Verbraucherzentrale
Bundesverband

Digitale Teilhabe und Schutz von Minderjährigen gewährleisten

Positionspapier des Verbraucherzentrale Bundesverbands e.V. (vzbv) zum Schutz von Minderjährigen bei der Nutzung digitaler Dienste

11. März 2026

Inhalt

I. Verbraucherrelevanz ... 3

II. Zusammenfassung ... 4

III. Einleitung ... 4

IV. Digitale Dienste sicher gestalten statt pauschal verbieten ... 5

1. Kinder- und jugendfreundliche digitale Dienste ... 6
1.1 Grundlegende Accounteinstellungen ... 7
1.2 Design und Interface ... 8
1.3 Kinderaccounts ... 11
2. Altersüberprüfung ... 12
2.1 Anwendung von Altersüberprüfung für erwachsene Nutzer:innen ... 13
2.2 Regulierung von Altersüberprüfung ... 13

Impressum ... 14

I. Verbraucherrelevanz

Kinder und Jugendliche nutzen digitale Dienste täglich, um sich zu vernetzen, kreativ auszudrücken und an der digitalen Welt teilzuhaben. Doch leider gehört zur Realität auch: Insbesondere Online-Plattformen setzen in ihren Geschäftsmodellen Designs ein, die auf maximale Nutzungsdauer und Datenverwertung ausgerichtet sind. Manipulative Designmechanismen wie Endlos-Scrollen, Autoplay und algorithmische Verstärkung bergen hohe Risiken für die psychische Gesundheit, da sie suchtfördernd sein können. Damit verbunden sind wiederkehrende Nutzungsschleifen, Kontrollverlust und die Verdrängung anderer Aktivitäten sowie Sozialkontakte.

Eine repräsentative Befragung des Verbraucherzentrale Bundesverbands (vzbv) zeigt klar: Ein Großteil der befragten Verbraucher:innen (93 Prozent) sieht Mängel beim Schutz von Minderjährigen im Internet. 65 Prozent der Befragten kritisieren fehlende Alterskontrollen, 54 Prozent bemängeln unzureichende Inhaltefilter, und 51 Prozent sehen zu wenig Engagement der Plattformen beim Schutz junger Nutzer:innen.[1] Besonders problematisch werden TikTok (79 Prozent) und Instagram (57 Prozent) bewertet. Diese Ergebnisse sind nicht überraschend, wenn man einen Blick auf die Einstellungen und das Design von großen Plattformen wirft.

Eine Untersuchung des vzbv aus Januar 2025 von Dark Patterns auf Online-Marktplätzen und Social-Media-Plattformen[2] kommt zu dem Schluss, dass manipulative Designs wie Autoplay, Endlos-Scrollen und aggressive Push Benachrichtigungen flächendeckend bei allen untersuchten Plattformen auch nach dem Inkrafttreten des Digital Services Act (DSA) eingesetzt werden. Ein ähnliches Bild zeigt sich in einem vzbv Praxischeck von unfairen Praktiken und manipulativen Designelementen bei Online-Games aus März 2025[3]. Alle der untersuchten Spiele setzen manipulative Designs ein, wobei 60 Prozent unmittelbare Kaufaufforderungen direkt beim App-Start zeigten. Intransparente Preisdarstellungen, häufig ausschließlich verwendete In-Game-Währung und der Einsatz von Countdows bei Angeboten, um Zeitdruck zu erzeugen, fanden sich auf allen untersuchten Gaming-Plattformen. Studien zeigen, dass auf maximale Aufmerksamkeit ausgerichtete Plattformdesigns das Wohlbefinden Jugendlicher beeinträchtigen, weil sie kontinuierliche Reizimpulse setzen und dadurch Schlaf, Konzentration und psychische Stabilität belasten.[4] Insbesondere die Nutzung von TikTok und YouTube sind dabei mit einem erhöhten Risiko für Angst- und Depressionssymptome sowie einem verminderten Selbstwert verbunden.[5] Diese Ergebnisse verdeutlichen den hohen Handlungsbedarf.

---

[1] Verbraucherzentrale Bundesverband: vzbv Jahresendbefragung 2025, November 2025, S. 15 – 18.

[2] Verbraucherzentrale Bundesverband: Manipulatives Design auf Online-Marktplätzen und Social-Media-Plattformen. Eine Untersuchung zur Umsetzung von Artikel 25 Digital Services Act (DSA), Januar 2025, [online] https://www.vzbv.de/sites/default/files/2025-01/vzbv_Dark-Patterns_Untersuchung.pdf.

[3] Verbraucherzentrale Bundesverband: Unfaire Praktiken und manipulatives Design in Online-Games & auf Spiele-Plattformen. Ein Praxischeck, März 2025, [online] https://www.vzbv.de/sites/default/files/2025-01/vzbv-Praxischeck_Manipulative_unfaire_Praktiken_Online-Spiele.pdf.

[4] 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, Juni 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, Juni 2025.

[5] van der Wal et al.: Diverse platforms, diverse effects: Evidence from a 100-day study on social media and adolescent mental health, Current Psychology, Dezember 2025.

II.Zusammenfassung

Ziel muss sein, dass digitale Dienste wieder zu Orten werden, an denen Kinder und Jugendliche kreativ sein können, sich austauschen und selbstbestimmt an der digitalen Welt teilhaben. Damit dies wieder möglich ist, müssen Digitale Dienste so gestaltet werden, dass sie eine sichere Nutzung ermöglichen. Aus Sicht des vzbv sind dafür folgende Aspekte wichtig:

- Pauschale Verbote digitaler Dienste, so zum Beispiel ein Social-Media Verbot, sind keine nachhaltige Lösung. Sie beschränken die digitale Teilhabe von Minderjährigen, ohne die eigentlichen Risiken, die primär aus dem Design der Plattformen zum Beispiel personalisierte Empfehlungssysteme und den Grundeinstellungen resultieren, wirksam zu adressieren.
- Der regulatorische Fokus sollte auf strukturellen Lösungen liegen: Sichere Grundeinstellungen und ein faires Plattformdesign sind per Default für alle Nutzer:innen vom Anbieter verpflichtend umzusetzen, um so eine sichere digitale Teilhabe von Minderjährigen zu gewährleisten.
- Ein faires Plattformdesign und sichere Grundeinstellungen beinhaltet unter anderem folgendes: Private Profile, deaktivierte Standortfreigabe und eingeschränkte Kontaktoptionen müssen Standard sein. Manipulative Design-Elemente wie Autoplay und Endlos-Scroll sind zu verbieten, Algorithmen von Empfehlungssystemen dürfen nicht auf Engagement-Signalen basieren, sondern auf von Nutzer:innen eingegebene Interessen. Tracking und personalisierte Werbung sind zu verbieten, sensible Funktionen wie Kamera und Mikrofon nur nach ausdrücklicher Zustimmung zu aktivieren. In-Game-Käufe und Lootboxen sind standardmäßig zu deaktivieren, klare Ausgabelimits einzuführen. Ergänzend sind einfache Löschfunktionen sowie niedrigschwellige Meldesysteme und kindgerechte Sprache erforderlich.
- Erwachsene Nutzer:innen können über den Nachweis ihrer Volljährigkeit das faire Plattformdesign und die Grundeinstellungen verändern. Hierfür können Instrumente der Altersüberprüfung wie beispielsweise die Europäische Digitale Brieftasche (EUDI-Wallet) eingesetzt werden. So kann eine flächendeckende Altersverifikationspflicht als
- Zugangsvoraussetzung für alle Nutzer:innen verhindert werden.
- Die eingesetzten Mittel zur Altersüberprüfung müssen datenschutzfreundlich sein und keine biometrischen Verfahren oder umfassende Identitätsprüfungen erfordern. Transparenz, Datenminimierung und freiwillige Nutzung, etwa bei der EUDI-Wallet, sind unverzichtbar.

III. Einleitung

In Europa wird auf verschiedenen Ebenen (Europäisches Parlament[6], Rat der Europäischen Union[7], Europäische Kommission[8]) über Verbote sozialer Medien für Minderjährige und über verpflichtende Alterskontrollen im Netz diskutiert. Hintergrund sind Forderungen nach einem Mindestalter von 16

[6] European Parliament: Children should be at least 16 to access social media, say MEPs, 2025, [online] https://www.europarl.europa.eu/news/en/press-room/20251120IPR31496/children-should-be-at-least-16-to-access-social-media-say-meps, 09.03.2026.

[7] European Newsroom: To ban or not to ban: EU countries debate social media age limits, 2025, [online] https://europeannewsroom.com/to-ban-or-not-to-ban-eu-countries-debate-social-media-age-limits/, 09.03.2026.

[8] EU Perspectives: EU moves to set digital age of majority, 2025, [online] https://euperspectives.eu/2025/09/eu-moves-to-set-digital-age-of-majority/, 09.03.2026.

Jahren für soziale Netzwerke und strengeren Jugendschutzmaßnahmen mehrerer Mitgliedsländer.[9] Die Debatte in Deutschland verläuft kontrovers: während der Kinderschutzbund vor dem Verlust digitaler Teilhabe warnt und sich gegen pauschale Verbote ausspricht[10], fordern hochrangige Politiker verschiedener Parteien klare Verbote. Die Bundesregierung hat im September 2025 eine Expertenkommission eingerichtet, die Handlungsempfehlungen bis Mitte 2026 entwickeln soll.[11]

Am 16. Februar 2026 hat sich die SPD innerhalb eines Impulspapiers für ein Social-Media Verbot für unter 14-jährige und für striktere, nach Alter gestaffelte, Design und Default Vorgaben für Minderjährige ausgesprochen.[12] Die CDU hat auf ihrem Parteitag am 20. und 21. Februar 2026 ebenfalls ein Social-Media Verbot für unter 14-jährige beschlossen und sich dafür ausgesprochen das besondere Schutzbedürfnis bis zum 16. Lebensjahr im digitalen Raum auszugestalten.

IV. Digitale Dienste sicher gestalten statt pauschal verbieten

Digitale Anwendungen sind für Kinder und Jugendliche zentrale Räume für Kommunikation, Austausch und soziale Integration. Die UN-Kinderrechtskonvention[13] garantiert in Artikel 17 Minderjährigen den Zugang zu Medien. Ein Verbot würde diesem Grundsatz widersprechen, da es das Recht auf Zugang zu Informationen und Teilhabe beschränkt. Darüber hinaus warnen Expert:innen, dass ein Verbot weder realistisch umsetzbar noch zielführend ist. Statt Risiken wie Cybergrooming oder exzessive Nutzung zu reduzieren, kann es zu sozialer Isolation führen und den Erwerb von Medienkompetenz verhindern.[14] Außerdem weichen Kinder und Jugendliche in solchen Situationen häufig auf andere digitale Angebote aus, zum Beispiel von sozialen Medien zu Spiele-Plattformen, was die Risiken nicht senkt, sondern lediglich verlagert. Die Bundeszentrale für Kinder- und Jugendmedienschutz betont, dass Kinder ein Recht auf digitale Teilhabe haben und Plattformen verpflichtet sind, sichere Umgebungen zu schaffen.[15] Auch Fachorganisationen wie

---

[9] Tagesschau: EU für Mindestalter in sozialen Netzen, 2025, [online] https://www.tagesschau.de/ausland/europa/eu-fuer-mindestalter-in-sozialen-netzen-100.html, 12.11.2025.

[10] Zeit Online: Kinderschutzbund fordert klare Altersgrenzen, 2025, [online] https://www.zeit.de/gesellschaft/zeitgeschehen/2025-08/kinderschutzbund-minderjaehrige-internet-altersgrenze-debatte, 12.11.2025.

[11] Deutschlandfunk: Neue Expertenkommission für mehr Kinder- und Jugendschutz im Netz, [online] https://www.deutschlandfunk.de/neue-expertenkommission-fuer-mehr-kinder-und-jugendschutz-im-netz-100.html, 10.12.2025.

[12] SPD-Bundestagsfraktion: Sichere Soziale Medien. Schutz von Kindern und Jugendlichen im digitalen Raum stärken, Impulspapier, Februar 2026, [online] https://www.spdfraktion.de/system/files/documents/impulspapier-sichere-soziale-medien.pdf.

[13] UN-Kinderrechtskonvention, 1989, [online] https://www.unicef.de/194402/data/77afdd9d17e246129b04e8aef70a01ab, 05.12.2025.

[14] ZDF heute: Experten gegen Smartphone-Verbot an Schulen, 2025, [online] https://www.zdfheute.de/panorama/smartphone-verbot-kinder-jugendliche-bildung-100.html, 05.12.2025; sh:z: Altersbeschränkungen für Social Media: Experten warnen vor Hürden, 2025, https://www.shz.de/deutschland-welt/schleswig-holstein/artikel/altersbeschraenkungen-fuer-social-media-experten-warnen-vor-huerden-49473581, 05.12.2025.

[15] BzKJ: Debatte um Social-Media-Verbot: Junge Menschen haben ein Recht auf digitale Teilhabe, 2025, [online] https://www.bzkj.de/bzkj/service/alle-meldungen/debatte-um-social-media-verbot-junge-menschen-haben-ein-recht-auf-digitale-teilhabe-251386, 18.11.2025.

UNICEF unterstreichen, dass digitale Räume nicht nur Risiken, sondern auch Chancen für Bildung und soziale Integration bieten.[16]

Zusätzlich besteht die Gefahr des heimlichen Nutzens: Wenn Kinder und Jugendliche trotz eines Verbots soziale Medien verwenden, steigt das Risiko, dass sie problematische Inhalte oder Übergriffe nicht melden, aus Angst vor Sanktionen. Dies kann Schutzmechanismen und Präventionsarbeit erheblich untergraben. Statt restriktiver Maßnahmen wie zum Beispiel eine pauschale und flächendeckende Altersbeschränkung für die Nutzung von digitalen Angeboten wie Social-Media braucht es deshalb klare Vorgaben, die Anbieter in die Verantwortung nimmt: digitale Dienste müssen so gestaltet sein, dass sie sicher und transparent für alle sind und Minderjährige umfassend schützen. Nur ein regulatorischer Ansatz, der strukturelle Risiken beseitigt und digitale Teilhabe gewährleistet, ist aus Sicht des vzbv zukunftsfähig.

Die Europäische Kommission hat in Bezug auf Vermittlungsplattformen im Juli 2025 Leitlinien[17] zu Artikel 28 des Digital Services Act (DSA) veröffentlicht und damit einen ersten Vorstoß in Richtung kinderfreundlichere digitale Dienste gemacht. Artikel 28 DSA verpflichtet Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, angemessene und verhältnismäßige Maßnahmen zu ergreifen, um ein hohes Maß an Privatsphäre, Sicherheit und Schutz zu gewährleisten. Die Leitlinien dienen als Orientierung für Plattformbetreiber und nationale Behörden und sind unverbindlich. Digitale Plattformen haben damit viel Spielraum bei der Umsetzung und erhalten keine klaren verpflichtenden Vorgaben für zentrale Bereiche wie Kontoeinstellungen, Design und Empfehlungssysteme sowie Altersverifikation. Dies gefährdet die Wirksamkeit des Kinder- und Jugendschutzes bei Online-Plattformen.

Ein umfassender Schutz von Minderjährigen kann jedoch nur gewährleistet werden, wenn sämtliche digitale Angebote, zu denen Minderjährige Zugang haben und von denen Risiken für ihre Privatsphäre und Sicherheit ausgehen, durch strukturelle Veränderungen ein sicheres Umfeld für junge Nutzer:innen schaffen.

1. Kinder- und jugendfreundliche digitale Dienste

Sichere Grundeinstellungen und ein Design, das Schutzmechanismen von Anfang an integriert, sind wirksamer und verhältnismäßiger als pauschale Zugangsbeschränkungen. Sie ermöglichen digitale Teilhabe, ohne die Grundrechte auf Information und Kommunikation einzuschränken, und erhöhen zugleich die Sicherheit vor Risiken wie Cybergrooming, Datenmissbrauch und unangemessenen Inhalten.

[16] UNICEF Schweiz: Kinderrechte im digitalen Raum, 2025, [online] https://www.unicef.ch, 18.11.2025.

[17] Europäische Kommission: Leitlinien für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 der Verordnung (EU) 2022/2065 (Digital-Services-Act), 2025, [online] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202505519.

1.1 Grundlegende Accounteinstellungen

Die Voreinstellungen für Nutzerkonten bei digitalen Anwendungen sind zentral, da die meisten Nutzer:innen diese nach der Kontoeinrichtung nicht aktiv verändern.[18] Laut der Leitlinien zu Art. 28 DSA sollen Anbieter von Online-Plattformen sicherstellen, dass Datenschutz, Sicherheit und Schutz bei allen Kontoeinstellungen für Minderjährige im Vordergrund stehen. Die konkreten Vorgaben im Bereich Accounteinstellungen sind zu begrüßen. Kritisch ist jedoch, dass Art. 28 DSA und die dazugehörigen Leitlinien Anbietern einen erheblichen Gestaltungsspielraum bei der Umsetzung der Vorgaben zu Grundeinstellungen überlassen. Zudem ist kritisch, dass laut der Leitlinien Minderjährige bestimmte Voreinstellungen dennoch anpassen können.

Aus Sicht des Verbraucherschutzes ist entscheidend, dass Schutzmechanismen für alle Accounts als Standard aktiviert sind. Erwachsene Nutzer:innen sollten jedoch die Möglichkeit bekommen, ihre Volljährigkeit nachzuweisen, um entsprechende Anpassungen wie die Standortfreigabe oder erweiterte Kontaktoptionen vorzunehmen. Der Altersnachweis sollte dabei beschränkt auf das Alter beziehungsweise die Volljährigkeit erfolgen und keine weiteren Angaben wie das genaue Geburtsdatum enthalten. So werden Minderjährige durch voreingestellte Accounteinstellungen geschützt. Altersverifikation dient nicht als allgemeine Zugangshürde, sondern kann ein Instrument sein, wenn bestimmte Funktionen durch erwachsene Nutzer:innen bewusst eingeschaltet oder verändert werden sollen.

- **Private Profile als Standard**: Öffentliche Profile auf sozialen Medien erhöhen das Risiko von unerwünschten Kontaktaufnahmen, Cybermobbing, Grooming oder anderen Formen des Missbrauchs. Besonders Kinder und Jugendliche sind gefährdet, da sie häufig noch nicht über die Erfahrung oder das Bewusstsein verfügen, welche Informationen sie preisgeben sollten und welche Risiken damit verbunden sind. Minderjährige Nutzer:innen können so leichter Ziel von Belästigung, Manipulation oder unerwünschten Anfragen werden. Die DSA-Leitlinien empfehlen zwar sichere Voreinstellungen, verpflichten Plattformen jedoch bisher nicht dazu, Profile standardmäßig privat zu stellen. Eine **verbindliche Vorgabe**, dass Accounts standardmäßig privat sein müssen, ist daher notwendig, insbesondere für alle Nutzerkonten, die über Chatfunktionen den Austausch mit anderen ermöglichen. Private Profile schützen Kinder und Jugendliche vor direkter Exposition und unerwünschten Kontakten, reduzieren die Wahrscheinlichkeit von Missbrauch und tragen dazu bei, dass Minderjährige sicher und selbstbestimmt digitale Anwendungen nutzen können.
- **Deaktivierte Standortfreigabe:** Die automatische Weitergabe von Standortdaten über Apps oder soziale Medien kann die Sicherheit von Kindern und Jugendlichen erheblich gefährden. Standortinformationen ermöglichen es Dritten, physische Aufenthaltsorte nachzuverfolgen, was zu Überwachung, Stalking oder gezieltem Missbrauch führen kann. Kinder und Jugendliche verfügen oft noch nicht über die Erfahrung oder das Bewusstsein, welche Risiken die Weitergabe von Standortdaten mit sich bringt, und können dadurch besonders leicht Opfer von Gefahren werden. Daher sollten Standortfreigaben standardmäßig deaktiviert sein und nur nach ausdrücklicher Zustimmung von volljährigen Nutzer:innen aktiviert werden können.

[18] Cho, H., Roh, S., & Park, B.: Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings, Computers in Human Behavior, 2019, S. 1-13;

Jachimowicz, J. M., Duncan, S., Weber, E. U., & Johnson, E. J.: When and why defaults influence decisions: a meta-analysis of default effects. Behavioural Public Policy, 2019.

- **Eingeschränkte Kontaktoptionen:** Die Möglichkeit, dass Fremde direkt Kontakt zu Minderjährigen aufnehmen können, stellt ein zentrales Risiko für Grooming, Belästigung und sexualisierte Gewalt dar. Anbieter digitaler Dienste müssen daher verpflichtet werden, direkte Kontaktoptionen standardmäßig zu blockieren. Dieses Vorgehen reduziert die Wahrscheinlichkeit, dass Kinder Opfer unerwünschter Kontaktaufnahmen oder manipulativer Ansprache werden, und stärkt ihre Sicherheit im digitalen Raum.
- **Tracking-Mechanismen und personalisierte Werbung verbieten:** Viele Online-Angebote erfassen systematisch Nutzungsdaten über verschiedene Websites, Apps und Endgeräte hinweg und führen diese zu umfassenden Persönlichkeits- und Interessenprofilen zusammen. Diese Profile bilden die Grundlage für personalisierte Werbung und beeinflussen, welche Inhalte Nutzer:innen sehen, wie sie angesprochen werden und welche Kauf- oder Verhaltensimpulse gesetzt werden. Für Kinder und Jugendliche sind diese Praktiken besonders problematisch, da sie die Funktionsweise von Tracking und datenbasierter Personalisierung häufig nicht verstehen und die langfristigen Folgen einer Datennutzung kaum abschätzen können. Das bestehende Einwilligungsmodell greift hier zu kurz: Zustimmung wird meist unter Zeitdruck, ohne echte Wahlfreiheit und ohne altersgerechte Transparenz erteilt. Dadurch werden Schutzbedürfnisse junger Menschen systematisch unterlaufen, während kommerzielle Interessen dominieren. Um diesen strukturellen Risiken personalisierter Online-Werbung wirksam zu begegnen, sind verbindliche Einschränkungen datenbasierter Tracking- und Profilbildungspraktiken erforderlich.
- **Einschränkung sensibler Funktionen**: Der Zugriff auf Kamera und Mikrofon in digitalen Diensten und Apps kann erhebliche Missbrauchsrisiken bergen. Kinder und Jugendliche können so intime Daten preisgeben, die von Dritten für Belästigung, Überwachung oder Grooming genutzt werden. Besonders Minderjährige sind häufig noch nicht in der Lage, die Folgen der Freigabe sensibler Funktionen einzuschätzen oder sich dagegen zu wehren. Daher müssen Zugriffe auf Kamera und Mikrofon standardmäßig eingeschränkt sein und dürfen nur nach ausdrücklicher Zustimmung und kontextspezifisch aktiviert werden können.
- **Standardlimits für Zahlungen und Deaktivierung von In-Game-Käufen:** Kinder und Jugendliche sind besonders anfällig für impulsive Käufe in digitalen Spielen und auf Plattformen, da ihr Verständnis für Geld und wirtschaftliche Konsequenzen noch in der Entwicklung ist. Ohne Schutzmechanismen können sie leicht finanziell ausgenutzt werden, sei es durch Mikrotransaktionen, Lootboxen oder In-Game-Käufe. Anbieter digitaler Dienste sollten deshalb Standardlimits für Zahlungen einführen und In-Game-Käufe für alle minderjährigen Accounts standardmäßig deaktivieren.

1.2 Design und Interface

Manipulatives Plattformdesign kann ein erhebliches Risiko für die Sicherheit, den Schutz und die Privatsphäre der Nutzer:innen darstellen. Da Minderjährige aufgrund ihres Entwicklungsstandes und ihrer psychologischen Verwundbarkeit eine besonders schutzbedürftige Verbrauchergruppe sind, lassen sie sich leichter dazu verleiten, persönliche Daten preiszugeben oder unbeabsichtigte Online-Käufe zu tätigen. Auch an dieser Stelle machen die DSA-Leitlinien Vorgaben für Anbieter von Online-Plattformen. So wird betont, dass Maßnahmen, die Minderjährigen Kontrolle über ihre Online-Erfahrungen ermöglichen, ein wirksames Mittel darstellen, um ein hohes Maß an Privatsphäre, Sicherheit und Schutz zu gewährleisten. Dazu gehört, dass die Gestaltung der

Benutzeroberfläche altersgerecht erfolgt und Minderjährige nicht durch manipulative Design-Elemente zu übermäßiger Nutzung verleitet werden dürfen.

Auch wenn die DSA-Leitlinien hier in die richtige Richtung gehen, da sie wichtige Empfehlungen enthalten, bleiben die Vorgaben unverbindlich, womit den Anbietern von Online-Plattformen viel Gestaltungsraum gegeben wird. Manipulative Elemente wie Autoplay, endloses Scrollen oder künstliche Verknappung werden nicht konsequent verboten und KI-Funktionen dürfen grundsätzlich aktiviert werden. Zudem werden nicht alle digitalen Dienste vom DSA erfasst. Dazu gehören beispielsweise KI-Companionship-Anwendungen oder Chatbots, die nicht in große Online-Plattformen eingebettet sind. Dabei kann von ihnen ebenfalls eine Gefahr für Kinder- und Jugendliche ausgehen.[19] Damit entsteht ein Schutzrahmen, der in der Praxis nicht ausreicht. Ein wirksamer Schutz erfordert verbindliche Vorgaben für alle, sowie klare Standards, die manipulative Designs und kommerzielle Ausbeutung unterbinden.

- **Verbot manipulativer Design-Elemente:** Viele digitale Anwendungen setzen gezielt manipulative und süchtig machende Designelemente wie Autoplay, endloses Scrollen, Push-Benachrichtigungen, Gamification oder algorithmisch gesteuerte Empfehlungen ein, um Aufmerksamkeit und Nutzungsdauer zu maximieren. Diese sogenannten Dark Patterns untergraben die Selbstbestimmung, indem sie natürliche Stopppunkte entfernen, Belohnungsschleifen erzeugen und dadurch Kontrollverlust sowie suchtähnliches Nutzungsverhalten begünstigen. Studien zeigen, dass Nutzer:innen dadurch häufig länger und intensiver interagieren, als sie beabsichtigen, was Aufmerksamkeit, Selbstwahrnehmung und Wohlbefinden beeinträchtigen kann.[20] Besonders Kinder und Jugendliche sind gefährdet, da ihre Selbstregulationsfähigkeiten und ihr Belohnungssystem noch nicht vollständig entwickelt sind und sie manipulative Muster oft nicht bewusst erkennen. Eine medienpädagogische Untersuchung zeigt, dass junge Menschen Dark Patterns oft nicht bewusst wahrnehmen und dadurch anfälliger für exzessive Nutzung oder Verhaltenszwänge sind.[21] Langfristig kann dies zu Schlafstörungen, Konzentrationsproblemen, erhöhtem Stress und negativen Auswirkungen auf schulische Leistungen und soziale Interaktionen führen.[22] Um die Selbstbestimmung zu stärken und gesundheitliche Risiken zu reduzieren, sollten manipulative Designelemente verboten werden. Ergänzend sind verpflichtende Pausenhinweise, Zeitlimits und klare Exit-Punkte vorzusehen.
- **Einfache Löschfunktionen:** Komplexe Löschprozesse erschweren die Kontrolle über eigene Inhalte und gefährden die Wahrnehmung datenschutzrechtlicher Rechte. Wenn Löschfunktionen versteckt sind, mehrere Schritte erfordern oder nur über unterschiedliche Menüs erreichbar sind, steigt das Risiko, dass personenbezogene Daten länger als notwendig verarbeitet werden. Dies

---

[19] Bundeszentrale für Kinder- und Jugendmedienschutz: Kinder und Jugendliche im Gespräch mit KI – Einordnung und Empfehlungen aus der medienpädagogischen Praxis, 2026, [online] https://www.bzkj.de/resource/blob/280518/2b7acfaa7f0148d34e84a63811b7e5a5/20261-kinder-und-jugendliche-im-gespraech-mit-ki-einordnung-und-empfehlungen-aus-der-medienpaedagogischen-praxis-data.pdf.

[20] Verbraucherzentrale Bundesverband: Manipulatives Design auf Online-Marktplätzen und Social Media, Januar 2025, [online] https://www.vzbv.de/sites/default/files/2025-01/vzbv_Dark-Patterns_Untersuchung.pdf.

[21] Kammerl, Rudolf, et al.: Dark Patterns und Digital Nudging in Social Media-wie erschweren Plattformen ein selbstbestimmtes Medienhandeln? Expertise für die Bayerische Landeszentrale für neue Medien, Nomos, Juli 2023.

[22] Paulus, F.W. Digitale Medien und Schlaf bei Kindern und Jugendlichen: Prävention und Intervention. Paediatr. Paedolog. 59, 236–243, Februar 2024.

kann zu einer ungewollten Weitergabe oder Nutzung sensibler Informationen führen und steht im Widerspruch zu den Grundsätzen der Datenminimierung und Speicherbegrenzung nach der Datenschutzgrundverordnung (DSGVO). Digitale Dienste müssen daher einfache, leicht auffindbare und unmittelbar wirksame Löschfunktionen für Inhalte und Konten bereitstellen. Nur so können rechtswidrige Inhalte schnell entfernt und für Minderjährige unzugänglich gemacht werden.

- **Niedrigschwellige Meldungen:** Fehlende oder komplizierte Meldemöglichkeiten verhindern schnelle Reaktionen bei Gefahren wie Cybermobbing, Belästigung oder sexualisiertem Missbrauch. Besonders Kinder und Jugendliche sind betroffen, da sie oft nicht über die Erfahrung oder das Wissen verfügen, um komplexe Meldesysteme korrekt zu bedienen. Komplizierte Prozesse können dazu führen, dass Vorfälle nicht gemeldet werden, wodurch der Schutz der Minderjährigen erheblich eingeschränkt wird. Die Vorgaben der DSA-Leitlinien zu Moderation und Meldesystemen sind grundsätzlich ein Schritt in die richtige Richtung, bleiben jedoch in wichtigen Details unzureichend. So fehlt beispielsweise eine klare Anforderung, dass Meldungen mit maximal 2-Klicks[23] möglich sein müssen. Dies sollte dabei auch für nicht registrierte Nutzer:innen gelten. Nur so kann gewährleistet werden, dass Kinder und Jugendliche ohne lange Umwege Gefahren melden und Schutzmaßnahmen schnell greifen können. Diese Anforderung sollte für alle digitalen Dienste gelten, zu denen Minderjährige Zugang haben, um effektiven, unmittelbaren Schutz zu gewährleisten und das Vertrauen der Nutzer:innen in die Plattformen zu stärken. Ein einfaches, intuitives Meldesystem ist essenziell, damit Kinder und Jugendliche Gefahren schnell anzeigen können, Missbrauch verhindert wird und digitale Plattformen ihrer Schutzpflicht gegenüber Minderjährigen effektiv nachkommen.
- **Kinderfreundliche Sprache und klare Sicherheitsfunktionen:** Viele Sicherheitsfunktionen in digitalen Anwendungen wie soziale Medien sind heute komplex formuliert und schwer zugänglich, sodass insbesondere Kinder und Jugendliche Schwierigkeiten haben, sie korrekt zu nutzen. Komplexe Sprache, verschachtelte Menüs oder unübersichtliche Datenschutzeinstellungen erschweren den Zugang zu Schutzmechanismen und können dazu führen, dass Minderjährige versehentlich sensible Daten freigeben oder riskante Inhalte konsumieren. Eine klare, verständliche Gestaltung in einfacher, altersgerechter Sprache stärkt die Medienkompetenz von Kindern und Jugendlichen. Sie können Sicherheitsfunktionen leichter verstehen, eigenständig nutzen und so bewusste Entscheidungen über ihre Daten und ihr Verhalten online treffen. Konkrete Vorgaben für Anbieter digitaler Dienste sind notwendig, damit Funktionen wie Privatsphäre-Einstellungen, Meldemechanismen und Blockierfunktionen standardmäßig verständlich, sichtbar und leicht zugänglich umgesetzt werden. Kinderfreundliche Sprache und intuitive Sicherheitsfunktionen sind entscheidend, um Minderjährige wirksam zu schützen, ihre Selbstständigkeit im Umgang mit digitalen Medien zu fördern und die Nutzung von Schutzmechanismen überhaupt erst praktikabel zu machen.
- **Begrenzung algorithmischer Empfehlungssysteme:** Algorithmen, die auf Engagement-Signalen basieren, fördern problematische Inhalte und können in gesundheitsgefährdende

[23] Das 2-Klick-Konzept (oder Zwei-Klick-Lösung) ist ein technisches und rechtliches Verfahren auf digitalen Plattformen, das darauf ausgelegt ist, die Datenschutzkonformität (DSGVO) zu erhöhen und die Nutzerfreundlichkeit zu verbessern. Dieses sollte für die Meldung von Inhalten übertragen werden.

Nutzungsmuster führen. Insbesondere Minderjährige sind hierfür besonders anfällig. Empfehlungssysteme müssen stattdessen auf explizite Präferenzen und Qualitätskriterien ausgerichtet sein, um die psychische Gesundheit zu schützen. Laut Leitlinien zu Artikel 28 des DSA sollen Empfehlungssysteme an die Bedürfnisse von Minderjährigen angepasst werden, um problematische Inhalte zu vermeiden. Aus Sicht des vzbv ist es jedoch zudem erforderlich, dass Plattformen keine Verhaltensdaten von Kindern nutzen, sondern ausschließlich explizite Signale zum Beispiel das Ankreuzen bestimmter Interessen berücksichtigen dürfen.[24]

- **Schutz vor bildbasierter Gewalt und Missbrauch:** Bilder von Minderjährigen werden im Internet häufig kopiert, weiterverbreitet oder in manipulierten Formaten wie Deepfakes missbraucht. Solche Inhalte können nicht nur das persönliche Ansehen und die Privatsphäre der Kinder verletzen, sondern auch langfristige psychische Folgen wie Angst, Scham oder Vertrauensverlust auslösen. Minderjährige sind besonders gefährdet, weil sie oft die Risiken der Veröffentlichung von Bildern oder Videos noch nicht vollständig einschätzen können und noch nicht über die Erfahrung oder die rechtlichen Mittel verfügen, um sich zu schützen. Technische Schutzmaßnahmen wie Screenshot-Blocker, Kopierschutz, automatische Unkenntlichmachung sensibler Inhalte oder Algorithmen zur Erkennung und Entfernung missbräuchlicher Bilder müssen daher verpflichtend implementiert werden. Ohne solche Maßnahmen besteht die Gefahr, dass Inhalte schnell viral gehen, dauerhaft im Internet verfügbar bleiben oder gezielt zur Erpressung, Belästigung oder Cybermobbing verwendet werden. Besonders problematisch ist dies für Kinder und Jugendliche, weil sie noch in der Entwicklung ihrer sozialen und emotionalen Kompetenzen sind und sich oft der langfristigen Folgen nicht bewusst sind. Zudem kann die Veröffentlichung intimer oder kompromittierender Bilder das Risiko erhöhen, dass Minderjährige Opfer von Online-Grooming oder sexualisierter Gewalt werden. Ein verpflichtender technischer Schutz ist notwendig, um Kinder und Jugendliche vor dauerhaften Schäden, Missbrauch und Manipulation zu schützen und ihnen ein sicheres Online-Umfeld zu gewährleisten.
- **Transparente und einfache Einstellungsoptionen:** Nutzer:innen müssen jederzeit leicht nachvollziehen und ändern können, welche Daten sie teilen und welche Funktionen auf einer Plattform aktiv sind. In der Praxis sind solche Optionen oft versteckt, fragmentiert oder in komplizierter Sprache dargestellt. Dadurch bleiben riskante Funktionen unbeabsichtigt aktiviert. Insbesondere Kinder und Jugendliche verfügen häufig noch nicht über die Erfahrung oder das Wissen, um komplexe Menüs zu verstehen oder verborgene Funktionen zu erkennen. Ohne leicht zugängliche und verständliche Einstellungen sind sie besonders anfällig für unbeabsichtigte Datenfreigaben. Anbieter digitaler Dienste müssen daher verpflichtet werden, alle relevanten Einstellungen klar sichtbar und in einfacher, altersgerechter Sprache darzustellen.

1.3 Kinderaccounts

Kinderaccounts werden von Plattformen häufig als Instrument zum Schutz Minderjähriger präsentiert. Sie sollen altersgerechte Inhalte bereitstellen, die Kommunikation einschränken und

[24] Ein explizites Signal ist ein klar formuliertes, bewusst gegebenes Signal, das direkt und eindeutig eine bestimmte Information, Absicht oder Präferenz kommuniziert. Es steht im Gegensatz zu impliziten Signalen, die nur indirekt oder aus dem Verhalten abgeleitet werden können. Ein explizites Signal lässt keinen Interpretationsspielraum darüber, was gemeint ist. Das Ankreuzen eines Kontrollkästchens („Ich möchte Newsletter erhalten“) ist ein explizites Signal. Dagegen wäre, wenn man nur oft eine Seite besucht, aber nichts anklickt, ein implizites Signal.

Eltern Kontrollmöglichkeiten geben. In der Praxis sind solche Accounts jedoch kein hinreichender Schutz vor den zentralen Risiken digitaler Umgebungen. Sie adressieren weder manipulative Plattformdesigns noch algorithmische Empfehlungsmechanismen, die exzessive Nutzung fördern. Damit entsteht eine Scheinsicherheit: Die grundlegenden Gefahren bleiben bestehen, wenn Geschäftsmodelle auf maximaler Aufmerksamkeit und Datenverwertung beruhen. Hinzu kommt die Komplexität für Eltern: Fragmentierte Systeme und unübersichtliche Einstellungen erschweren die Verwaltung und führen zu geringer Wirksamkeit. Ein isolierter Fokus auf Kinderaccounts greift daher zu kurz. Notwendig ist ein ganzheitlicher Ansatz, der das Plattform Design und die Grundeinstellungen in den Blick nimmt.

- **Keine Scheinsicherheit durch Kinderaccounts:** Kinderaccounts dürfen nicht als Lösung für den Schutz Minderjähriger betrachtet werden. Sie können grundlegende Risiken wie manipulative Plattformdesigns, algorithmische Empfehlungsmechanismen und exzessive Nutzung nicht verhindern. Der Schutz muss primär auf Ebene des Designs und der Geschäftsmodelle ansetzen.
- **Vermeidung digitaler Exklusion:** Kinderaccounts dürfen nicht dazu führen, dass marginalisierte Gruppen (zum Beispiel Kinder von Menschen ohne Ausweisdokumente) vom digitalen Raum ausgeschlossen werden. Lösungen müssen barrierearm und inklusiv gestaltet sein.
- **Komplexität für Eltern reduzieren:** Die Verwaltung von Kinderaccounts muss einfach und transparent sein. Komplexe Einstellungen oder fragmentierte Lösungen über verschiedene Plattformen hinweg sind nicht akzeptabel.

2. Altersüberprüfung

Altersüberprüfungen können ein Instrument zum Schutz von Kindern und Jugendlichen sein. Allerdings sollten sie nicht als Zugangshürde mit der Folge, dass alle Nutzer:innen ihr Alter verifizieren müssen, eingesetzt werden. Dies könnte zu einer flächendeckenden Identifizierung aller Nutzer:innen führen und ist kritisch zu bewerten. Problematisch ist auch, dass verpflichtende Altersverifikationen regelmäßig auf Identitätsdokumente oder biometrische Verfahren zurückgreifen und damit eine erhebliche Menge besonders sensibler personenbezogener Daten verarbeiten. Die Systeme sind häufig unzuverlässig, sodass Minderjährige trotz technischer Hürden Zugang erhalten, während zugleich umfangreiche Datenbestände entstehen, die neue Sicherheitsrisiken schaffen. Weiterhin besteht die Gefahr, dass strikte Alterskontrollen zu Ausweichbewegungen auf weniger regulierte oder informelle digitale Dienste führen, was den Schutz Minderjähriger eher schwächt als stärkt.

Der regulatorische Fokus sollte daher auf strukturellen Lösungen liegen: Sichere Grundeinstellungen und ein faires Plattformdesign sind per Default für alle Nutzer:innen vom Anbieter verpflichtend umzusetzen, um so eine sichere digitale Teilhabe von Minderjährigen zu gewährleisten. Erwachsene Nutzer:innen sollten dabei die Möglichkeit erhalten, Funktionen und Einstellungen wie beispielsweise die automatische Standortfreigabe, direkte Kontaktaufnahme oder bestimmte Anwendungen zum Beispiel Autoplay durch einen Nachweis der Volljährigkeit anzupassen.

2.1 Anwendung von Altersüberprüfung für erwachsene Nutzer:innen

- **Ganzheitlicher Ansatz:** Altersüberprüfung ist nur ein Baustein. Sie muss eingebettet sein in ein umfassendes Schutzkonzept, das primär Designvorgaben und Grundeinstellungen vorgibt, sowie Inhaltsregulierung und Medienkompetenz fördert.
- **Rechtsklarheit und Zweckbindung:** Altersverifikation darf nur auf einer präzisen gesetzlichen Grundlage erfolgen und muss sich strikt am Zweck des Jugendschutzes orientieren. Eine flächendeckende Identitätsprüfung aller Nutzer:innen gefährdet die Anonymität und kann negative Effekte erzeugen, bei denen Menschen aus Angst vor Überwachung auf wichtige Informationsangebote verzichten.

2.2 Regulierung von Altersüberprüfung

- **Verbot biometrischer Verfahren zur Altersprüfung:** Biometrische Verfahren zur Altersüberprüfung, etwa die Analyse des Gesichts oder der Stimme, wirken auf den ersten Blick wie eine bequeme technische Lösung. In der Praxis sind sie jedoch fehleranfällig, diskriminierend und können Kinder- und Jugendliche nicht hinreichend schützen. Solche Systeme bergen zudem hohe Datenschutzrisiken, denn sie benötigen Gesichtsbilder oder andere besonders sensible Daten. Werden solche Daten zentral gespeichert, besteht die Gefahr von Missbrauch, Datenlecks oder Profilbildung. Ein Verbot oder eine strenge Regulierung solcher Verfahren ist notwendig, um Grundrechte zu wahren und Missbrauch zu verhindern.
- **Klare gesetzliche Grenzen für die Datenerhebung bei Alterskontrollen:** Damit Zugangsbeschränkungen für digitale Angebote wie Social-Media nicht unfreiwillig zu einer Art digitalem Ausweiszwang werden, braucht es klare gesetzliche Grenzen. Daten dürfen nur in dem Umfang erhoben werden, der unbedingt notwendig ist (Grundsatz der Datenminimierung).
- **Datenschutzfreundliche Gestaltung:** Viele Verfahren erheben unnötig viele personenbezogene Daten, was Missbrauch und Profilbildung begünstigt. Dabei existieren bereits datenschutzfreundliche Alternativen, die das Alter bestätigen können, ohne weitere persönliche Informationen offenzulegen: Technologien wie Zero-Knowledge-Proofs oder Token-basierte Nachweise ermöglichen eine Altersbestätigung, ohne dass ein Foto, ein Ausweisdokument oder eine biometrische Messung erforderlich ist. Diese Ansätze schützen die Privatsphäre, reduzieren Risiken und stärken die Selbstbestimmung von Kindern und Jugendlichen.
- **Transparenzpflichten für Altersverifikationssysteme:** Es ist wichtig, dass Nutzer:innen verstehen können, wie ein Altersverifikationssystem funktioniert: welche Daten erhoben werden, wie lange sie gespeichert bleiben und wie das System Missbrauch verhindert.
- **Pflicht zur Datenschutz-Folgenabschätzung:** Unabhängige Prüfungen und eine verpflichtende Datenschutz-Folgenabschätzung helfen, Risiken frühzeitig zu erkennen. Nutzer:innen werden unnötig gefährdet, wenn Altersverifikationssysteme implementiert werden, ohne zuvor zu analysieren, welche Nebenwirkungen sie haben könnten, etwa Fehleinstufungen, Sicherheitsrisiken oder den Ausschluss bestimmter Nutzergruppen. Eine verpflichtende Folgenabschätzung würde hier stärkere Kontrolle ermöglichen, damit Risiken frühzeitig erkannt und minimiert werden können.
- **Recht auf anonyme Nutzung erhalten:** Anonymität im Netz schützt die freie Meinungsäußerung, ermöglicht Recherche in sensiblen Kontexten und schützt besonders verletzliche Gruppen vor Überwachung.

- **Einsatz der EUDI-Wallet kontextsensitiv und freiwillig:** Der Einsatz der europäischen digitalen Brieftasche sollte vorsichtig und technologieoffen diskutiert werden. Die EUDI-Wallet befindet sich noch in der Entwicklung. Erst nach ihrer Bereitstellung lässt sich seriös beurteilen, ob sie sich für eine verbraucherfreundliche und datensparsame Altersverifikation eignet. Eine frühzeitige Festlegung auf ein noch unfertiges Produkt wäre riskant, da nicht absehbar ist, ob die technischen Anforderungen, der Datenschutz und die Nutzerfreundlichkeit tatsächlich erfüllt werden. Deshalb darf die Wallet weder verpflichtend sein noch als einzige Lösung betrachtet werden. Entscheidend ist, dass verschiedene datensparsame und niedrigschwellige Alternativen geprüft und getestet werden, damit keine Gruppe ausgeschlossen wird und die digitale Teilhabe gewährleistet bleibt.

Impressum

Herausgegeben von:
Verbraucherzentrale Bundesverband e.V.
Rudi-Dutschke-Straße 17, 10969 Berlin

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

Der Verbraucherzentrale Bundesverband e.V. ist im Deutschen Lobbyregister und im europäischen Transparenzregister registriert. Sie erreichen die entsprechenden Einträge hier und hier.