

Schriftliche Stellungnahme zum Hearing 2 „Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste“ der unabhängigen Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt“

Team klicksafe und Team Kinder- und Jugendmedienschutz, Medienanstalt Rheinland-Pfalz

06.02.2026

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?

Aus Sicht von *klicksafe* als europäischer Safer-Internet-Initiative in Trägerschaft der Medienanstalt Rheinland-Pfalz ist ein wirksamer Kinder- und Jugendmedienschutz durch ein integriertes Zusammenspiel von:

- verbindlicher Regulierung und konsequenter Aufsicht,
- effektiver Ko-Regulierung unter hinreichender Wahrung von kinder- und jugendbezogenen Gemeinwohlinteressen durch anerkannte Einrichtungen freiwilliger Selbstkontrolle
- verantwortungsvoller Plattformgestaltung („Safety by Design & by Default“)
- Aktivierung der Verantwortlichkeit von Medienintermediären bzw. VLOS und VLOP (namentlich Suchmaschinen und sozialen Netzwerken) für einen effektiven und nachhaltigen Kinder- und Jugendmedienschutz
- konsequenter Beachtung inhalte- und infrastrukturbezogener Risiken von KI für eine positive, dem Wohl von Kindern und Jugendlichen verpflichteten Medienordnung sowie grundrechte- und grundwertesensibler Ausgestaltung von Aufsichtstools unter Einbindung von KI
- Beachtung des Subsidiaritätsprinzips für eine wirksame und minderjährigennahe Durchsetzung geltenden Kinder- und Jugendmedienschutzrechts
- starker Medien-, einschließlich Digital- und KI-Kompetenzförderung aller Zielgruppen mit besonderer Berücksichtigung interkultureller und internationaler Herausforderungen
- Wissenstransfer von der phänomenologischen Expertise von jugendschutz.net in die Arbeit dritter Einrichtungen des Kinder- und Jugendmedienschutzes

zu erreichen.

I. Risiken, Schutzmaßnahmen und Gestaltung digitaler Dienste

1. Wirksamste Maßnahmen zur Risikominderung

Auch wenn für die nachfolgenden einzelnen Bereiche passende Empfehlungen abgegeben werden, bleibt die verlässliche Altersprüfung die wichtigste Maßnahme, um Kinder und Jugendliche vor nicht altersgemäßen Risiken zu schützen. Alle nachgelagerten (und durchaus

sinnvollen Maßnahmen innerhalb der Dienste) können die Problematik einer Falschangabe bei Erstanmeldung nicht auffangen.

Darüber hinaus ist zu überlegen, ob Dienste zu Standardisierungen ihrer Maßnahmen(darstellung) aufgefordert werden können, da diese in jedem Dienst anders funktionieren und dargestellt werden.

a) Digitale sexualisierte Gewalt

- verpflichtende Risikobewertungen
- standardmäßig restriktive Kontaktfunktionen für Minderjährige
- technische Grooming-Erkennungssysteme unter strengen Datenschutzauflagen
- Schutzfunktion Sextortion: Verhinderung von Nacktheit in Direktnachrichten der Plattformen
- leicht zugängliche Melde- und Notfallmechanismen
- enge Kooperation mit Strafverfolgungsbehörden, Beratungs- und Meldestellen

b) Suchtbegünstigende Gestaltungspraktiken

- Verbot bzw. strenge Regulierung von Dark Patterns
- Abschaffung manipulativer Mechaniken wie Endlos-Scroll oder variable Belohnungssysteme für Minderjährige
- transparente Kennzeichnung von Lootboxen (keine Lootboxen für Kinder)
- altersabhängige Nutzungszeitbegrenzungen
- enge Zusammenarbeit von Kinder- und Jugendmedienschutzeinrichtungen mit Einrichtungen der Suchtbekämpfung und -prävention sowie mit den Glücksspielaufsichtsbehörden, namentlich der GGL

c) Hate Speech, Desinformation, Extremismus

- algorithmisches Downranking und Einsatz von Deamplification-Mechanismen (geringere oder Unterbindung algorithmischer Verbreitung: beispielsweise bei Empfehlungen, Trends, „Für Dich“-Feeds)
- verpflichtende Reaktionsfristen der Anbieter
- altersangepasste Empfehlungslogiken
- stärkere Kontextualisierung problematischer Inhalte
- Markierung von zweifelhaften Quellen
- Förderung geprüfter Informationsquellen
- enge Zusammenarbeit von Kinder- und Jugendmedienschutzeinrichtungen mit Faktencheckern sowie Einrichtungen der Extremismusforschung und -bekämpfung

d) Cybermobbing und Interaktionsrisiken

- einfache Blockier-, Stummschaltungs- und Reportfunktionen
- Default-Einstellungen mit eingeschränkter Sichtbarkeit
- verpflichtende Reaktionsfristen der Anbieter

- Hinweise auf Opferunterstützung
- enge Zusammenarbeit von Kinder- und Jugendmedienschutzeinrichtungen mit Einrichtungen zur Bekämpfung von Cyberkriminalität
- Aktivierung der Verantwortlichkeit von Finanzdienstleister*innen und Influencer*innen für einen effektiven und nachhaltigen Kinder- und Jugendmedienschutz

e) Selbstgefährdungsrisiken

- KI-gestützte Erkennung kritischer Muster
- verpflichtende Kriseninterventionen (z. B. Hilfsangebote)
- keine algorithmische Verstärkung selbstschädigender Inhalte
- Zusammenarbeit mit anerkannten Hilfestellen der Suizidprävention

f) Kommerzielle Ausnutzung und Datenschutzrisiken

- konsequente Durchsetzung bestehender Schutzmechanismen in der DSGVO und der KI-Verordnung der EU
- Verbot von Profiling zu Werbezwecken bei Minderjährigen
- datensparsame Grundeinstellungen
- klare Trennung von Werbung und Inhalt

2. Rolle von Gestaltungsentscheidungen

Gestaltungsentscheidungen sind zentraler Hebel für Prävention. Gefährdungen entstehen häufig nicht durch Inhalte allein, sondern durch deren systemische Verstärkung.

Besonders relevant sind:

- Default-Einstellungen (privat statt öffentlich)
- transparente Empfehlungslogiken
- altersangepasste Interface-Gestaltung
- wirksame Parental-Control-Systeme
- Auffindbarkeit von Schutzeinstellungen

3. Umgang mit algorithmisch verstärkten Risiken durch Diensteanbieter

Plattformen müssen verpflichtet werden zu:

- regelmäßigen algorithmischen Risikoanalysen
- Offenlegung zentraler Parameter gegenüber Aufsichtsbehörden
- externen Algorithmus-Audits
- nachweisbaren Minderungsmaßnahmen

4. Prioritäten

1. Verbindliche Risikoanalysen mit Aufsichtskontrolle
2. Eröffnung externer Algorithmenprüfung
3. Praktisches Testverfahren / Systemtest / Testprofile

Wirksamkeitsindikatoren:

- Reduktion gemeldeter Vorfälle
- geringere Nutzungsdauer und Nutzungstiefe

II. Plattformverantwortung, Regulierung und Durchsetzung

1. Konkretisierung der Verantwortung

- Evaluierung und ggf. Modifizierung des bisherigen Verbots von ex-ante-Kontrollen
- gesetzlich definierte, altersdifferenzierte Sorgfaltspflichten
- verpflichtende Risiko- und Folgenabschätzungen mit Vorschlägen zur Minimierung/Reduzierung von Risiken
- transparente, leicht erreichbare und verständliche Melde- und Abhilfeprozesse
- Berichtspflichten

2. Überprüfbarkeit

- Unabhängige, staatsferne Aufsicht und Regulierung
- standardisierte Transparenzberichte
- Beteiligung von Kindern, Jugendlichen, Zivilgesellschaft

3. Verbesserung der Umsetzung bestehender Vorschriften

- bessere Verzahnung von DSA, JMStV und JuSchG
- Anerkennung fortbestehender mitgliedstaatlicher Gestaltungsspielräume im Interesse eines bestmöglichen Kinder- und Jugendmedienschutzes
- Stärkere Beachtung des Marktortprinzips bei Gefährdungen für das Kindeswohl durch Angebote aus dem (EU-) Ausland
- Beschleunigte Verfahren für die Feststellung eines systemischen Versagens von Vermittlungsdiensten und Suchmaschinen
- klare Zuständigkeiten auf europäischer und nationaler Ebene
- Vernetzung zuständiger Stellen
- ausreichende Ressourcen für Aufsichtsbehörden und Trusted Flagger

4. Regelungslücken

- Pflicht zu verlässlicher Altersprüfung bei Account-Eröffnung
- Algorithmen-Einschränkung (Unterbindung Scrolling, Empfehlungssysteme für Minderjährige)
- Änderungen an Verantwortungskaskade; Verzicht auf strenges Subsidiaritätsprinzip bei Inanspruchnahme von Content-, Host- und Access Providern
- Verbot von Nudify-Apps
- KI-Kennzeichnung

5. Verschlüsselung

Starke Verschlüsselung ist zentral für den Schutz der Privatsphäre, allerdings ist nicht ersichtlich, dass damit automatisch ein verbesserter KJMS einher geht, da die Maßnahme für alle Nutzer*innen zur Verfügung steht, ggf. also auch für Erwachsene, die sich als minderjährig ausgeben.

Eine Ende-zu-Ende-Verschlüsselung kann automatisierte Inhaltsanalysen, Erkennung illegaler Inhalte verhindern und damit das Aufdecken z.B. von sexualisierter Gewalt gegen Kinder, die Identifizierung von Täter-Netzwerken sowie frühzeitige Intervention bei akuter Gefährdung auch erschweren.

Andererseits eröffnen schwächere technische Maßnahmen andere Missbrauchsformen (Massenüberwachung o.ä.).

- präventive Designmaßnahmen vor der Verschlüsselung
- klare Meldewege
- keine anlasslose Massenüberwachung

6. Rolle von Betriebssystemen und App-Stores

- Gatekeeper-Funktion (Zugang, Definition technische Standards, Entscheidung über Sichtbarkeit und Funktionalität) unter gesetzlich verankerten Kriterien
- Herstellung von Kinder- und Jugendmedienschutz by Design und by Default
- Bereitstellung von Vorgaben für Kinder- und Jugendprofile
- Konfigurationsoptionen für Einschränkungen für bestimmte Altersgruppen

7. Wirtschaftliche Implikationen

- Eingeschränkte Werbe- und Verkaufsmöglichkeiten
- Verringerung von Haftungsrisiken, wenn KJMS ordnungsgemäß zur Anwendung kommt/Rechts- und Planungssicherheit
- Vertrauens- und Renommee Gewinn / Investor*innen

III. Altersgrenzen, Altersverifikation und Schutzräume

1. Altersgrenzen

- Pornografie nur für Erwachsene
- Glücksspiel, glücksspielähnliche Elemente nur für Erwachsene
- Kontaktabbau nur für Erwachsene
- Angebote/Dienste mit algorithmischer Personalisierung / Einsatz von Dark Patterns nur für Erwachsene
- Social Media nicht für Kinder, erst ab Jugendalter

Kriterien:

Nutzung vorhandener Kriterien zur Altersabstufung bzw. Verbot unzulässiger Inhalte

2. Altersverifikation

Zielsetzung bei Altersverifikation muss sein, dass die altersgemäße Zugänglichkeit geregelt ist, nicht die Identifizierbarkeit von Personen. Orientierung an Verhältnismäßigkeit, Datensparsamkeit, Zweckbindung und Schutz der Grundrechte.

Erforderlich ist ein risikobasierter Ansatz:

- niedriges Risiko → Altersschätzung
- hohes Risiko → verlässliche Verifikation

Beispiel:

Bildungsangebote ohne Interaktion – Zugang mit Selbstdeklaration

Angebote mit Kommunikationsoptionen o.ä. – technische Altersabsicherung

Pornografie/Glücksspiel – verlässliche Altersverifikation

Für alle Risiko-Stufen gibt es bereits funktionierende Systeme. Es braucht jedoch noch eine einheitliche, für den europäischen Markt anerkannte AVS-Lösung, die große Plattformanbieter mit Sitz in anderen europäischen Ländern implementieren sollten.

3. Geeignete Altersabsicherungen

- risikobasiert (je höher das Gefährdungspotenzial, desto stärker die Absicherung)
- attributsbasiert (Alter statt Identität)
- datensparsam
- barrierearm und diskriminierungsfrei
- technisch kombinierbar

4. Spezifische Schutzräume für Kinder und Jugendliche

Altersgerechte digitale Räume sind notwendig und sinnvoll, sofern:

- klare Zugangsbeschränkungen bestehen
- pädagogische Konzepte integriert sind
- kontinuierliches Missbrauchsmonitoring gewährleistet ist

IV. Chancen, Teilhabe und spezielle Problemfelder

1. Chancen durch technischen Jugendmedienschutz (by design)

- altersangemessener Zugang zu Informationen
- vertrauenswürdige digitale Umgebungen
- sichere Nutzung digitaler Lernangebote
- sichere digitale Beteiligung
- Stärkung demokratischer und digitaler Kompetenzen
- Verringerung von Silencing Effekten
- Schaffen von Vertrauen in digitale Kommunikation, wenn diese sicher ist.

- Soziale Vernetzung ohne Belästigungen oder Gefährdungen
- Förderung von Kreativität
- Weniger Bloßstellung, weniger Druck
- Self-Empowerment

2. Begrenzung übermäßigen Medienkonsums

- transparente Nutzungszeitinformationen
- Abschaltung suchtfördernder Mechaniken
- Anbieterpflichten zur Nutzungssteuerung

3. Sharenting und Kinder-Influencing

Erforderlich sind:

- Kinderrechte vor Wirtschaftsinteressen der Eltern stellen.
- technische Schutzmechanismen gegen Weiterverbreitung
- intensive Medienbildungsarbeit für Eltern

Team klicksafe, Leitung Deborah Woldemichael

Team Kinder- und Jugendmedienschutz, Leitung Doris Westphal-Selbig