

Januar 2026

Schriftliche Stellungnahme für die Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt“

der T-Systems International GmbH

Hearing 2 – Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler
Dienste

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?

Antwort zur Leitfrage

Die wirksamste Strategie basiert auf drei ineinandergreifenden Säulen: Technische Maßnahmen müssen Sicherheit „by design“ in Plattformen verankern, nicht als nachträgliche Ergänzung. Regulatorische Maßnahmen müssen klare Verantwortung für Plattformen schaffen und deren Durchsetzung mit Konsequenzen verbinden. Pädagogische Maßnahmen befähigen Kinder und Jugendliche, Technologien kritisch zu reflektieren und Manipulationen zu erkennen.

Diese Kombination ist entscheidend: Technik ohne Regulation schafft Schlupflöcher, Regulation ohne Technik wird umgangen (siehe die Möglichkeiten der self declaration bei der Altersverification unter dem DAS), Pädagogik ohne systemische Änderungen belastet Individuen mit Verantwortung, die eigentlich die Systeme sowie die Plattformen bzw. Anbieter gefährdender Inhalte selbst tragen sollten.

Kapitel I: Risiken, Schutzmaßnahmen und Gestaltung digitaler Dienste

Der technische Jugendmedienschutz muss sich gegen sechs zentrale Risikogruppen richten: sexualisierte Gewalt, suchtfördernde Praktiken, schädliche Inhalte, Mobbing, Selbstgefährdung und kommerzielle Ausnutzung. Die Gestaltung von Plattformen – von Default-Einstellungen bis zu Algorithmen – bestimmt dabei fundamental, ob diese Risiken entstehen oder von vorneherein minimiert werden. Besonders wichtig – wenn auch herausfordernd zu steuern und überprüfen und nur durch kluge Regulierung möglich – ist die Erkennung und Minderung algorithmisch verstärkter Risiken durch unabhängige Risikoanalysen, transparente Empfehlungssysteme und Nutzer-Kontrolle über Algorithmen.

I.1. Maßnahmen gegen spezifische Risiken

a) Digitale sexualisierte Gewalt (Cybergrooming, Sextortion, Missbrauchsdarstellungen)

Automatische Erkennung verdächtiger Kontaktmuster (z.B. schneller Vertrauensaufbau, Isolationversuche) kombiniert mit strikten Default-Einstellungen bei Kontaktfunktionen (Private Nachrichten nur von bekannten Kontakten, Altersunterschiede-Warnung). Automatische Content-Filter für CSAM und Sextortion-Versuche sowie einfach auffindbare Meldungskanäle mit menschlicher Prüfung sind essentiell.

Top-Maßnahmen:

- Standardmäßig aktivierte Beschränkungen (private Nachrichten nur von bekannten Kontakten, Altersunterschiede-Warnung)
- Automatische Erkennung von Grooming-Mustern (Sprach-/Bildanalyse)
- Blockierung verdächtiger Links/Dateien vor Zugriff durch Kinder
- Altersgerechte Aufklärung über Cybergrooming (in-App-Interventionen)

b) Suchtbegünstigende/hochgradig bindende Gestaltungspraktiken (Lootboxen, Dark Patterns)

In Spielen sollte eine Transparenzpflicht für Lootbox-Gewinnwahrscheinlichkeiten in Klartext und Anzeige aller Kosten in echter Währung gelten. Ein Verbot manipulativer Designs (Infinite Scroll ohne aktive Nutzer-Interaktion, erzwungene Weiterleitungen zu kostenpflichtigen Inhalten) kann zudem auf Social Media Plattformen Suchtmuster reduzieren. Zudem sollte es für Minderjährige tägliche/wöchentliche Ausgabenlimits und Mandatory Break-Reminders nach bspw. 90 Minuten geben.

Top-Maßnahmen:

- Engagement-Ziele NICHT auf Maximierung von Nutzungsdauer oder In-App-Ausgaben optimieren
- Empfehlungssysteme sollten Wohlbefinden priorisieren (z.B. Engagement-Breaks, Inhaltsvielfalt)
- Lootboxen-Beschränkung: Mindestens Kennzeichnungspflicht, übergeordnet zu prüfen: Altersbeschränkung ≥ 16 oder ≥ 18 für Titel mit Lootboxen, alle Kosten in echter Währung sichtbar machen (keine versteckte oder variable Währung)
- Infinite Scroll nur mit aktiver Benutzer-Interaktion (kein automatisches Vorwärtsscrollen)
- Tägliche/wöchentliche/monatliche Ausgabenlimits (plattformübergreifend)
- Mandatory Break-Reminders nach 90 Min. (Angabe zur Bildschirmzeit, Aufforderung zu Pause)

c) Hate Speech, Desinformation und extremistische Inhalte

Um problematische Inhalte effektiv zu adressieren, können auf problematischen Plattformen KI-basierte Inhaltsfilter mit Kontextverständnis (statt reinem Keyword-Matching) eingesetzt werden. Empfehlungssysteme („Recommendation systems“) müssen insbesondere auf Social Media, wo sie enormen Einfluss haben, problematische Beiträge algorithmisch abwerten; ergänzend können bei identifizierten Desinformationen automatisch Gegenargumente und Fact-Checker-Links eingeblendet werden. Für eskalierte Inhalte sollten stets Rapid-Response-Teams der Anbieter/Plattformbetreiber bereitstehen.

Top-Maßnahmen:

- Priorisierung problematischer Inhalte in Empfehlungen (Algorithmische Abwertung, nicht nur Löschung)
- Rapid-Response-Teams für eskaliert problematische Inhalte
- KI-basierte Inhaltsfilter (Kontext verstehen, nicht nur Keyword-Matching)
- Sichere Räume fördern (z.B. verifizierte Informationsquellen)

d) Belästigung/Cybermobbing und weitere Interaktionsrisiken

Ein wirksamer Schutz vor Belästigung und Cybermobbing beginnt mit einem datenschutzorientierten Plattformdesign: Standortdaten, Geräteinformationen und Metadaten dürfen grundsätzlich nicht öffentlich einsehbar sein. Nutzerinnen und Nutzern muss es zudem unkompliziert möglich sein, belästigende Personen zu blockieren. Ergänzend sind leicht zugängliche Ressourcen für psychologische Unterstützung bereitzustellen, damit Betroffene bei Bedarf zeitnah Hilfe finden können.

- Datenschutz-by-Design (Standort, Geräte-Info, Metadaten sollten nicht öffentlich sein)
- Kontaktschutz (Anfragen von Fremden können blockiert werden, Gruppenbeitritte erfordern Zustimmung)
- Historien-Schutz (alte Posts nicht wiederauffindbar machen)
- Frühe Intervention der Plattformen (Warnungen, Konten-Sperren)
- Einfache Blockfunktionen und Melde-Mechanismen
- Psychologische Unterstützung (Ressourcen, Helpline-Links)
- Sperren von Tätern, ggf. Meldung an Behörden
- Aufklärung zu Cybermobbing und Konsequenzen

e) Selbstgefährdungsrisiken (Selbstschädigung/Suizid, Essstörungen, Challenges)

Um Risiken im Zusammenhang mit Selbstgefährdung, wie Essstörungen, Selbstschädigung oder Suizid, wirksam zu begegnen, ist eine automatische Erkennung entsprechender Inhalte unerlässlich. Empfehlungsalgorithmen müssen so gestaltet sein, dass sie derartige Inhalte nicht weiter eskalieren oder verbreiten. Stattdessen ist es wichtig, bei entsprechenden Suchanfragen oder Anzeichen für Selbstgefährdung gut sichtbare Hilfsangebote einzublenden – etwa Kontaktdaten von Krisentelefonen oder Fachstellen –, damit betroffene Personen unmittelbar Unterstützung erhalten können.

- Automatische Erkennung von Selbstgefährdungs-Inhalten (Text, Bilder, Videos)
- Algorithmische Unterbrechung: Empfehlungsalgorithmen dürfen Inhalte zu Essstörungen, Selbstschädigung oder Suizid nicht eskalieren/verbreiten
- Sichtbare Hilfsressourcen bei Suchanfragen zu Selbstschädigung (Krisentelefone, Fachstellen)

- Möglichkeit, vertrauenswürdige Personen zu benachrichtigen

f) Kommerzielle Ausnutzung sowie Daten- und Privatsphäre-Risiken

Um Minderjährige wirksam zu schützen, ist das Verbot von Verhaltens-Tracking und Profilbildung für diese Altersgruppe unerlässlich. Für Nutzer unter 18 Jahren sollte keine personalisierte Werbung ausgespielt werden. Private Nachrichten sollten durch End-to-End-Verschlüsselung abgesichert sein, um die Vertraulichkeit zu gewährleisten. Darüber hinaus sollte die Datenerhebung auf das notwendige Minimum begrenzt werden, wobei Betroffene jederzeit das Recht auf die Löschung ihrer Daten haben müssen.

- Keine Profilbildung auf Basis sensibler Kategorien (Gesundheit, sexuelle Orientierung, politische Überzeugungen etc.)
- Verbot von Verhaltens-Tracking für personalisierte Werbung (Art. 28 DSA)
- Tracking begrenzen auf funktionale Zwecke (Sicherheit, User Experience)
- Keine personalisierte Werbung für Minderjährige
- Transparente Kennzeichnung von Werbung & Influencer-Partnerschaften
- Klare Datenschutzerklärungen in Kindersprache

I.2. Gestaltungsentscheidungen als zentrale Hebel

Die Gestaltung ist nicht nebensächlich – sie bestimmt oft, ob Risiken entstehen. Sichere Defaults (private Profile, kein Tracking, keine personalisierte Werbung) müssen Standard sein, nicht versteckt hinter Opt-Outs. Empfehlungs- und Rankingsysteme sind fundamentale Risiko-Verstärker oder -Minimerer: Ein Algorithmus optimiert auf Wohlbefinden statt Engagement-Maximierung ändert das gesamte Risikoprofil. Sharing-/Kontaktfunktionen sollten standardmäßig restriktiv sein (Kontaktanfragen nur von bekannten Personen). Sicherheitsfunktionen müssen prominent und einfach erreichbar sein.

Lösungsansätze:

- Voreingestellt sollte immer die sicherste Variante sein (z.B. private Profile, keine Tracking, keine personalisierte Werbung)
- Sicherheitseinstellungen dürfen nicht versteckt sein
- Elternfunktionen sollten leicht zugänglich sein
- Manipulative Designs (versteckte Opt-Outs) sind unzulässig

I.3. Algorithmisch verstärkte Risiken erkennen und mindern

Plattformen müssen systematisch Risiken identifizieren – welche Inhalte werden am meisten für junge Nutzer empfohlen? Gibt es Muster bei Selbstgefährdung? Unabhängige Audits externer Prüfstellen und Daten-Transparenz für Forscher sind notwendig. Engagement-Maximierung als

Optimierungsziel muss verboten oder mindestens de-priorisiert werden zugunsten von Wohlbefinden, Inhaltsvielfalt und Lernförderung. Nutzer brauchen Kontrolle: einen Reset-Knopf für Empfehlungsalgorithmus und Einstellungen, um bestimmte Inhalts-Kategorien auszuschließen.

Lösungsansätze:

- Plattformen müssen systematisch Risiken identifizieren (z.B. welche Inhalte werden am meisten für junge Nutzer empfohlen? Gibt es Muster bei Selbstgefährdung?)
- Daten-Transparenz für Forscher (Zugang zu Algorithmus-Daten)
- Engagement-Maximierung als Ziel verbieten oder mindestens: De-Priorisieren schädlicher Inhalte. Alternative Ziele: Wohlbefinden, Inhaltsvielfalt, Lernförderung
- Reset-Knopf für Empfehlungsalgorithmus (Nutzer kann Geschichte löschen und "neue Schieferung" starten)
- Einstellungen, um bestimmte Inhalts-Kategorien auszuschließen

I.4. Prioritäten und Erfolgskriterien

Die Top-3-Maßnahmen übergreifend sind:

(1) Default-Security-Positionen – sichere Voreinstellungen als Standard, nicht als Opt-In;

(2) Plattformverantwortung durch regelmäßige unabhängige Risikoaudits mit öffentlich einsehbaren Sicherheitsberichten und Konsequenzen;

(3) Algorithmen-Transparenz & Nutzer-Kontrolle – wie Empfehlungen funktionieren muss offen gelegt werden, Nutzer brauchen Einstellungen (Algorithmus-Reset, Content-Ausschluss), und Engagement-Maximierung darf nicht schaden.

Erfolgskriterien sind technisch messbar: Beschwerden und Meldungen sollten sinken, Reaktionszeiten der Plattform unter 24 Stunden liegen. Durch Befragungen von Kindern/Jugendlichen (vor/nach) lässt sich das Sicherheitsgefühl messen. Die Prävalenz von Exposition gegenüber schädlichen Inhalten (CSAM, Hate Speech, Desinformation) sollte dokumentiert werden. Längerfristig: externe Audits überprüfen Plattform-Sicherheitsmaßnahmen unabhängig.

Kapitel II: Plattformverantwortung, Regulierung und Durchsetzung

II.1. Konkretisierung der Plattformverantwortung

Sorgfaltspflichten müssen vier Bereiche abdecken: (1) Risikoanalyse: Systematische Identifikation, welche Risiken für Kinder/Jugendliche auf der Plattform existieren, dokumentiert mit regelmäßigen Updates (mindestens jährlich); (2) Schutzmaßnahmen-Implementierung: Design-Anforderungen, Ressourcen-Allokation für Moderation und Sicherheit, regelmäßige Trainings und Audits; (3) Melde-

und Abhilfewege: einfache prominente Meldungskanäle mit Bearbeitungsfrist (24-48h für Dringendes), Begründung von Entscheidungen, Widerspruchsmöglichkeiten; (4) Transparenzpflichten: Offenlegung von Algorithmen-Funktionsweisen, jährliche Safety-Reports mit Statistiken, Daten-Zugang für Forschende.

Nationale Konkretisierung sollte DSA Art. 28 umsetzen: Verbot von Profiling-Werbung für U18, sichere Kontaktfunktionen, Anleitung in kindgerechter Sprache, schnelle Meldungssysteme, Zugang zu Support und Hilferessourcen.

II.2. Überprüfbarkeit durch Audits und Reporting

Die Überprüfbarkeit von Plattformen kann jederzeit durch regulatorische Stellen ausdefiniert werden. Diese können zum Beispiel verlangen, dass interne Audits, externe Audits durch akkreditierte Prüfsteller, und regulatorische Audits durch Behörden (BzKJ, Landesmedienanstalten) müssen systematisch erfolgen müssen. Jährliche Safety-Reports (öffentlich oder zusammengefasst), Content-Moderation-Berichte (Anzahl Verstöße pro Kategorie, Response-Zeiten), und Incident-Reporting für schwere Fälle (Sextortion, Suizidversuche) können in diesem Zusammenhang Transparenz für Nutzer, Gesellschaft und Regulatoren schaffen. Kinderbeiräte und Zivilgesellschafts-Meldungen ermöglichen externe Perspektive auf Plattform-Sicherheit.

II.3. Verbesserung der Umsetzung bestehender Vorschriften

Das Enforcement muss verstärkt werden: Bußgelder für Nicht-Compliance, Sperrungen für wiederholte Regelbrecher sowie transparente Verfahren mit dokumentierter Kommunikation. Die Leitlinien der EU-Kommission zu Art. 28 DSA vom 14. Juli 2025 bieten eine inhaltliche Grundlage, eine präzisierende nationale Konkretisierung durch das BzKJ sollte folgen. Neben rechtlichen Vorgaben braucht es auch konkrete technische Umsetzungsmöglichkeiten – etwa standardisierte, datenschutzfreundliche Altersverifikationslösungen auf EU-Ebene, z.B. die derzeit entwickelte EU Age Verification App, die im Auftrag der Europäischen Kommission u.a. von T-Systems konzipiert wird und EU-Mitgliedsstaaten sowie Plattformen eine interoperable, privacy-by-design-basierte Infrastruktur für die Umsetzung der Minderjährigenschutzanforderungen des DSA bereitstellt. Best-Practice-Sharing zwischen Plattformen, gezielte Forschungsförderung zum Verständnis von Plattformeffekten sowie technische Unterstützung (z.B. Open-Source-Tools für Inhaltsmoderation und Referenz-Implementierungen) können die praktische Umsetzung zusätzlich beschleunigen.

II.4. Regelungslücken und neue Instrumente

Häufig fehlen EU-einheitliche Vorgaben oder technische Referenzlösungen, die Plattformen eine klare und effiziente Implementierung ermöglichen. Beispiele sind (1) Suchtmechaniken (bspw. Lootboxen) – keine harmonisierte Regulierung auf EU-Ebene; möglich: verbindliches Verbot für U16 oder verpflichtende Transparenz bei Gewinnwahrscheinlichkeiten; (2) Algorithmen-Verantwortung – kein explizites Verbot der Engagement-Maximierung bei nachweisbaren Risiken; der DSA sollte hier präzisiert werden; (3) App-Stores – fragmentierte nationale Standards; Empfehlung: EU-weite Regulierung für OS/App-Store-Anbieter mit einheitlichen Altersstufensystemen und technischen Schnittstellen; Die Bereitstellung EU-einheitlicher technischer Lösungen (z.B. standardisierte

Altersverifikation „EU Age Verification“, interoperable Jugendschutz-APIs) würde Plattformen die rechtskonforme Umsetzung erheblich erleichtern und Compliance-Kosten senken.

II.5. Verschlüsselung vs. Überwachung

Verschlüsselung ist wertvoll und notwendig für Privatsphäre, aber das Spannungsfeld zu CSAM-Bekämpfung ist real. Unsere Empfehlung: End-to-End-Verschlüsselung beibehalten, CSAM-Bekämpfung aber durch andere Mittel (Nutzer-Reports, Behavioral Signals, externe Datenquellen wie NCMEC-Datenbank, Strafverfolgung). Client-Side Scanning (CSS) ist technisch anfällig und datenschutz-bedenklich - falls unvermeidbar, nur unter strikten Bedingungen mit Transparenz, unabhängiger Prüfung und Limitierung auf CSAM.

II.6. Betriebssysteme und App-Stores

iOS, Android und Windows haben unterschiedliche Jugendschutz-Standards. Empfehlung: OS sollten sichere Defaults für Kinder-Konten bieten (Zeit-Limits, Content-Filter, Kontakt-Limits zentral konfigurierbar). App-Stores brauchen einheitliche Altersstufensysteme (EU-weit PEGI-ähnlich, harmonisiert). Default-Kauf-Beschränkungen und optionale Altersverifizierung vor Download sind sinnvoll. Regulatorisch: DSA-Ergänzung für OS/App-Store-Anbieter, JuSchG-Konkretisierung, harmonisierte Altersstufensysteme.

II.7. Wirtschaftliche Implikationen

Ein umfassender Jugendmedienschutz verursacht Kosten für Plattformen (KI-Moderation, Algorithmen-Redesign, Audits) und Personal. Wenn Engagement-Maximierung begrenzt wird, können Ad-Einkünfte sinken; Beschränkung von Microtransactions mindert weitere Einnahmen. Allerdings können Plattformen, die hohen Standards erfüllen, sich als „sicher“ vermarkten und Wettbewerbsvorteil bei Eltern/Pädagogen gewinnen. Letztlich werden die (sozialen) Kosten, die durch mangelnden Kinder- und Jugendschutz entstehen, von den Plattformen an unsere Gesellschaften externalisiert. Vor diesem Hintergrund ist eine Regulierung der Plattformen zur Internalisierung dieser Kosten bzw. der grundsätzlichen Vermeidung der Probleme sehr sinnvoll.

Kapitel III: Altersgrenzen, Altersverifikation und Schutzräume

Verbindliche Altersgrenzen für bestimmte digitale Angebote sind erforderlich, müssen aber evidenzbasiert, durchsetzbar und differenziert sein. Eine sichere, datenschutzfreundliche Altersverifikation ist der Schlüssel – hier zeigt sich ein Paradigmenwechsel: Das EU-Projekt Age Verification App unter Führung von T-Systems und Scytáles setzt neue Standards durch echte Verifikation statt zum Beispiel Estimation, mit der Systeme umgangen werden können. Parallel sind speziell gestaltete digitale Schutzräume für Kinder und Jugendliche sinnvoll, ersetzen aber nicht die Regulierung großer Plattformen.

III.1. Verbindliche Altersgrenzen

Verbindliche Altersgrenzen sind erforderlich und sinnvoll, um Kinder und Jugendliche wirksam vor entwicklungsgefährdenden Inhalten und Interaktionsrisiken zu schützen. Solche Grenzen schaffen rechtliche Klarheit für Anbieter und bieten eine einheitliche Orientierung für Eltern und pädagogische Fachkräfte.

Kriterien für die Festlegung von Altersgrenzen:

1. Risikobewertung: Die Art und Schwere spezifischer Gefährdungen (z.B. Kontakttrisiken durch Cybergrooming, Exposition gegenüber suchtfördernden Mechaniken, Cybermobbing) muss systematisch analysiert werden.
2. Entwicklungspsychologische Evidenz: Altersgrenzen sollten sich an wissenschaftlich fundierten Erkenntnissen über kognitive, emotionale und soziale Entwicklungsstufen orientieren – etwa zur Impulskontrolle, kritischen Medienkompetenz und Vulnerabilität gegenüber Manipulation.
3. Internationale Best Practices: Bewährte Standards (z.B. COPPA in den USA mit Mindestalter 13, DSGVO-Vorgaben, britischer Online Safety Act) sollten berücksichtigt und auf europäische Verhältnisse adaptiert werden.
4. Evidenzbasierte Forschung: Unabhängige wissenschaftliche Studien zu Nutzungseffekten, Risikoprävalenzen und Wirksamkeit von Schutzmaßnahmen müssen die Grundlage bilden – nicht kommerzielle Interessen oder politische Opportunität.

III.2. Altersverifikation: Privacy-by-Design als neuer Standard

Die EU hat einen Paradigmenwechsel eingeleitet. Die von der Europäischen Kommission entwickelte EU Age Verification Solution mit Pilot ab Juli 2025 setzt neue Standards. Die Lösung wird von T-Systems und dem schwedischen Partner Scytáles AB entwickelt und bereits in EU Pilot-Ländern getestet.

Die Innovation: Diese Lösung nutzt echte Verifikation statt Estimation. Der Nutzer lädt die App herunter, bestätigt sein Alter (z.B. über eID oder Ausweisdaten), und die App transmittiert nur ein einfaches "≥18 JA/NEIN" – ohne dass persönliche Daten offenbaren werden. Dies ist der „Goldstandard“ für digitale Altersverifikation.

Warum diese Lösung sinnvoll ist:

- Privacy-by-Design: Nur Altersnachweis, keine Datensammlung
- Zero-Knowledge-Proofs: Systeme können Alter bestätigen, ohne persönliche Infos zu erfassen
- Keine wirtschaftlichen Anreize für Datenmissbrauch: Im Gegensatz zu Estimation-basierten Systemen (Facial Recognition, Behavioral Profiling), die oft von Plattformen mit Dateninteressen entwickelt werden

III.3. Formen der Altersabsicherung (Age-Assurance)

Echte Verifikation als einzig tragfähiger Ansatz: Aus datenschutz- und diskriminierungsrechtlicher Sicht kann nur echte Altersverifikation (Nachweis des tatsächlichen Alters via eID, Ausweisdaten oder andere vertrauenswürdige Identitätsnachweise) eine rechtssichere und zuverlässige Grundlage für Altersgrenzen bilden. Estimation-basierte Verfahren sind nicht empfehlenswert:

- Schätzung via Verhaltens-Signale oder Gerätedaten erfordert umfangreiches Tracking von Nutzungsmustern, Sprache und Device-Informationen – dies widerspricht fundamentalen Datenschutzprinzipien und schafft wirtschaftliche Anreize für Plattformen, Daten zu missbrauchen.
- Facial Recognition/biometrische Schätzung weist systematische Diskriminierungspotenziale auf (insbesondere bei nicht-westlichen Ethnien, Kindern mit atypischen Gesichtszügen) und erzeugt hochsensible biometrische Daten ohne ausreichende Rechtfertigung.
- Beide Ansätze haben hohe Fehlerquoten und sind technisch leicht umgehbar.

Token-/Wallet-basierte Verifikation als datenschutzkonformer Standard: Die von T-Systems und Scytáles für die Europäische Kommission entwickelte EU Age Verification App zeigt, wie echte Verifikation privacy-by-design funktionieren kann: Der Nutzer verifiziert sein Alter einmalig über vertrauenswürdige Quellen (eID, Ausweisdokument), erhält einen digitalen Alters-Token im eigenen Wallet/Telefon und transmittiert bei Bedarf nur die minimal notwendige Information („≥18 JA/NEIN“) – ohne Offenlegung persönlicher Daten an Dritte. Diese Architektur mit Zero-Knowledge-Proofs ist europaweit interoperabel, EUDI-Wallet-kompatibel und erfüllt höchste Datenschutzstandards.

Vermeidung von Risiken: Minimale Datenerfassung (nur Altersnachweis), dezentrale Speicherung beim Nutzer, keine Profilbildung durch Plattformen, regelmäßige Sicherheitsaudits und klare rechtliche Zweckbindung gewährleisten Schutz vor Over-Collection und Missbrauch

III.4. Digitale Schutzräume für Kinder und Jugendliche

Speziell gestaltete Räume sind wertvoll, ersetzen aber nicht die Regulierung großer Plattformen. Walled Gardens (wie YouTube Kids, fragFINN) bieten vollständige Kontrolle, sind aber inhaltlich begrenzt. Altersgerechte Algorithmen innerhalb großer ermöglichen Teilhabe am Mainstream.

Technisch realisierbar sind: Content-Filter (Whitelist vs. Blacklist), Kontaktschutz (nur Peers bestimmten Alters, keine Erwachsenen), Funktions-Limits (kein Live-Streaming für Jüngste), Zeit-Management (automatische Limits mit Pause-Reminders). Rechtlich/organisatorisch: Zertifizierung für Standards-erfüllende Plattformen, EU-Förderung für kleine Anbieter, klare Regulierung von „Kinderplattformen“.

Kapitel IV: Chancen, Teilhabe und spezielle Problemfelder

IV.1. Chancen durch technischen Jugendmedienschutz

Technischer Jugendmedienschutz „by design“ eröffnet zentrale Teilhabechancen: Sichere Suchmaschinen und kuratierte Bildungsinhalte fördern Information und Lernen, digitale Partizipations-Plattformen stärken demokratische Beteiligung, kreative Räume ohne suchtfördernde Mechaniken ermöglichen selbstbestimmte Freizeitgestaltung. Zudem können KI-gestützte Ressourcen zur Früherkennung psychischer Krisen und gesundheitsfördernde Apps (Bewegung, Achtsamkeit) präventiv wirken.

IV.2. Begrenzung übermäßigen Medienkonsums

Plattformen sollten technische Schutzmaßnahmen integrieren: automatische Nutzungspausen nach 90 Minuten, altersgestaffelte Tageslimits, Downtime-Modi und sanfte Nudges mit Aktivitätsalternativen. Eltern benötigen funktionierende Parental Controls (Zeit-, App-, Kontaktlimits) und Family-Sharing-Optionen. Ergänzend sind gesellschaftliche Maßnahmen erforderlich: Digitale-Detox-Programme in Schulen, Aufklärung über Übernutzungsrisiken sowie niedrigschwellige Offline-Alternativen (Sport, Kultur, Naturerfahrung).

IV.3. Sharenting und KidFluencing: Missbrauchsprävention

Das Teilen von Kinderfotos durch Eltern (Sharenting) ist rechtlich zulässig, birgt jedoch erhebliche praktische Risiken – von dauerhafter digitaler Identitätsbildung ohne Zustimmung der Kinder bis hin zu missbräuchlicher Nutzung geteilter Bilder in CSAM-Kontexten.

Technische Maßnahmen: Plattformen könnten automatische Erkennungssysteme für missbräuchlich verwendete Kinderbilder implementieren und diese proaktiv entfernen oder highlighten. Warnhinweise beim Upload von Kinderbildern („Denken Sie an die langfristigen Folgen für Ihr Kind“) sind ein sinnvolles Mittel.

Regulatorische Maßnahmen: Für kommerzielle Kinderauftritte (KidFluencer, Family-Vlogger) könnten – analog zu Regelungen für Kinder-Schauspieler – behördliche Genehmigungsverfahren, bspw. mit verpflichtenden Treuhandkonten für Einnahmen (gesperrt bis zum 18. Geburtstag) angedacht werden.

Die Autoren



Dirk Backofen ist Tribe Lead Digital Identities bei der T-Systems International GmbH und verantwortlich für die Geschäftseinheit digitale Identitätstechnologien (EUDI-Wallet, eID, Smart eID). Er koordiniert alle Aktivitäten der Telekom/T-Systems im Projekt „Ökosystem digitaler Identitäten in Deutschland“ und leitet die Entwicklung EUDI-kompatibler Wallet-Systeme für die EU Large Scale Piloten LSP I und LSP II. Im Kontext des Jugendmedienschutzes verantwortet er die Entwicklung der EU Age Verification App, die im Auftrag der Europäischen Kommission als datenschutzfreundliche, interoperable Lösung zur Umsetzung der DSA-Minderjährigenschutzanforderungen konzipiert wird. Dirk Backofen vertritt zudem die Deutsche Telekom/T-Systems als Vorstandsmitglied im Gesellschafterrat und Aufsichtsrat von Verimi und hat das Geschäftsmodell „Wallet as a Service“ entwickelt.



Fabian Horbach ist Senior Manager für digitale Administration, IT-Strategie und Transformationsmanagement mit über 10 Jahren Erfahrung in der Beratung des öffentlichen Sektors. Er unterstützt Bundes- und Landesbehörden sowie öffentliche Unternehmen bei der digitalen Transformation, KI-Governance, IT-Architektur und Compliance – darunter die Implementierung von Governance-Rahmenbedingungen im Einklang mit dem EU-KI-Gesetz. Als Manager im Projekt EU Age Verification bringt er seine Expertise in regulatorischer Umsetzung,

Interoperabilität und skalierbaren Public-Sector-Lösungen direkt in die Entwicklung datenschutzkonformer Altersverifikationssysteme ein.