

Unabhängige Expertenkommission

"Kinder- und Jugendschutz in der digitalen Welt"

Hearing 2 – Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste

Der **Digital Services Coordinator (DSC) in der Bundesnetzagentur** nimmt im Folgenden Stellung zu den Fragen der unabhängigen Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt“. Wir weisen in diesem Zusammenhang darauf hin, dass für die Durchsetzung der Bestimmung zum Kinder- und Jugendschutz nach Art. 28 Digital Services Act (DSA) die Medienanstalten der Länder (LMA) sowie die bei der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) eingerichtete Stelle zur Durchsetzung von Kinderrechten in digitalen Diensten (KidD) gemäß dem Digitale-Dienste-Gesetz (DDG) zuständig sind. Der DSC ist beim Thema Kinder- und Jugendmedienschutz ausschließlich koordinierend tätig. Für Datenschutzaspekte ist die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) zuständig. Der DSC ist beim Thema Kinder- und Jugendmedienschutz ausschließlich koordinierend tätig. Die aus dieser Koordinierungsrolle und unserer Zusammenarbeit auf der europäischen Ebene gewonnenen Erkenntnisse stellen wir gerne der unabhängigen Expertenkommission zur Verfügung.

LEITFRAGE

Welche Kombination aus technischen, regulatorischen und pädagogischen Maßnahmen ist aus Ihrer fachlichen Sicht am wirksamsten, um Kinder und Jugendliche im digitalen Raum zu schützen und ihre Teilhabechancen zu stärken?

I Risiken, Schutzmaßnahmen und Gestaltung digitaler Dienste

1. Welche Maßnahmen sind aus Ihrer Sicht am wirksamsten, um die folgenden Risiken für Kinder und Jugendliche in digitalen Diensten zu verhindern, zu erschweren oder in ihren Folgen zu begrenzen:
 - a. digitale sexualisierte Gewalt (z.B. Cybergrooming, Sextortion, Missbrauchsdarstellungen),
 - b. suchtbegünstigende/hochgradig bindende Gestaltungspraktiken (z.B. Mikrotransaktionen, Lootboxen/Zufallsmechaniken, Dark Patterns),

Der DSC hat im Jahr 2024 eine Studie zu gesellschaftlichen Auswirkungen von digitalen Diensten mit Fokus auf Suchtgefahren erstellen lassen.¹ In der Studie kommen die Autoren zu dem Schluss, dass es eines ganzheitlichen Ansatzes bedarf, der sowohl Maßnahmen in der Regulatorik wie Altersverifikation, Inhaltskontrolle und Berichtspflichten bedarf, um den Zugang zu süchtig machenden Inhalten zu beschränken und die Transparenz zu erhöhen. Die Studie hebt hervor, dass das Einführen von Maßnahmen zur Prävention wider dem Geschäftsmodell der digitalen Dienste ist, welches darauf abzielt, eine möglichst hohe Nutzungszeit und damit erhöhte Werbeeinnahmen zu erzielen.

Der Digital Services Act schafft eine Handhabe zur Begegnung zahlreicher dieser Risiken, so durch die Vorschriften des Art. 28 DSA zum Kinder- und Jugendschutz sowie im Falle von sehr großen Online-Plattformen und Online-Suchmaschinen durch die Vorschriften des Art. 34/35 zur Bewertung und Minderung systemischer Risiken auf den entsprechenden Diensten. Sowohl die EU-Kommission als auch nationale DSCs bzw. zuständige Behörden wie BzKJ und LMA führen bereits Verfahren mit Blick auf die Durchsetzung dieser Vorschriften bzw. wirken durch Übermittlung von Informationen an Verfahren der EU-Kommission sowie grenzüberschreitenden Verfahren anderer DSCs mit.

Die Kommission hat am 06.02.2026 vorläufige Feststellungen veröffentlicht, dass die Online-Plattform TikTok die Risiken seines süchtig machenden Designs nicht ausreichen bewertet und gemindert habe. Zu diesen Designs zählen Infinite Scroll, Autoplay, Push-Benachrichtigungen und hochpersonalisierte Empfehlungen.

- c. Hate Speech, Desinformation sowie verschwörungsideologische und extremistische Inhalte, Belästigung/Cybermobbing und weitere Interaktionsrisiken (z. B. Doxxing, Stalking, koordinierte Angriffe),

Der DSC ist nicht für die Bewertung von Inhalten zuständig. Der DSC nimmt also keine Bewertung vor, ob ein konkreter Inhalte Hate Speech oder Desinformation darstellt. Auch möchten wir darauf hinweisen, dass Desinformation grundsätzlich nicht rechtswidrig ist, jedoch im Einzelfall rechtswidrig oder sogar strafbar sein kann (z.B. Betrug, Holocaustleugnung).

¹ Abrufbar unter

https://www.dsc.bund.de/DSC/DE/Aktuelles/studien/GesellschaftlicheAuswirkungenSuchtgefahren.pdf?__blob=publicationFile&v=3

Die EU-Kommission führt in ihren Leitlinien zur Minderung systemischer Risiken in Wahlprozessen vom 26.04.2024² aus, dass ausländische Desinformationskampagnen ein systemisches Risiko für Wahlprozesse und die gesellschaftliche Debatte im Sinne von Art. 34 Abs. 1 lit. c DSA darstellen können. Die EU-Kommission ist für die Durchsetzung der Vorschriften der Art. 34/35 über systemische Risiken ausschließlich zuständig.

Im Rahmen unserer Tätigkeit erreichen uns Informationen und Studien von anderen Behörden und sonstigen Stakeholdern, dass mögliche Desinformation in systemischen Ausmaßen insbesondere von Fake Accounts und Bot Accounts aus dem Ausland im Rahmen von ausländischen Desinformationskampagnen („Doppelgänger“, „Storm-1516“) sowie über Werbung auf digitalen Diensten ausgespielt werden. Wirksame Gegenmaßnahmen von sehr großen Online-Plattformen und Suchmaschinen nach Art. 34/35 DSA können etwa Anpassung der Algorithmen und ein Vorgehen gegen Fake Accounts sowie entsprechende Werbeanzeigen sein.

Die EU-Kommission führt bereits einige Verfahren, in denen diese Risiken mit Blick auf die Einhaltung von Art. 34/35 DSA untersucht werden.

- d. Selbstgefährdungsrisiken (z. B. Selbstschädigung/Suizid, Essstörungen, gefährliche Challenges),

Grundsätzlich verstärken interaktionsbasierte Algorithmen die Ausspielung von bestimmten Inhalten. Entsprechend würden Inhalte mit Selbstgefährdungsrisiken dem User bei einer entsprechenden Neigung verstärkt ausgespielt.

² Abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:C_202403014

Hier erscheint ebenfalls eine Anpassung von Algorithmen sinnvoll. Insoweit ist die EU-Kommission für die Durchsetzung der Vorschriften über systemische Risiken nach Art. 34/35 DSA ausschließlich zuständig.

- e. kommerzielle Ausnutzung sowie Daten- und Privatsphäre-Risiken (z. B. profiling/Tracking, irreführende Werbung, Scams)?

Mangels Zuständigkeit für den Datenschutz ist insoweit keine Antwort durch den DSC möglich.

- 2. Welche Rolle spielen dabei konkrete Gestaltungsentscheidungen von Diensten (z.B. Default-Einstellungen, Empfehlungs- und Rankingsysteme, Sharing-/Kontaktfunktionen, Interface-Design, Parental-Control-Funktionen)?

Der DSC verweist auf die Leitlinien der EU-Kommission zu Art. 28 DSA³, die einen Leitfaden zur Umsetzung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen innerhalb digitaler Dienste sind. Bei der Erstellung der Leitlinien zu Art. 28 DSA hat die EU-Kommission bereits die Informationen vieler Experten im Rahmen einer öffentlichen Konsultation gesammelt und in den Leitlinien berücksichtigt. Darüber hinaus gab es in der weiteren Abstimmung eine Kommentierung durch die zuständigen Behörden.

- 3. Wie können Diensteanbieter algorithmisch verstärkte Risiken (z.B. durch KI-basierte Empfehlungen und Profiling) erkennen, bewerten und wirksam mindern?

Durch den Einsatz KI-basierter Empfehlungssysteme entstehen grundsätzlich keine neuen Risiken, bereits vorhandene Probleme können jedoch hierdurch verstärkt werden. Zur Erkennung, Bewertung und wirksamen Minderung sind wirksame und kindgerechte Meldeverfahren, mediale Bildung von Kindern und Jugendlichen, Eltern und LehrerInnen und eine Anpassung der Ausgestaltung dieser Algorithmen notwendig.

³ Abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:C_202505519

Maßnahmen der Diensteanbieter können etwa der Einsatz chronologischer Feeds (als Default Einstellung) anstatt interaktionsbasierter Empfehlungssysteme, die Umleitung auf Hilfeseiten bei jugendgefährdenden Suchanfragen und die Einschränkung von Nutzungszeiten zu bestimmten Uhrzeiten sein.

Benennen Sie nach Möglichkeit Prioritäten (Top-3-Maßnahmen) und Kriterien/Indikatoren, wie die Wirksamkeit von Maßnahmen überprüft wird/werden sollte.

Mangels Zuständigkeit für die Durchsetzung des Art. 28 DSA kann der DSC insoweit keine Antwort dazu geben, wie die Wirksamkeit von Maßnahmen überprüft werden kann. Aus anderen Ländern haben wir erfahren, dass etwa ein Vergleich von bestimmten Parametern vor und nach Einführung von Maßnahmen hilfreich sein kann, etwa wie lange durchschnittliche tägliche Nutzungszeit von Minderjährigen auf Social Media oder die Ausspielung an bzw. bewusste Nutzung von pornografischen Inhalte durch Minderjährige vor/nach einer Maßnahme ist. Tritt nach einer Maßnahme eine statistisch signifikante Minderung ein, könnte dies auf die Wirksamkeit einer Maßnahme hindeuten.

II Plattformverantwortung, Regulierung und Durchsetzung

1. Wie sollte die Verantwortung der Plattformbetreiber gegenüber Kindern und Jugendlichen rechtlich und praktisch konkretisiert werden (z.B. Sorgfaltspflichten, Risikoanalysen, Melde- und Abhilfewege, Transparenzpflichten)?

Der DSA enthält bereits Vorschriften zur Adressierung der genannten Risiken durch Plattformbetreiber, hierunter so z.B.

- zur Ausgestaltung von Allgemeinen Geschäftsbedingungen in verständlicher kinder- und jugendgerechter Sprache, wenn sich der Dienst in erster Linie an Minderjährige richtet oder überwiegend von Minderjährigen genutzt wird (Art. 14 Abs. 3 DSA),
- zum Online-Schutz Minderjähriger (Art. 28 DSA) sowie
- zur Bewertung und Minimierung von systemischen Risiken auf sehr großen Online-Plattformen und Suchmaschinen, hierunter nachteiligen Auswirkungen in Bezug auf den Schutz von Minderjährigen (Art. 34 Abs. 1 UAbs. 2 lit. d DSA i.V.m. Art. 35 DSA).

2. Wie lässt sich die Verantwortung der Plattformbetreiber überprüfbar ausgestalten (z.B. Audits, Reporting, unabhängige Aufsicht, Beteiligung von Kindern und Zivilgesellschaft)?

Die genannten Vorschriften des DSA zum Kinder- und Jugendschutz werden bereits durch die nationalen Behörden (BzKJ, LMA, BzKJ) sowie durch die DSCs und zuständigen Behörden anderer Mitgliedsstaaten und die Europäische Kommission durchgesetzt.

Hierzu sind bereits Verfahren anhängig.

4. Wie kann die Umsetzung bestehender Vorschriften – insbesondere der Vorgaben zum Schutz Minderjähriger nach Artikel 28 DSA samt Leitlinien der Kommission – sowie des JMStV und JuSchG verbessert werden?

Die Umsetzung des Artikel 28 DSA wird insbesondere durch die Ausnahmeregelung für Kleinst- und Kleinunternehmen aus Art. 19 DSA erschwert. Wie sich bereits jetzt in Deutschland und anderen EU-Mitgliedstaaten zeigt, entfällt für eine Vielzahl digitaler Dienste die Pflicht für Kinder- und Jugendmedienschutz gemäß Art. 28 das aufgrund der Ausnahme für Kleinst- und Kleinunternehmen.

Kriterien für die Bestimmung von Kleinst- und Kleinunternehmen nach der Empfehlung 2003/361/EG, auf die Art. 19 DSA Bezug nimmt, sind v.a. die Anzahl der Mitarbeiter und der Umsatz. Diese Kriterien sagen nichts über die Nutzerzahlen und Reichweite eines Dienstes aus.

5. Gibt es aus Ihrer Sicht Regelungslücken im Bereich des technischen Kinder- und Jugendmedienschutzes, und welche Instrumente wären geeignet, diese wirksam zu schließen?

Die Europäische Kommission hat im Rahmen des DSA eine EU-weite Altersverifikationslösung entwickeln lassen. Diese muss von den Mitgliedstaaten auf die nationalen Gegebenheiten angepasst und betrieben werden. Die EU Age Verification App soll dabei eine Übergangslösung zur EUID-Wallet darstellen. In

Deutschland gibt es aktuell keine Regelung, welche eine Zuständigkeit für die nationale Implementierung der App vorsieht.

Dem DSC ist auch nicht bekannt, dass eine Altersverifikation im Zuge der Einführung der EUID-Wallet in Deutschland vorgesehen ist. Dies ist technisch möglich, jedoch bisher nach unserer Kenntnis nicht in den Spezifikationen vorgesehen. Insbesondere von Anbietern wird eine EU-weite Lösung bevorzugt.

6. Welche Rolle spielen starke Verschlüsselungslösungen (z.B. Ende-zu-Ende-Verschlüsselung) für den Schutz von Kindern – und welche Spannungsfelder ergeben sich mit Überwachungs- und Interventionsmöglichkeiten?

Der DSC kann hierzu mangels Zuständigkeit und Berührungspunkten zu seiner Tätigkeit keine Antwort geben.

7. Welche Rolle sollen Betriebssysteme und App-Stores für den technischen Jugendmedienschutz übernehmen (z.B. geräteweite Jugendschutzeinstellungen, einheitliche Altersstufen-/Label-Standards, Default- und Kaufbeschränkungen) und welche regulatorischen Instrumente wären dafür geeignet?

Technische Lösungen mit datensparsamen Ansätzen sind grundsätzlich zu begrüßen, allerdings kann dies nicht Diensteanbieter aus der Pflicht entlassen, ihre Dienste kinder- und jugendgerecht auszugestalten.

Dem DSC sind die Vorschläge von Diensteanbietern (hierunter u.a. Anbietern von Pornoplattformen), eine Altersverifikation ausschließlich über Betriebssysteme und App-Stores auszugestalten, bekannt. Sollte eine solche technische Lösung auf Ebene des Betriebssystems oder des App Stores in Erwägung gezogen werden, müsste eine solche Lösung je nach konkreter Ausgestaltung sorgfältig evaluiert und die Einbindung der über diese realisierten bzw. vermarkteten Dienste digitalen Dienste sichergestellt werden. Mangels weiterer Informationen zur konkreten Ausgestaltung kann hierzu keine genauere Aussage getroffen werden.

Unabhängig davon würde ein allein über einen App Store ausgestalteter technischer Jugendmedienschutz nicht ausreichend sein. Digitale Dienste können

auch auf anderem Wege in Anspruch genommen werden, z.B. über einen Download der App auf der Webseite des Anbieters. In dem Fall würde ein technischer Jugendmedienschutz fehlen.

8. Welche wirtschaftlichen und betrieblichen Implikationen gehen mit einem umfassenden Jugendmedienschutz einher?

Durch eine kinder- und jugendgerechte Ausgestaltung des Dienstes, welche ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen gewährleistet, entstehen den Diensteanbietern Kosten bei der Ausgestaltung dieser Anforderungen.

Darüber hinaus werden den Diensteanbietern möglicherweise Werbeeinnahmen entfallen, da die Ausspielung von nicht-minderjährigengerechter Werbung angepasst werden müsste und eine Anpassung von interaktionsbasierten Empfehlungssystemen möglicherweise die Verweildauer von Kindern und Jugendlichen auf den Plattformen reduziert.

Zudem könnten durch die Ausgestaltung wirksamer Meldewege weitere laufende Kosten durch den Einsatz von KI-basierter Systeme und/oder Moderationsteams entstehen.

III Altersgrenzen, Altersverifikation und spezifische Schutzräume

Halten Sie verbindliche Altersgrenzen für bestimmte digitale Angebote für erforderlich, und wenn ja: Nach welchen Kriterien sollten diese festgelegt werden?

1. Wie sollte eine altersangemessene Altersverifikation rechtlich und praktisch ausgestaltet werden?
2. Welche Formen der Altersabsicherung (Age-Assurance wie Schätzung, Verifikation, Token-, Wallet-basierte Nachweise) halten Sie für geeignet und wie können Over-Collection, Diskriminierung und Umgehbarkeit vermieden werden?
3. Braucht es aus Ihrer Sicht speziell gestaltete digitale Räume für Kinder und Jugendliche mit begrenztem oder ausgeschlossenem Zugang für Erwachsene, und wie ließen sich solche Räume technisch, rechtlich und organisatorisch realisieren?

Die Fragen III 1.-3. werden zusammen beantwortet. Der DSC hat in dieser Hinsicht keine Zuständigkeit, jedoch möchten wir auf Folgendes hinweisen: Die Implementierung von Altersverifikationssystemen für sich allein ist nicht ausreichend, den Vorschriften des Art. 28 DSA und – im Falle von sehr großen Online-Plattformen und Online-Suchmaschinen – Art. 34/35 DSA zu genügen. Der Einsatz eines Altersverifikationssystem alleine ist also nicht ausreichend, um einen ausreichenden Kinder- und Jugendschutz zu gewährleisten.

Bei Einführung einer Altersgrenze können Minderjährige zudem keine Medienkompetenz ausbilden und würden nach Eintritt der Altersgrenze erstmalig den Risiken ausgesetzt, dies sich aktuell auf digitalen Diensten finden.

Bei der Implementierung einer Altersverifikation ist insbesondere eine möglichst datensparsame Lösung zu bevorzugen, um ein hohes Maß an Privatsphäre zu gewährleisten.

IV Chancen, Teilhabe und spezielle Problemfelder

1. Welche Chancen für Information, Bildung, Beteiligung und Freizeit ergeben sich durch technischen Kinder- und Jugendmedienschutz, wenn er beispielsweise „by design“ in digitale Dienste integriert wird?

Wird ein Dienst kinder- und jugendgerecht ausgestaltet, so können Minderjährige in vielfacher Hinsicht nach den dem DSC vorliegenden Erkenntnissen und Einschätzungen zuständiger Stakeholder profitieren, so etwa durch politische Teilhabe, Förderung von kreativen Prozessen und sozialer Interaktion mit anderen Kindern und Jugendlichen.

2. Wie kann ein übermäßiger Medienkonsum von Kindern und Jugendlichen wirksam begrenzt werden, und welche Verantwortung tragen Anbieter hinsichtlich der Designentscheidungen, der Nutzungsdauer und des digitalen Engagements (Interaktionen)?

Nach den dem DSC vorliegenden Erkenntnissen und Einschätzungen zuständiger Stakeholder sind Designentscheidungen der zentrale Einflussfaktoren für die Nutzungsdauer und das digitale Engagement (d.h. Interaktion durch User) auf digitalen Diensten. Digitale Dienste sind durch ihr Design auf eine lange Nutzungsdauer und eine hohe Interaktion durch User, hierunter auch Kinder und Jugendliche, angelegt, da sie sich über Werbung finanzieren.

Eine entsprechende Anpassung des Designs digitaler Dienste kann entsprechend einem übermäßigem Medienkonsum von Kindern und Jugendlichen entgegenwirken, z.B. durch Unterbindung von sog. „Doom Scrolling“ (endlosem Scrollen) oder Anpassung der algorithmischen Empfehlungssystemen (z.B. durch Einstellung eines chronologischen Feeds als Default).

- 3.** Wie kann in Fällen von Sharenting und Family-/Kinder-Influencing einem Missbrauch von Bildern und personenbezogenen Daten technisch, regulatorisch und durch Medienbildung vorgebeugt werden?

Insoweit liegt keine inhaltliche Berührung zu den Aufgaben des DSC vor.