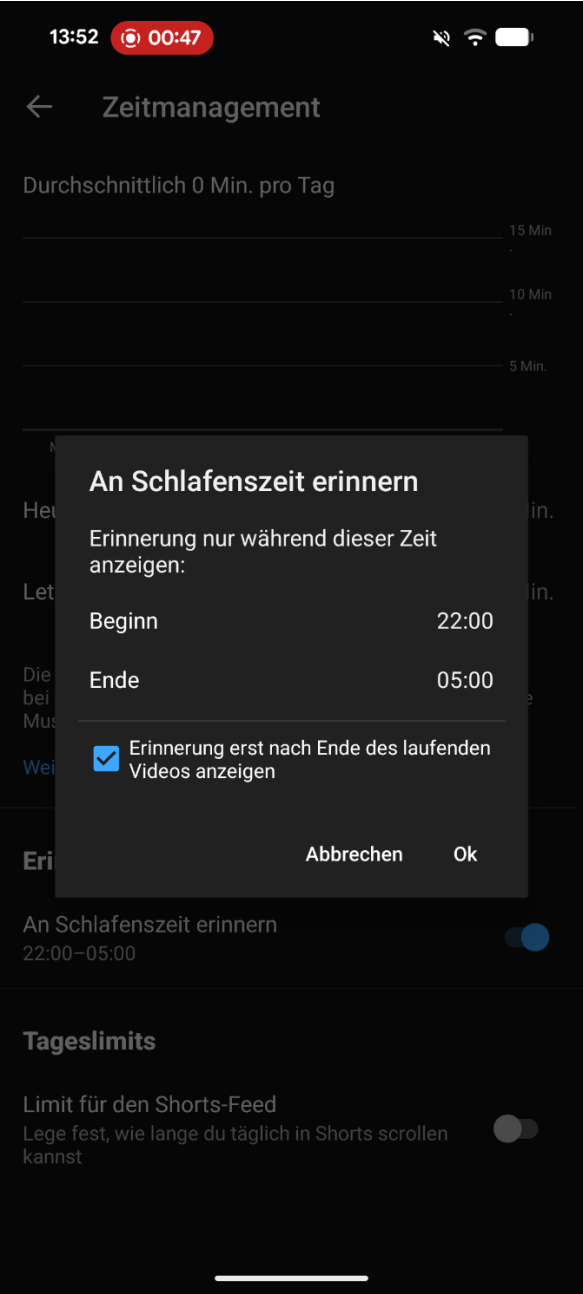


Figure 15: YouTube had set a default bedtime of 10:00 p.m. to 5:00 a.m. in the test.

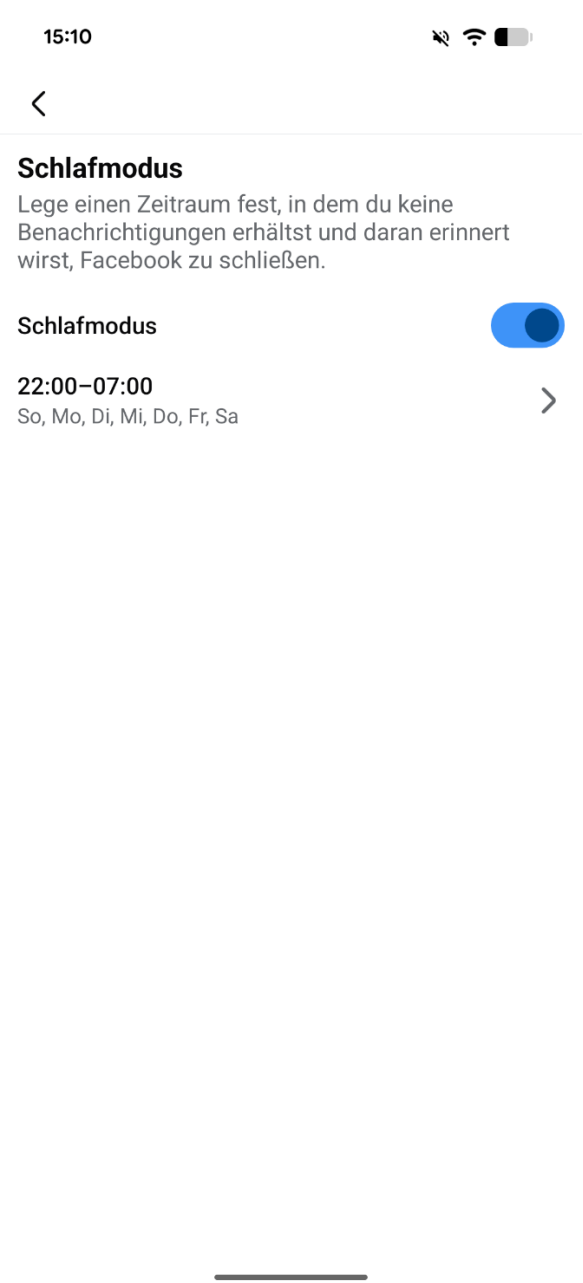


Figure 16: Facebook had set a default sleep mode from 10:00 p.m. to 7:00 a.m. in the test.

7. In-app purchases

Children and adolescents may be particularly vulnerable to making impulsive purchases on platforms as their understanding of money and economic consequences is still developing. Without appropriate protection mechanisms, they could easily be exploited financially, for example through in-app purchases – in vzbv’s view, this contradicts the guidelines of the European Commission.¹⁷

Of the platforms examined, Facebook and Snapchat display paid offers (monthly or annual subscriptions) to minors within the app (see Figs. 17, 18 and 19).

In addition to other means of payment such as credit cards, Facebook, for example, also allows payment with credit purchased in the Google Play Store (see Figs. 20 and 21). Snapchat uses manipulative design by specifically highlighting the annual subscription.

Examples: Snapchat+ and Facebook Fan Subscriptions



Figure 17: Premium features with a Snapchat+ subscription.

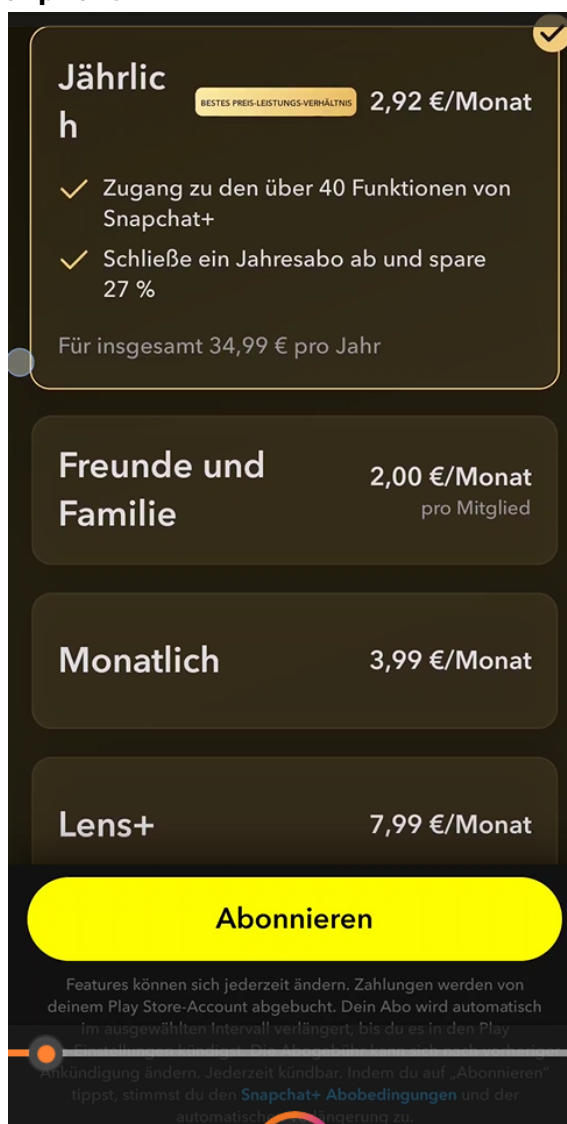


Figure 18: Pre-selected and highlighted annual membership.

¹⁷ See para. 68/69 of the European Commission's Guidelines.

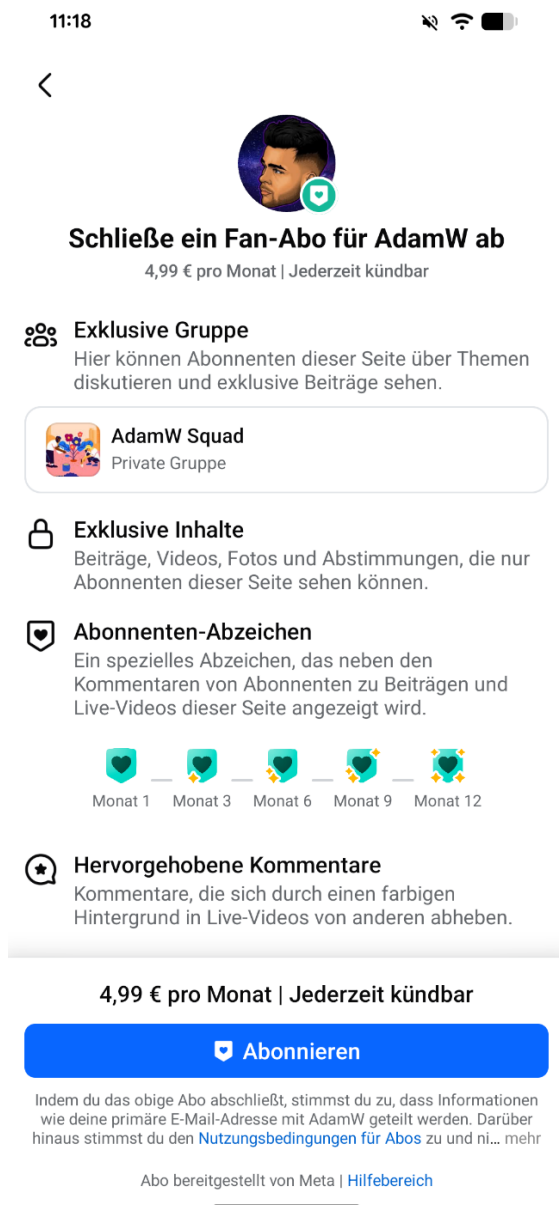


Figure 19: On Facebook, minors can purchase fan subscriptions for 4.99 euros per month.

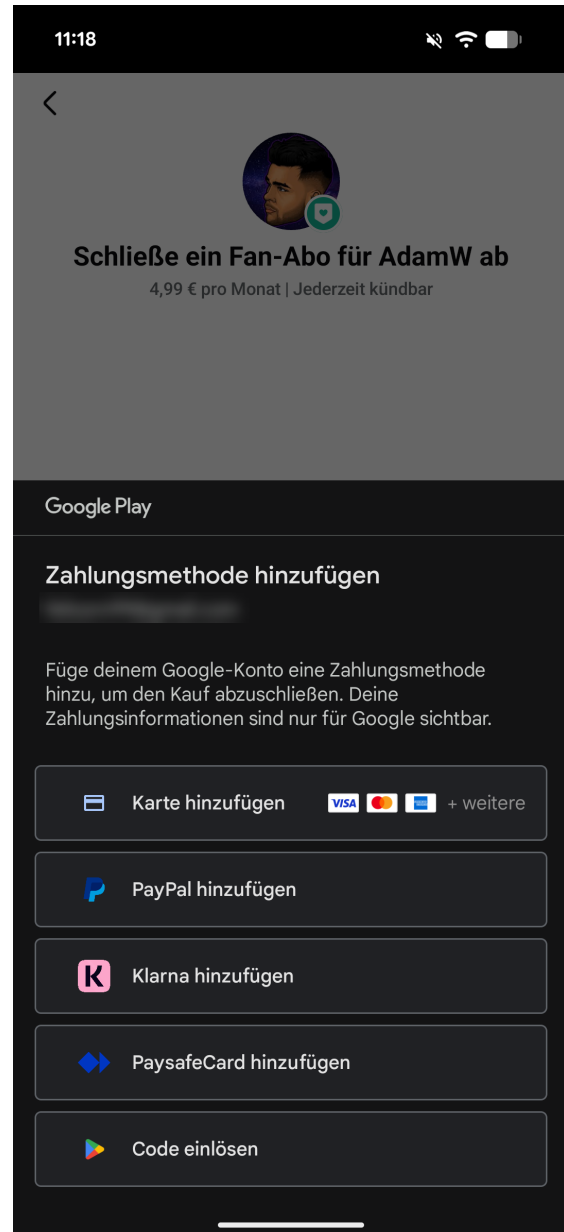


Figure 20: Fan subscriptions on Facebook can be paid for with Google Play codes, among other things.

11:30 00:24

×

Karte hinzufügen

Deine Kartennummer wird verschlüsselt und sicher gespeichert

Kartennummer

MM/JJ

Kartenprüfnumme...

USA ✓

Vollständiger Name

Adresse

Adresszeile 2 (optional)

Stadt

Speichern

Diese Angaben werden bei Meta Pay gespeichert und in der Kontenübersicht synchronisiert. Dort kannst du sie auch verwalten. [Mehr dazu](#)

Figure 21: Credit card details for Meta Pay can be saved in the Facebook test account.

8. Personalised advertising

Many online services systematically collect usage data across different websites, apps and devices and combine them into comprehensive profiles of users' personalities and interests. These profiles form the basis for personalised advertising, among other things. In vzbv's view, these practices are particularly problematic for children and adolescents, as they often cannot understand how tracking and data-based personalization work and are hardly in a position to assess the long-term consequences of such data use. The DSA recognises this and, in Article 28 (2), expressly prohibits providers from displaying personalised advertising aimed at minors on online platforms.

In some cases, the platforms examined provide contradictory and unclear information about personalised advertising. According to their own statements, two providers do not display any advertising at all to minors (Instagram) or do not display personalised advertising to them (YouTube). These two providers' apps also do not offer any settings relating to advertising. In the case of TikTok, it remained unclear in the test how the provider handles personalised advertising. No information was found within the app, and the settings for advertising were very limited.

Example Facebook

No adverts were displayed in the test account on Facebook. Nevertheless, the app contains detailed settings regarding users' advertising preferences, which can be changed by underage users themselves (see Fig. 22).

Strikingly, several data categories are selected by default, on the basis of which advertisements could be shown to underage users, for example relating to their relationship status or employer (see Fig. 23).

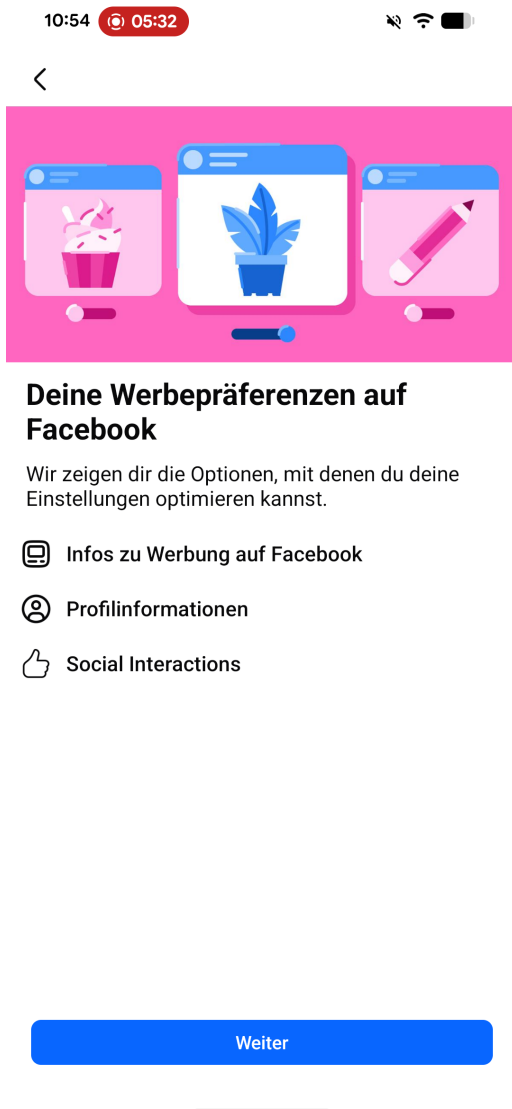


Figure 22: Facebook offers settings for advertising preferences.

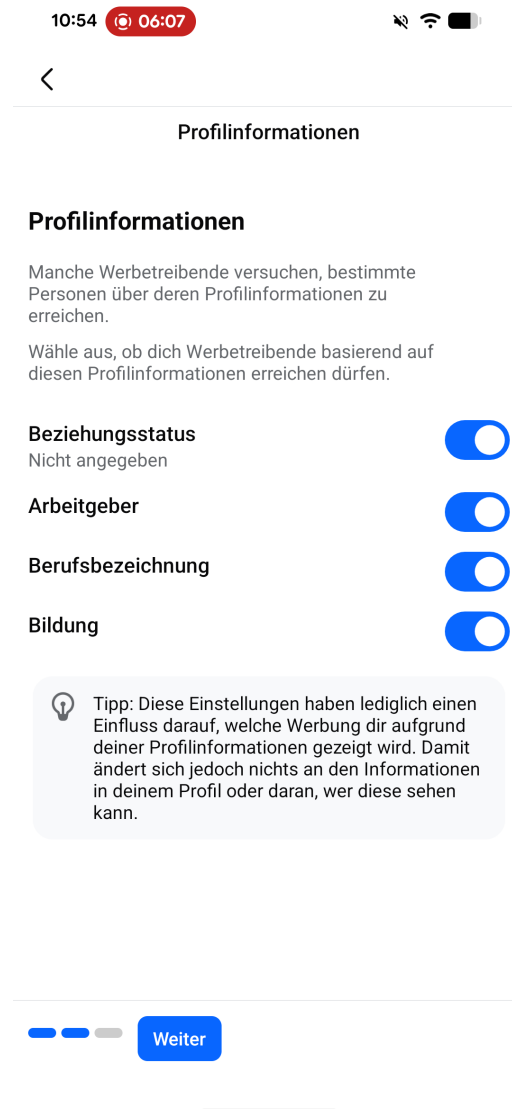


Figure 23: On Facebook, categories such as "relationship status" or "employer" are selected by default in the advertising preferences.

Example Snapchat

Although Snapchat states¹⁸ that people under the age of 18 are generally excluded from audience-targeted advertising, activity-based ads and third-party ad networks, and while settings for this are automatically disabled, all available types of data processing for advertising purposes (audience-targeted, based on other activities, third-party networks) are nevertheless enabled by default (see Figures 24 and 25).

The ad settings are similarly confusing: Snapchat states that it only uses interest categories to create adverts for specific target groups for users aged 18 and over, and that age restrictions apply

¹⁸ "If you are under the age of 18 and are based in the EEA or the UK, you will be automatically excluded from audience-based ads, activity-based ads, and third-party ad networks, regardless of what you have selected in the app."

to ads regardless of the settings selected (see Fig. 26).¹⁹ Nevertheless, all the ad categories on offer can be selected and enabled. These include the ad categories “alcohol” and “gambling”, which are unsuitable for children and adolescents (see Fig. 27).²⁰

It remained unclear to what extent the ad categories have an influence on the adverts displayed. During the test, adverts were displayed to underage users on Snapchat (a Rewe ad for apprenticeships) (see Fig. 28).²¹ According to Snapchat, the ad was displayed based on the “specified or assumed age group”. This could be interpreted as advertising based on personal data and, in vzbv’s view, would constitute a potential violation of Art. 28 (2) DSA.

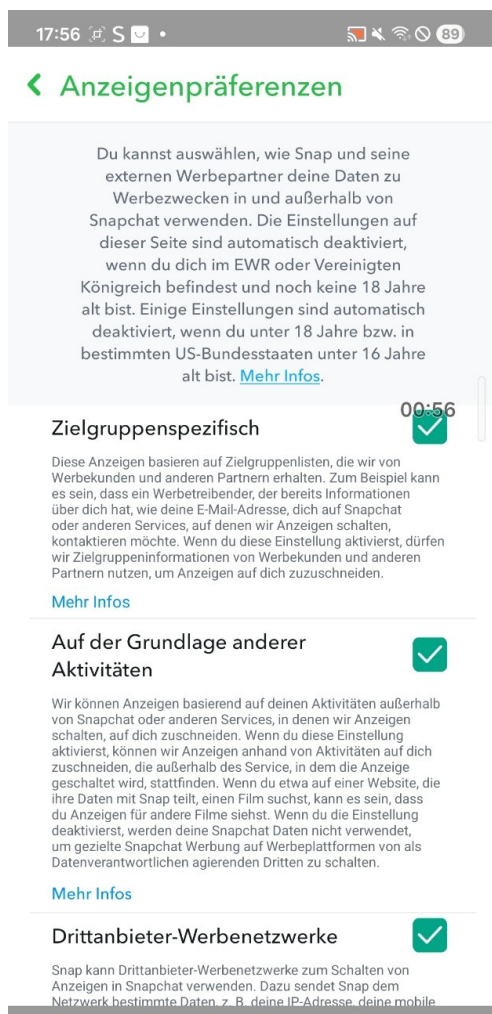


Figure 24: Confusing advertising settings: Although Snapchat states that the settings shown are disabled, they are actually selected.

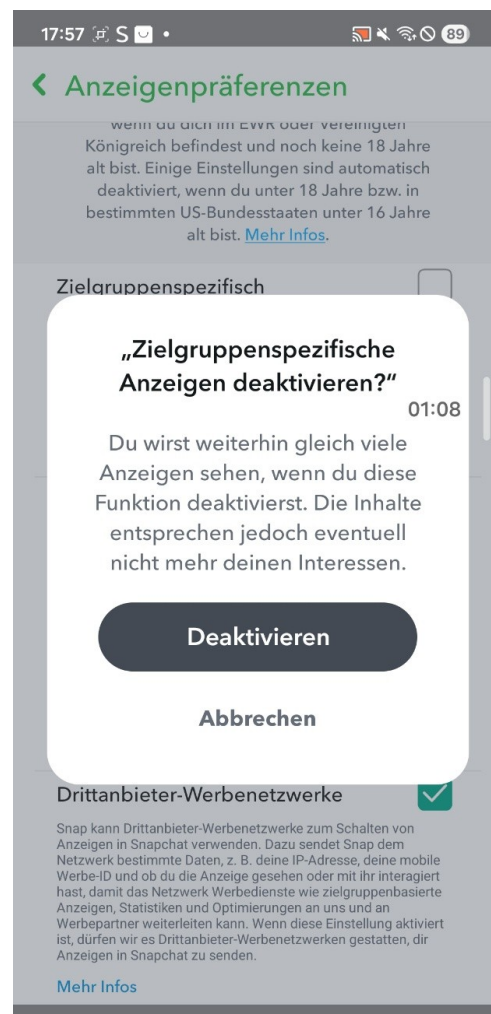


Figure 25: When attempting to disable ad preferences, a message appears stating that adverts will still be displayed – though they may be “less” interest-based.

¹⁹ "We use lifestyle categories to target adverts at specific audiences (except for users under the age of 18 in the EU and the UK). Regardless of these settings, the ads you see are subject to Snap’s advertising policies, which include, but are not limited to, age restrictions on ads that depict alcohol and gambling."

²⁰ No adverts containing this content were identified during the test.

²¹ Apart from Snapchat, YouTube was the only other platform on which adverts were shown during the test.

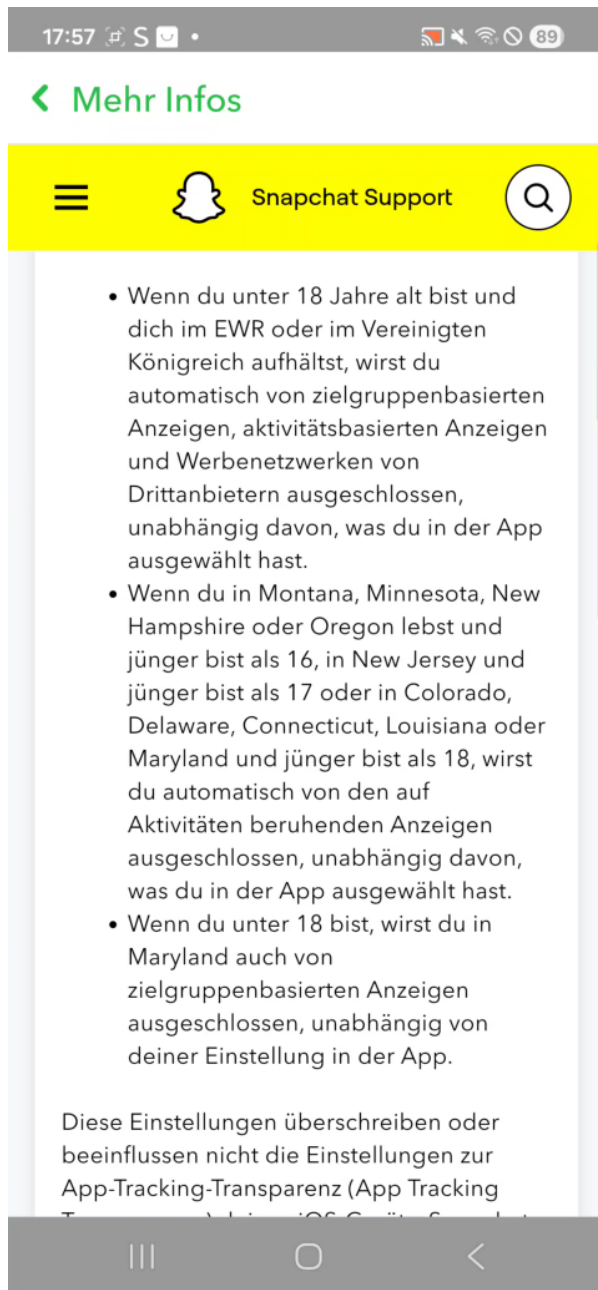


Figure 26: In its privacy section, Snapchat states that, regardless of the ad preferences selected, no targeted adverts are displayed.

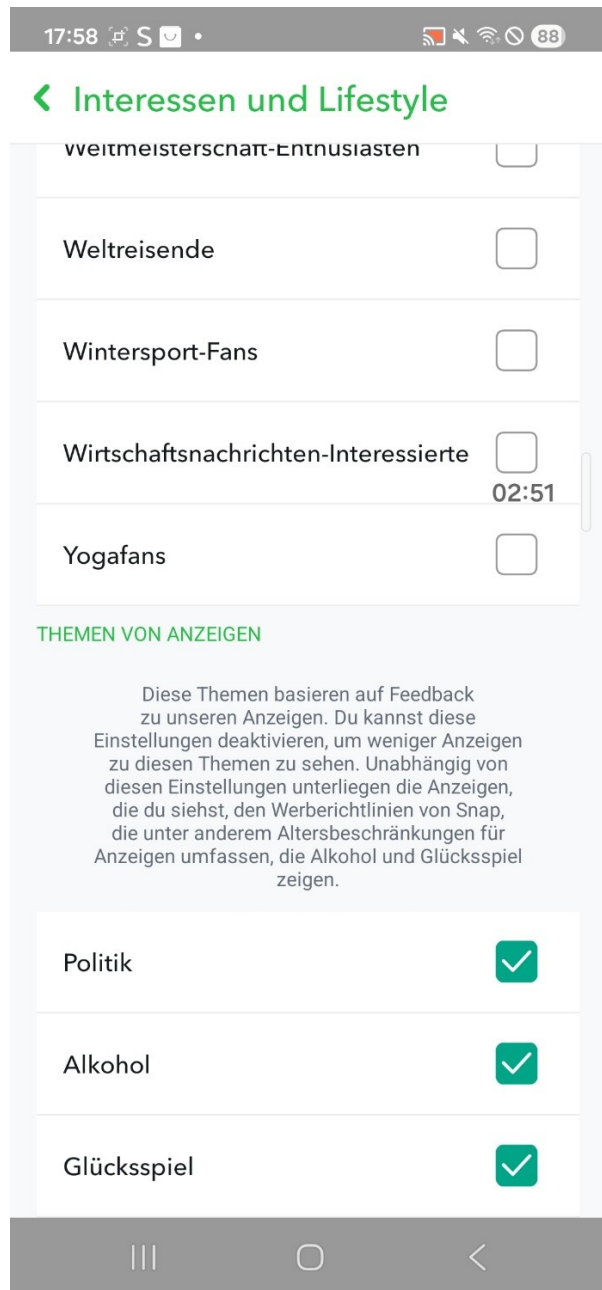


Figure 27: Snapchat states that age restrictions apply to ads regardless of the settings made. However, the ad categories "alcohol" and "gambling", which are unsuitable for children and adolescents, are pre-selected.



Figure 28: Advertisement shown to minors during the test.

9. Manipulative and potentially addictive design elements

Many digital applications deliberately use manipulative and addictive design elements to maximize attention and usage time.²² These "dark patterns" can undermine self-determination by removing natural stopping points, creating reward loops and thus fostering a loss of control and addiction-like usage behaviour. Children and adolescents are particularly at risk because their self-regulatory abilities and reward systems are not yet fully developed and they often do not consciously recognize manipulative patterns.

In vzbv's evaluation, all five platforms examined expose their underage users to manipulative design features that can lead to extensive or excessive use of the platform or compulsive behavioural patterns. vzbv considers this to constitute possible violations of Art. 28, the associated guidelines and Art. 25 DSA.²³

9.1 Autoplay, Infinite Scroll und Pull-to-Refresh

Autoplay²⁴, infinite scroll²⁵ and pull-to-refresh²⁶ are used as design elements by all five platforms examined – particularly in the short-form video feeds, which represent a fundamental part of the services offered by all five platforms (for example, Instagram Reels, Snapchat Spotlight or YouTube Shorts).

In vzbv's view, these mechanisms can create a pull that makes it difficult for users to quit. This can lead to unintentionally longer usage times. According to the guidelines of the European Commission, the autoplay function, in particular, should be disabled by default for children and adolescents. The tested providers do not comply with this.

9.2 Push notifications

The platforms sometimes send push notifications several times a day to encourage users to return to the app – in some cases using wording that appears manipulative and is designed to tap into the "Fear of Missing Out" (FOMO) (see Figs. 29 and 30). According to the European Commission's guidelines, push notifications that have been deliberately enabled should only inform users about interactions that result from direct contacts or interactions. The notifications received during the evaluation raise significant doubts about this and rather suggest that the platforms are not complying with this requirement.

²² Cf. Verbraucherzentrale Bundesverband e.V. (Federation of German Consumer Organisations): Manipulative designs on online marketplaces and social media platforms. Evaluating the implementation of Article 25 of the Digital Services Act (DSA), January 2025, [online] https://www.vzbv.de/sites/default/files/2025-11/25-01-15_MB-Report_Manipulative_designs.pdf.

²³ See para. 61 b) of the European Commission's Guidelines.

²⁴ Videos start automatically without having to click.

²⁵ New content keeps being added, with no apparent end in sight.

²⁶ A vertical swipe gesture on the touchscreen of the smartphone refreshes the content. The swipe gesture is often accompanied by haptic feedback and a brief loading sequence. This mechanism is strongly reminiscent of a slot machine.

Examples: TikTok and Facebook



Figure 29: TikTok sends push notifications with phrases like "Just for you, [username]" or "245K+ people have seen this."



Figure 30: Facebook sends push notifications with phrases such as "[username]: You have 11 photos" or "Waiting for you: 1 new reel"

9.3 Manipulative requests to access sensitive features

Access to features such as the camera and microphone in digital services and apps can pose significant risks of abuse. Children and adolescents can thereby disclose intimate information that could be used by third parties for harassment, surveillance or grooming. Minors, in particular, are often not yet able to assess the consequences of granting access to sensitive features or to defend themselves against their potential misuse.

The platforms examined repeatedly request users to grant access to, for example, their location, phone contacts or camera, or to authorise push notifications. In some cases, this is done using manipulative designs and wording.

With these requests, platforms entice minors to change their settings to a lower level of privacy, security, and protection. In vzbv's view, the platforms concerned do not implement the relevant requirement, which is explicitly mentioned in the European Commission's guidelines.²⁷

Example Facebook

Facebook asks its users to grant access to their phone book contacts as early as during the registration process. The "Activate" button is highlighted in a striking blue, while the "Not now" button is coloured grey (see Fig. 31).

Notably, clicking on 'Not now' brings up a pop-up asking, 'Are you sure you want to skip this step?' (see Fig. 32). In this way, Facebook once again challenges, in a persuasive manner, the decision the user has just made. Here, too, the 'Import contacts' option is highlighted in a striking blue colour, in contrast to the 'Skip' option.

²⁷ See para. 61 b) of the European Commission's Guidelines.

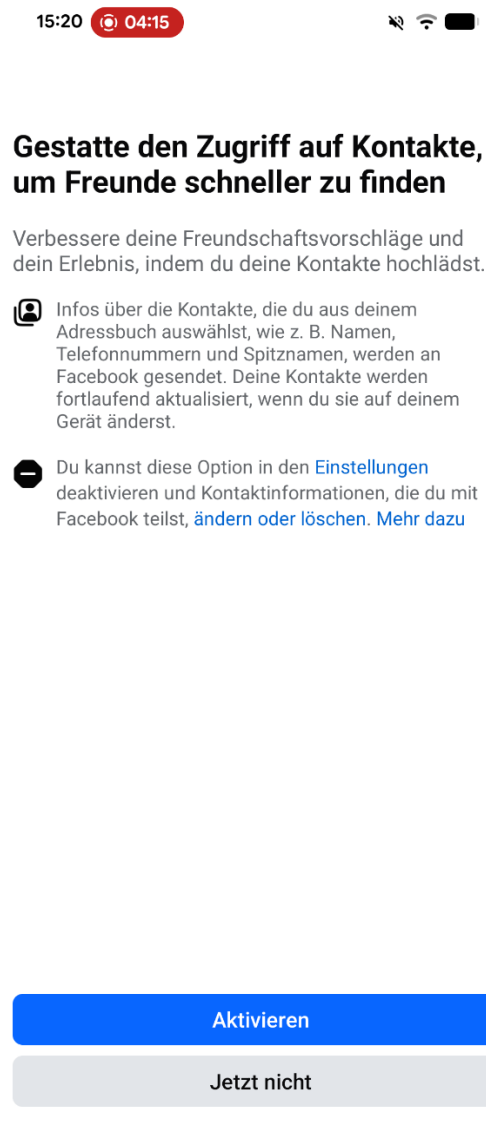


Figure 31: Facebook prompts users to import their phone book contacts with a conspicuous blue button.

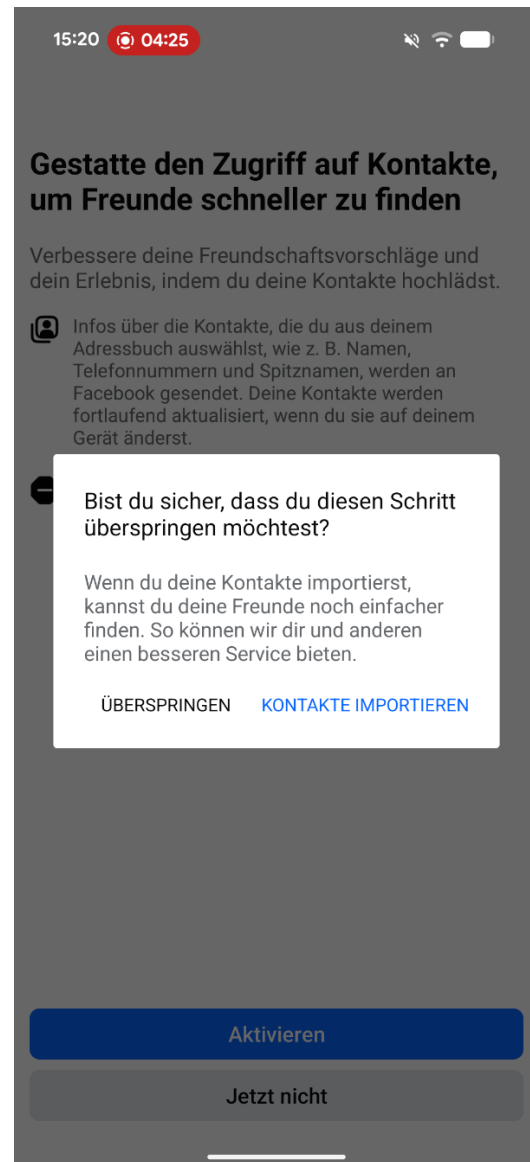


Figure 32: Facebook questions the user's decision not to import phone book contacts.

Example Snapchat

On the grounds of simplifying the registration process, Snapchat aims to ensure that users grant the app permissions as early as the registration stage ("Tap 'Allow' when prompted") (see Fig. 33). In addition, Snapchat is very clearly presented as a "camera app" in order to obtain permission to access the camera. At the same time, the app prompts users to add it to their lock screen (see Fig. 34). This can result in unauthorised people also having access to the Snapchat camera (as Snapchat itself points out).

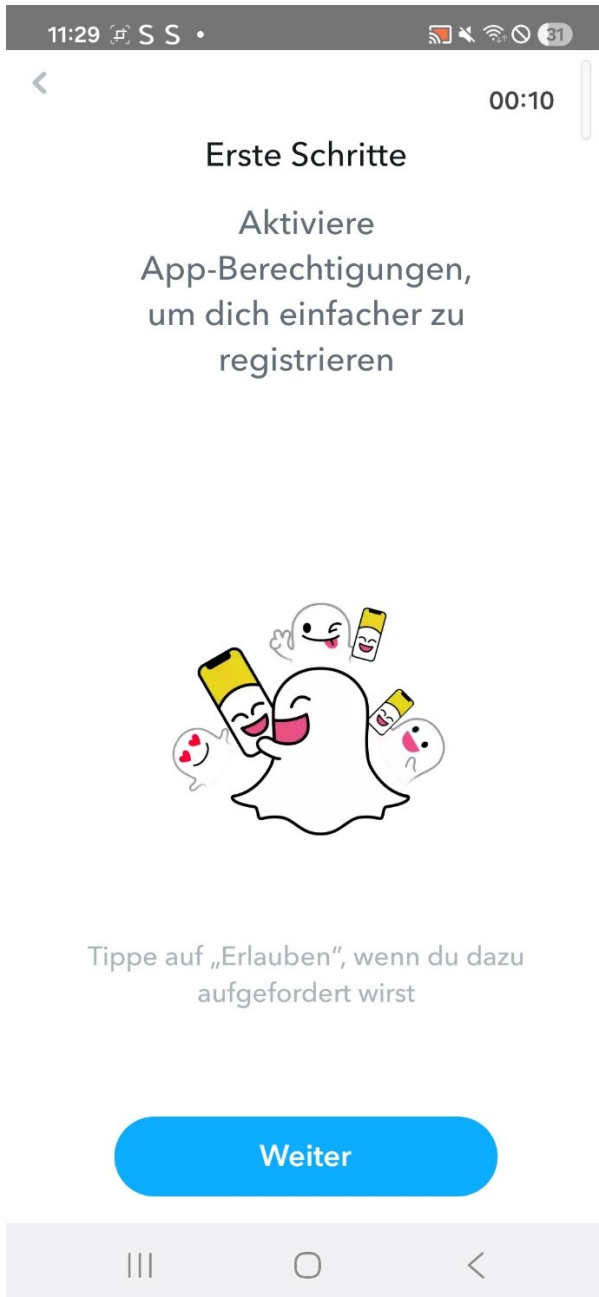


Figure 33: Snapchat aims to get users to grant permissions right from the registration stage, on the grounds that this simplifies the registration process.

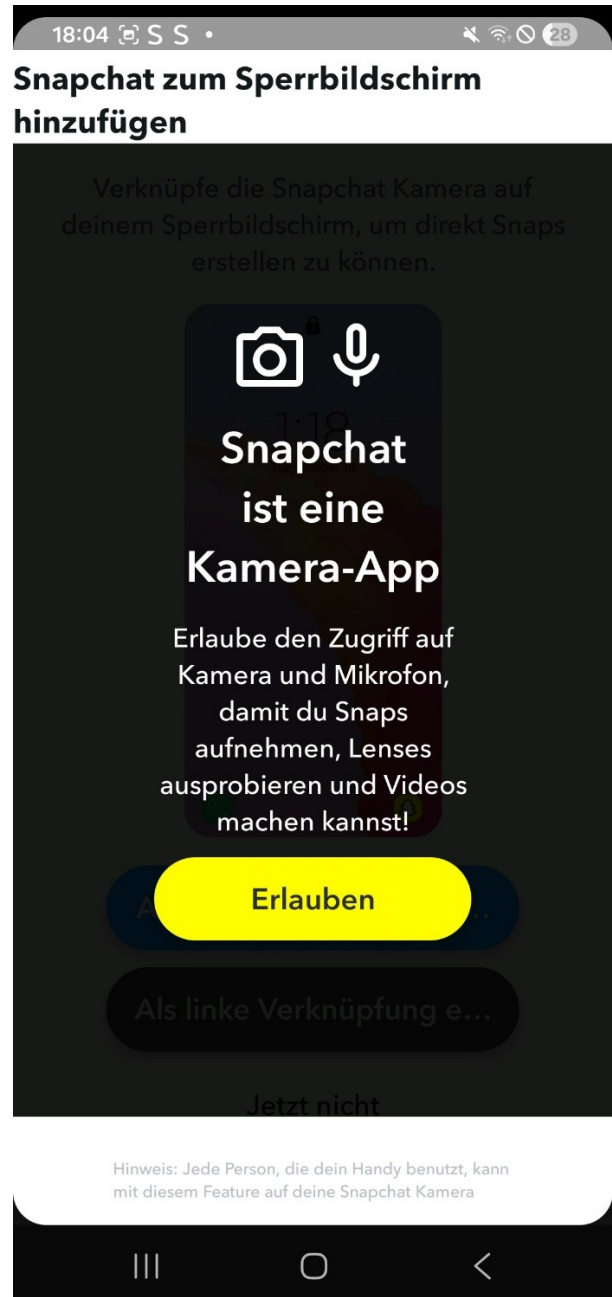


Figure 34: Snapchat is presented as a "camera app" to get permission to access the camera. At the same time, the app is asking to be added to the lock screen.



Figure 35: A cute illustration for a feature with consequences: Snapchat is asking users to share their contacts.

9.4 Gamification and reward systems

Example Snapchat

Whether it's Snap Scores, Streaks, Bitmoji or creating custom countdowns: Snapchat has a range of features which, in vzbv's view, are potentially addictive, designed to keep users on the platform for longer or maximise their interactions. This can lead to addiction-like behaviour.

The value of the "Snap Score" increases when friends and groups view a user's "Snaps" (photos or videos) or vice versa. Anyone who sends 'Snaps' to their friends every day earns a Streak, indicated

by a flame emoji in the messages section.²⁸ The flame is a veritable status symbol. If it “goes out”, users can pay to restore the Streak (see Figs. 36 and 37).

“Bitmojis” are available to customise or personalise user profiles. These are avatars that users can design, much like a character in an online game (see Fig. 38).

Features like these can encourage users to open the app every day and spend more time on it, as well as to make in-app purchases.

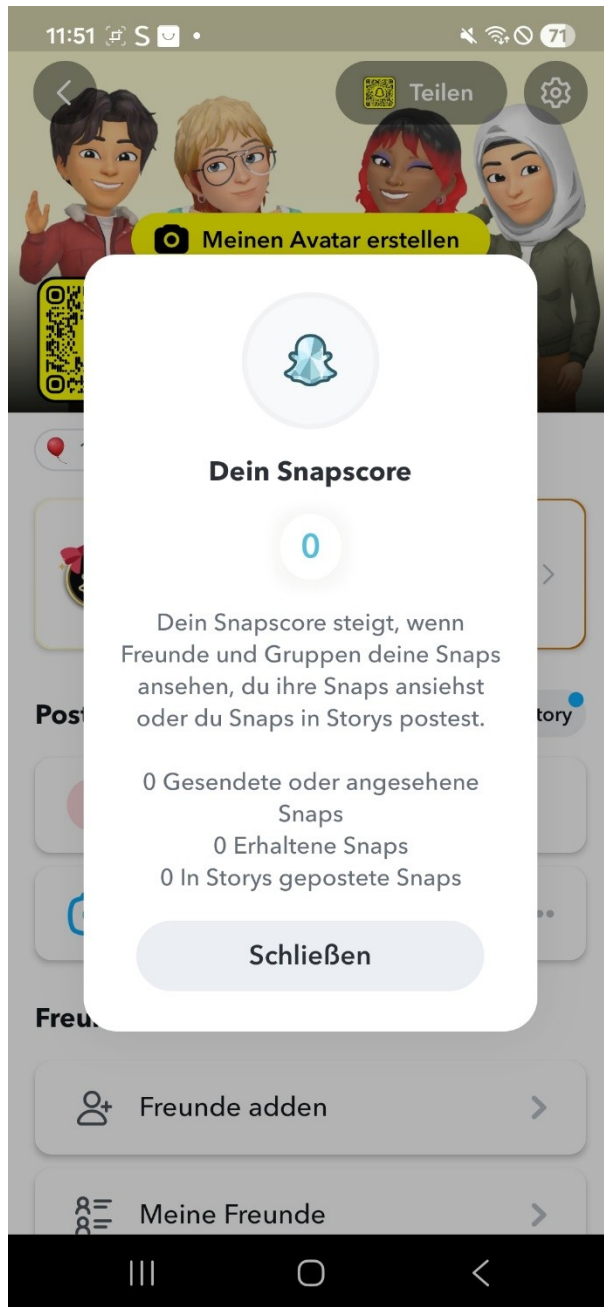


Figure 36: Wants to motivate users to interact on the platform: The “Snap Score”.

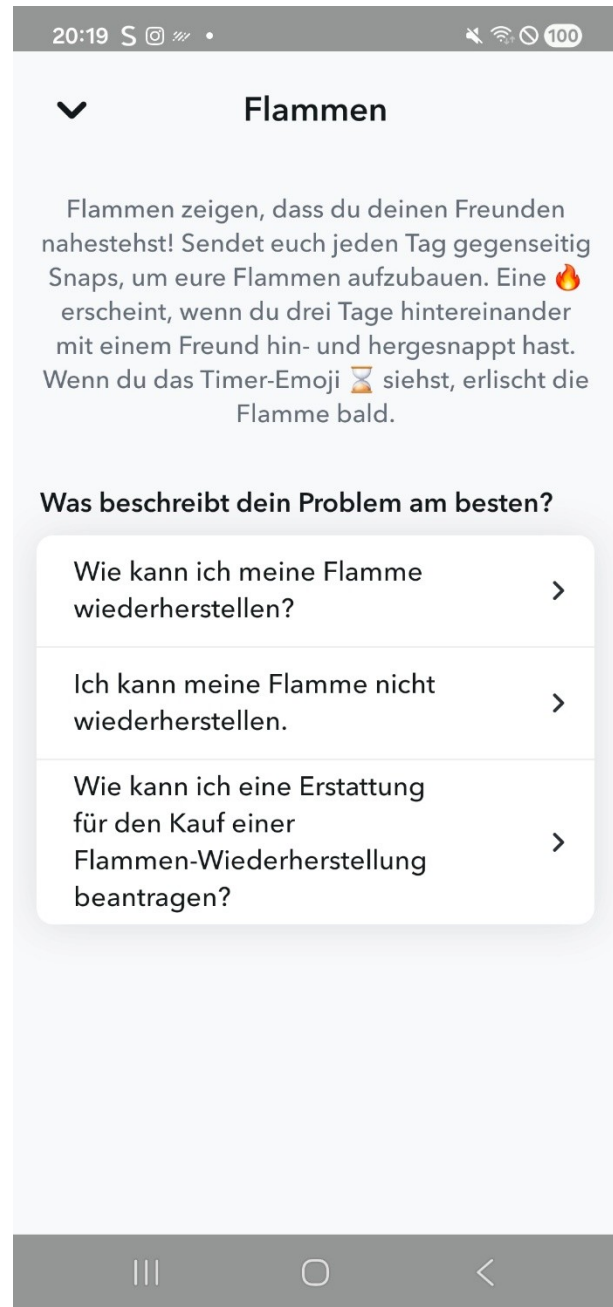


Figure 37: Can tempt you to visit the app at least daily: The Streak.

²⁸ <https://help.snapchat.com/hc/de/articles/7012394193684-Wie-funktionieren-Flammen-und-wann-laufen-sie-ab>



Figure 38: Personalised avatars are designed to keep users engaged with the app.

10. Algorithmic recommender systems

Recommender systems determine which content is given particular prominence on the platforms and displayed to users in their feeds. This also applies to underage users. As a result, providers exert a significant influence on the content, people or behaviours that children and teenagers are exposed to on their platforms. (AI-driven) recommendation and personalisation algorithms also aim to maximise the time spent on the platforms. Due to the way they operate, they pose significant risks to the mental health and development of children and adolescents.²⁹

In Articles 27 and 38, the DSA requires very large online platform providers, amongst other things, to provide easily accessible choices within their recommender systems and to offer at least one option that is not based on profiling.

All five platforms examined offer underage users various options within their apps for displaying feeds. However, in vzbv's view, these options are not always directly and easily accessible. All apps feature one or more specific feeds that are presumably not based on profiling. The option without profiling is not enabled by default on any of the five platforms examined. Minors are therefore always shown personalised feeds by default on the apps' home screens.

In three of the five apps examined (Snapchat, TikTok and YouTube), profiling can be disabled via relevant options in the app settings or in individual posts.

Example TikTok

In the test account, it was possible to disable the personalisation of feeds³⁰ in the TikTok app. To do this, users must actively search for the relevant setting and find it either in the app menu under "Settings and Privacy" or in the context menu of an individual video under the heading "Manage Feeds". There, the "Personalised Feeds" function can be deactivated using a button or a slider (see Fig. 44). The "For You" feed is then renamed "Popular" and apparently no longer displays personalised content. However, in vzbv's view, this option is not directly or easily accessible.

²⁹ See the studies in the chapter "Relevance for consumers".

³⁰ On the TikTok app's home screen, underage users can choose between four different feeds ("STEM", "Discover", "Followed", and "For You"). By default, when opening the app, the personalised "For You" feed is always displayed.



Figure 39: On TikTok, personalised feeds can be deactivated in the app via a slider.

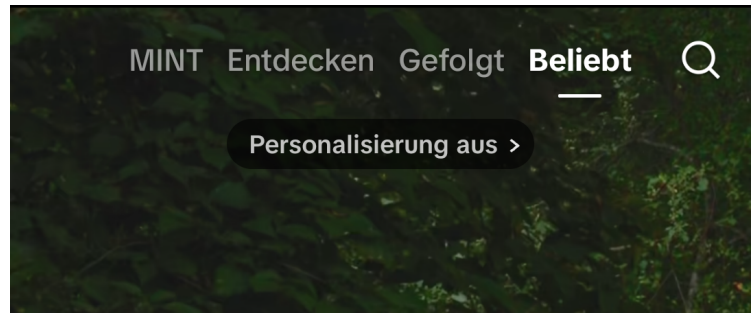


Figure 40: TikTok displays a message when personalisation is disabled.

It is striking that, if personalisation is switched off in the TikTok app, a reminder in the form of a pop-up labelled “Personalisation off” appears for a few seconds every time the feed on the home screen is refreshed (see Fig. 45). Tapping on it takes you directly to the settings where personalised feeds can be reactivated.

Users are therefore constantly reminded that personalisation is currently switched off in the app, as if this state were not actually intended by TikTok. If users find the recurring notification annoying and wish to hide it permanently, they have no choice but to re-enable personalisation. This is because no comparable notification is displayed when personalisation is enabled.

In vzbv’s view, this constitutes a “dark pattern” that may deter users from permanently disabling personalisation.

Example YouTube

If users wish to disable personalised feeds³¹ on YouTube, they must deactivate “YouTube History” (comprising their personal watch and search history) in the app settings (see Fig. 46). If necessary, they may also need to delete any previously saved history.

Afterwards, no videos will appear on the app’s home screen. There will then be virtually no feed in that space (see Fig. 47). Only a message will appear stating that the user can reactivate their history.

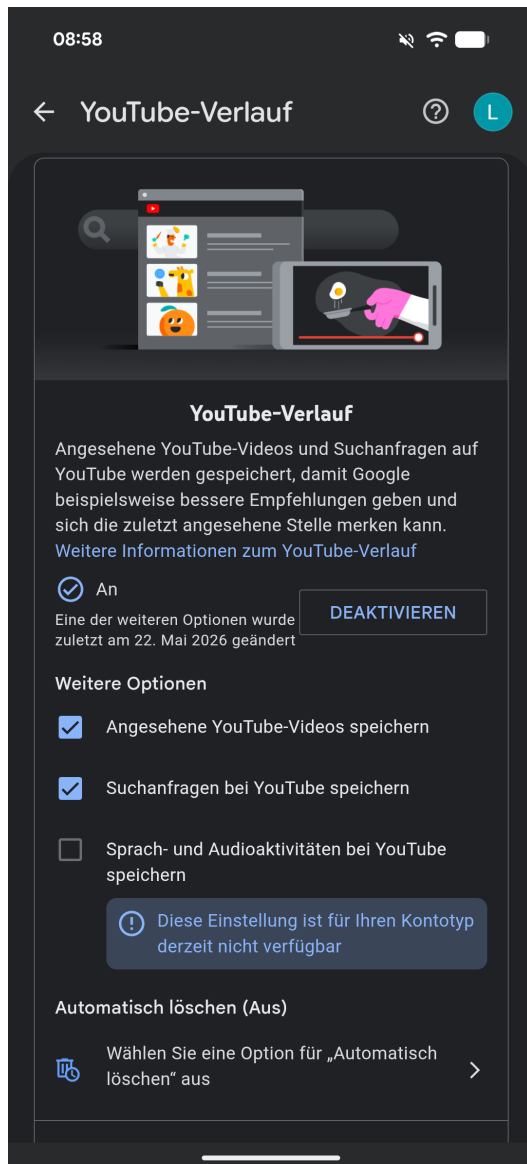


Figure 41: In the YouTube app, the so-called “YouTube history” can be deactivated.

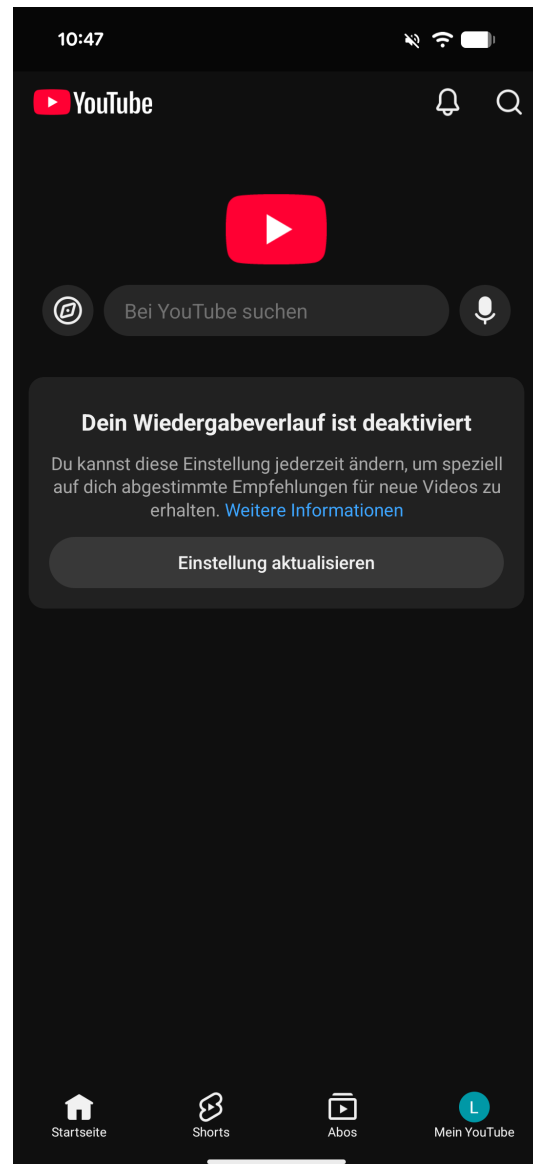


Figure 42: After disabling YouTube history, videos are no longer displayed on the app’s home page.

³¹ The YouTube app has three sections with different feeds: “Home”, “Shorts”, and “Subscriptions”. When opening the app, a personalised feed is displayed on the home screen by default.

It remains unclear how turning off YouTube history will affect other parts of the app. This is because YouTube's explanations only refer very vaguely to "possibly fewer recommendations" or "Your recommendations will be reset, but may still be influenced by activity linked to other Google products". Or: "If you pause your YouTube history, personalised features across Google services may be limited or disabled." This wording suggests that it may not be possible to switch personalisation off completely within the YouTube app.

In vzbv's view, opting out of personalisation on YouTube is very cumbersome to do and is also associated with various dark patterns: The fact that, after switching off personalisation, no videos are displayed at all on the home page is probably not a desirable situation for most users. This may, in some cases, pressure them into reactivating personalisation. Instead of 'Disable', the term 'Pause' is used in various places in relation to YouTube history. This gives the impression that YouTube can only be used without personalisation on a temporary basis.

Turning off personalisation is associated with various drawbacks. For example, a message in the app states: "If you pause your YouTube watch history, you may find it harder to find videos you've watched before, and you may receive fewer recommendations for new videos on YouTube and in other Google products." After disabling the history, the app repeatedly highlights in several places the option to re-enable it and the supposed benefits this brings. For example: "Your watch history is disabled. You can change this setting at any time to receive recommendations for new videos tailored specifically to you." Or: "YouTube tailored to your tastes. Using your watch history, we can show you the latest videos that match your interests." In vzbv's view, the app's design makes it much easier for users to (re-)enable their YouTube watch history than to disable it.

Example Snapchat:

Snapchat offers two ways within the app to disable personalised feeds.³² In both cases, several taps are required to reach the desired option. At the end of both paths is a slider that, by default, allows personalised content. However, if a user decides to deactivate it, Snapchat does not allow them to do so immediately. Instead, it first displays a pop-up window (see Fig. 48). Users must confirm the decision to disable personalised content once again. In vzbv's view, this pop-up may come across as a warning that could deter users from disabling personalisation.

In particular, phrasing such as 'You will continue to see content, but it will be more random and less tailored to your interests' can have a demotivating effect. At the same time, Snapchat remains very vague on this point, and it is unclear to what extent personalisation can be switched off completely or not.

³² Snapchat offers a Stories feed and a Spotlight feed. In the former, there are three feed categories: "Friends", "Following" and "Discover". The Spotlight feed is the platform's central short-form video feed and can be filtered by "For You" and "Following". In addition, there is content on the "Snap Map". According to Snapchat, the content there is generally not personalised: <https://help.snapchat.com/hc/de/articles/35157584066964-So-bewerten-wir-Content-in-Maps>

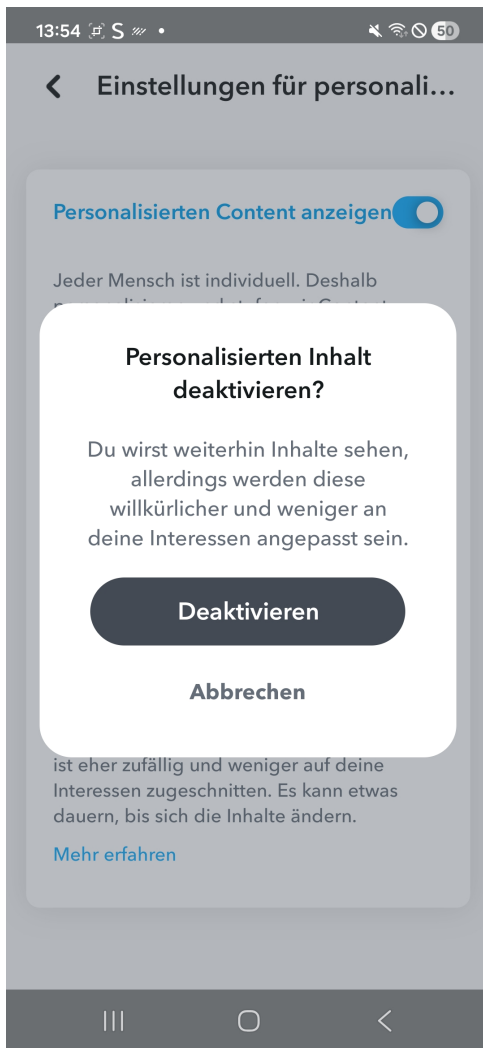


Figure 43: On Snapchat, a pop-up opens if users want to turn off the personalization of content.

Example Facebook

On the home screen of the Facebook app, the test account displays only a single personalised feed with no further options. To access alternative options, users must go to the menu (three-line icon). Among other things, the menu includes the “Feeds” option (see Fig. 44).

Tapping on this opens a view showing several feeds, all of which appear to be sorted chronologically (see Fig. 45). They are labelled: “All”, “Favourites”, “Friends”, “Groups” and “Pages”. The “All” feed displays the latest content from the Facebook account, sorted chronologically by publication date, and may therefore correspond to an option without profiling. However, this is not apparent from the name of the feed. There are no clear labels

relating to personalisation or profiling.

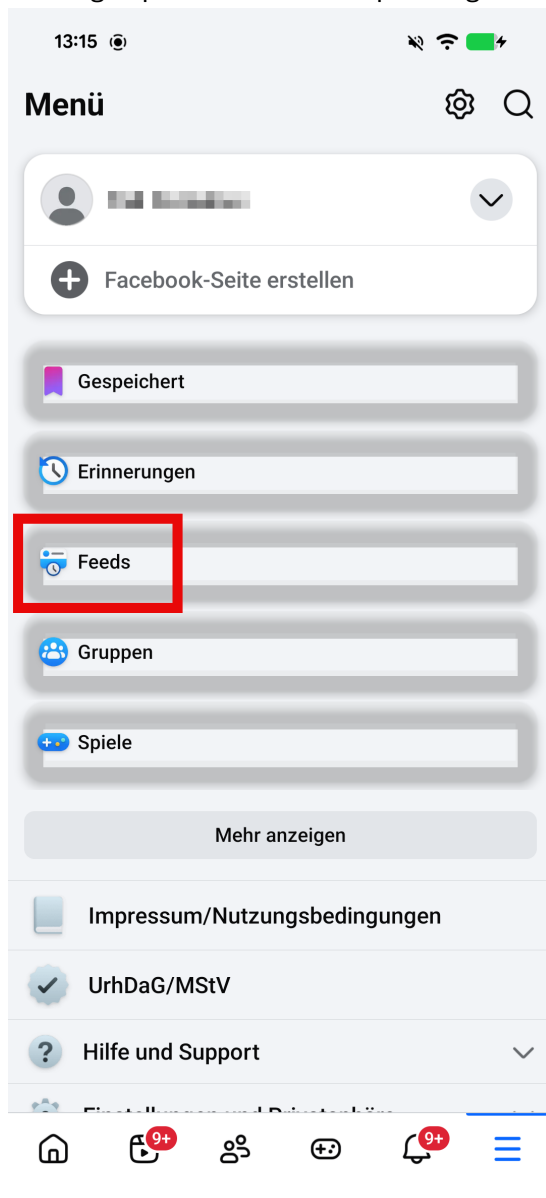


Figure 44: In the menu of the Facebook app, users will find the sub-item "Feeds" (highlighted in red here).

Compared with other apps examined, the feed alternatives described on Facebook do not need to be activated by users via a button or similar. They are available within the app from the outset. However, unlike the main feed, they can only be accessed via the settings menu and are, therefore, in vzbv's view, not easily or immediately accessible.

Another point of concern, in vzbv's view, is that there is no option to set the chronologically sorted view as the default feed. For example, if users close the app and then reopen it, they are taken back to the home page with the personalised feed every time.



Figure 45: In the "Feeds" section, current content is displayed in chronological order in the Facebook app.

Example Instagram:

Only in the “Explore” feed (magnifying glass) is the non-personalised option clearly labelled as such, namely ‘not personalised’.³³ According to Instagram, the two options in the main feed – “Following” and “Favourites” – do not contain suggested posts, but only content from accounts users follow or have marked as favourites.

What all non-personalised feeds have in common is that users have to select them themselves. Furthermore, they have to reapply the setting every time they open the app. Furthermore, when using non-personalised feeds in the main feed and the Reels feed, users do not have access to the navigation bar or the activity/notifications section (heart in the top right-hand corner), which makes it less likely that they will spend time there and highlights the unequal design of Instagram’s various feeds (see Figs. 51 and 52). In vzbv’s view, these practices are intended to discourage users from using non-personalised feeds.

³³ Instagram offers a total of three feeds, each with different options. On the home screen, users can filter the main feed using three options: “For you”, “Following” and “Favourites”. The “Reels” feed can be filtered by “for you” and “followed”. In addition, there is the category “Reels from Friends”. The “Explore” feed (magnifying glass) can be filtered by “for you” and “not personalised.” It displays content from across the entire platform based on a wide range of factors, including followed accounts, photos and videos a user has liked, etc. The suggested content is AI-based (<https://about.instagram.com/de-de/features/search-and-explore>).

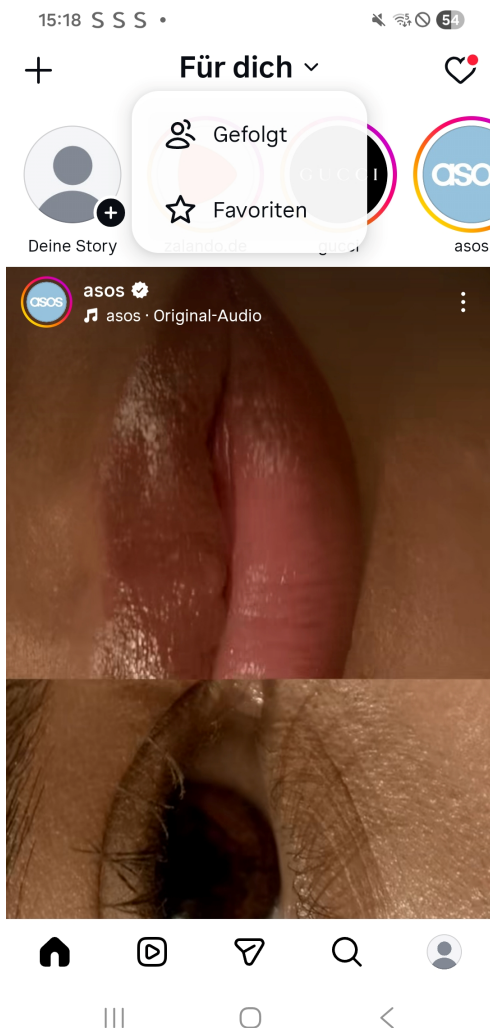


Figure 46: The navigation bar is included in the "For You" feed.



Figure 47: The navigation bar is missing from the "Following" feed.

11. Account deletion

Complex deletion processes make it difficult to control one's own content and jeopardise the exercise of data protection rights. If deletion functions are hidden, require several steps or can only be accessed via different menus, vzbv believes this increases the risk that personal data will be processed for longer than necessary.

On the platforms examined, for example, the option to delete one's own user account is sometimes very difficult to access and is made more complicated by manipulative design – which, in vzbv's view, contravenes the European Commission's guidelines (para. 56 e).

Example Facebook and Instagram

On the Meta platforms Facebook and Instagram, the "Deactivate account" option is preselected (rather than "Delete account"). When attempting to delete the account, the platform makes several attempts to influence the user's decision and suggests simply deactivating the account instead (see Figs. 39 to 42).

Furthermore, on Instagram, users must specify a reason for deletion in order to proceed with the process (see Fig. 43).



Figure 48: When trying to delete the Facebook account, the "Deactivate Account" option is preselected.

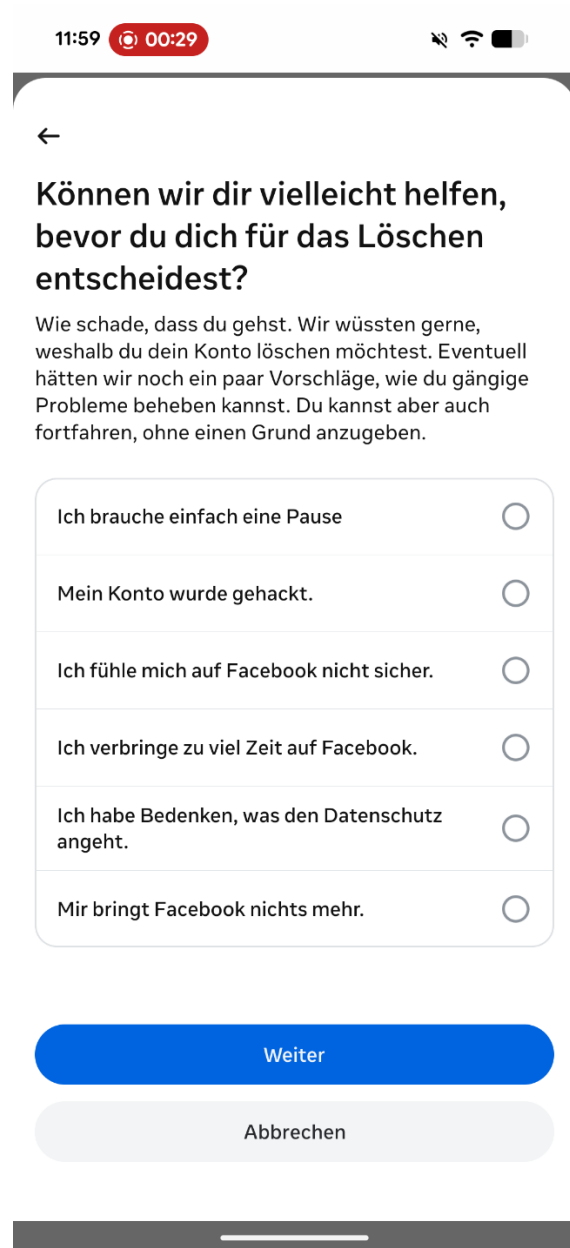


Figure 49: When attempting to delete their Facebook account, users will be asked to give a reason for the deletion.

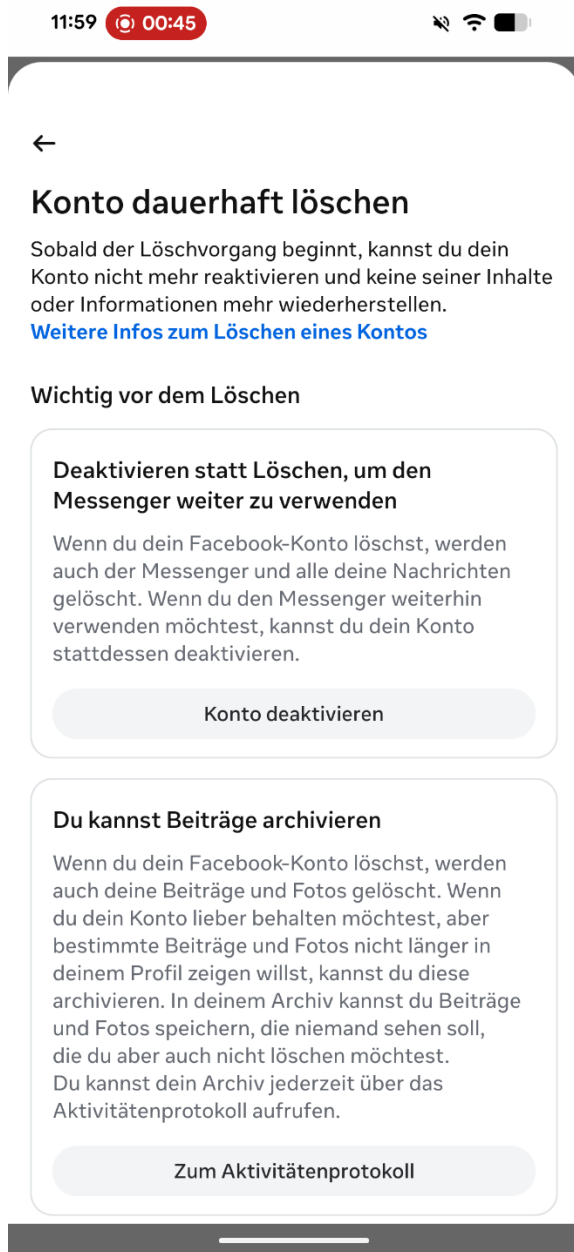


Figure 50: When trying to delete the Facebook account, supposed alternatives are repeatedly pointed out.



Figure 51: When trying to delete the Facebook account, supposed alternatives are repeatedly pointed out.

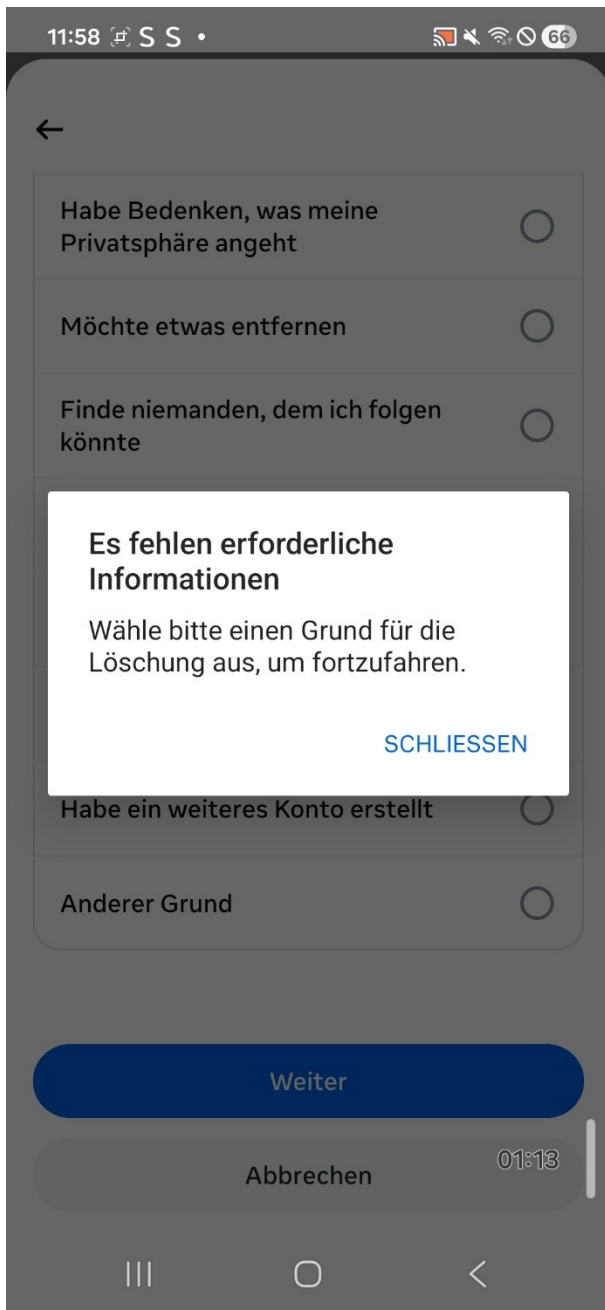


Figure 52: Instagram requires users to provide a reason why the account is to be deleted.

V. Political demands

Building safer digital services instead of imposing blanket bans

The study shows that platforms use harmful design features even though they know the accounts belong to children and adolescents. It follows that even when platforms are aware of the users' age group, this does not fundamentally change their approach to harmful design features. Even design elements explicitly identified by the European Commission in its guidelines on Article 28 of the Digital Services Act (DSA) as being harmful to children and teenagers – such as autoplay, infinite scroll and pull-to-refresh – are used by all five platforms examined, despite the platforms being aware that the accounts belong to minors.

Calling for the exclusion of minors by means of rigid age limits is not a solution. Rather, platforms must be required to change their business models, resulting in the complete and binding prohibition of harmful design features, such as those identified in this study. Only in this way can the evident risks to the development of children and adolescents be addressed sustainably, while at the same time ensuring their participation. Ultimately, platforms must be designed to be safe for everyone by default. Only a regulatory approach that tackles the problem at its root – that is, by eliminating structural risks and ensuring safe digital participation through design and default settings – is in the interests of all users and is, therefore, sustainable.

Manipulative designs and secure account settings

The investigation shows that the scope for platform discretion must be restricted. This is because, despite the guidelines, platforms continue, for example, to persistently urge users to grant access to their phone contacts. Manipulative designs are also repeatedly used, for instance, to permanently activate location sharing. These findings are consistent with recent court rulings: in two cases brought by vzbv, it was established that the DSA is inapplicable in cases involving manipulative designs³⁴. Apparently, the Act Against Unfair Competition takes precedence. Consequently, despite the guidelines and the provision in Section 25 of the DSA, the DSA often risks being rendered ineffective when it comes to dark patterns.

Recommender systems do not comply with standards

The study shows that none of the providers have the option 'without profiling' set as the default. Whilst this is not a requirement under the DSA, it is an important concern from a consumer perspective and a demand made by vzbv within the framework of the Digital Fairness Act.

Moreover, the findings clearly show that it is extremely difficult for users to select the mandatory option of a recommender system without profiling (as stipulated in Articles 27 and 38 of the DSA). In some cases, selection options are missing, or the option 'without profiling' is not clearly labelled, hidden, has to be reapplied every time, or does not work properly. Dark patterns are also used in the recommender system settings, designed to discourage users from using the non-personalised option.

³⁴ Oberlandesgericht Bamberg (Bamberg Higher Regional Court), judgment of 5 February 2025 (3 UKL 11/24 e) and Oberlandesgericht Bamberg (Bamberg Higher Regional Court), judgment of 4 February 2026 (3 UKL 8/25 e)

In addition to the demand that a non-profiling recommender system should be set as the default, it would be desirable from a user perspective for recommender systems to be based on interests actively selected by users themselves rather than on engagement signals.

Refining guidelines and making use of the Digital Fairness Act

The forthcoming revision of the DSA guidelines must clarify and strengthen the obligations regarding the protection of minors. However, this alone will not suffice. After all, guidelines are not laws. That is why the Digital Fairness Act (DFA) must be used as an opportunity to finally introduce robust, enforceable horizontal rules against harmful design practices across all digital services.

Imprint

Published by:

Verbraucherzentrale Bundesverband e.V.
(Federation of German Consumer Organisations)
Rudi-Dutschke-Straße 17, 10969 Berlin

T +49 30 25800-0
mbdigitales@vzbv.de
vzbv.de

Editing and text:

Team Monitoring Digital Markets

Status:

June 2026

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