

Unabhängige Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt“:

Hearing 2 – Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste

Berlin, 6. Februar 2026

Stellungnahme der FSM

Die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM e.V.) ist eine von der Kommission für Jugendmedienschutz (KJM) anerkannte Selbstkontrollereinrichtung für den Bereich Telemedien. Sie beaufsichtigt und berät eine Vielzahl von Unternehmen aus der Telekommunikations- und Online-Branche. Der Verein setzt sich seit 1997 dafür ein, dass Kinder und Jugendliche mit einem sicheren und besseren Internet aufwachsen können – insbesondere über die Bekämpfung illegaler, jugendgefährdender und entwicklungsbeeinträchtigender Inhalte in Online-Medien. Dazu betreibt die FSM eine Beschwerdestelle, an die sich alle wenden können, um Online-Inhalte zu melden, und ist Gründungsmitglied im internationalen Verbund der Beschwerdestellen INHOPE. Die FSM-Beschwerdestelle wird unter dem Dach von Saferinternet.de von der Europäischen Union kofinanziert. Darüber hinaus gehören die umfangreiche Aufklärungsarbeit und die Medienkompetenzförderung von Kindern, Jugendlichen und Erwachsenen zu den Aufgaben der FSM. Die FSM engagiert sich unter anderem in der Gesellschaft für Medienpädagogik und Kommunikationskultur (GMK), im Expert*innenkreis „Kinderrechte in der digitalen Welt“ des Deutschen Kinderhilfswerks (DKHW) sowie im Global Online Safety Regulators Network (GOSRN).

Im Folgenden nehmen wir zu den Fragen Stellung, soweit sie unseren Tätigkeitsbereich betreffen.

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?

Während Maßnahmen zum Schutz von Kindern und Jugendlichen vor schädlichen Medieninhalten lange Zeit von vielen auf **Mechanismen zur Zugangsverhinderung** sowie Verbreitungs- und Publizierungsbeschränkungen verengt wurden, fußt ein zeitgemäßer und wirksamer Jugendmedienschutz ganz selbstverständlich auf einer Kombination von solchen (meist technischen) Schutzvorkehrungen und weiteren, mindestens ebenso wichtigen Bausteinen.

Dass die **Befähigung zu einer aufgeklärten, sicheren und selbstbestimmten Mediennutzung** essenziell ist, liegt auf der Hand. Die schnelllebige Veränderung von Angeboten, Nutzungsweisen und sich daraus ergebenden veränderlichen Risikophänomenen ergibt dabei automatisch die Notwendigkeit, entsprechende Maßnahmen zur Medienkompetenzförderung nachhaltig anzubieten und aktuell zu halten.

Zudem muss die **Einbeziehung der Anbieter** von Inhalten und der Betreiber von Online-Plattformen von allen Seiten ernst genommen werden. Sie sind am ehesten in der Lage – und deshalb gesetzlich auch verpflichtet –, Risiken, die sich aus ihren Angeboten ergeben, zu bewerten und präventiv Gegenmaßnahmen zu ergreifen. Dienstespezifische und schnelle Reaktionen auf neue Herausforderungen sind in diesem Zusammenhang essenziell. Die Anbindung an staatlich anerkannte Einrichtungen der Freiwilligen Selbstkontrolle wie die FSM ermöglicht dabei eine enge Verzahnung mit wichtigen Stimmen aus Wissenschaft und Zivilgesellschaft sowie die bestmögliche Berücksichtigung eventueller nationaler Besonderheiten.

Schließlich spielt auch das elterliche Erziehungsprivileg eine entscheidende Rolle für einen gelingenden Jugendmedienschutz. Es bedeutet zugleich **Freiheit und Verpflichtung für Eltern**, erzieherische und Schutzmaßnahmen in Bezug auf Medien verantwortungsbewusst, aber auch flexibel und individuell einzusetzen – so, wie sie es für ihre eigene Familie für richtig halten. Staatliche Maßnahmen bieten dabei einen orientierenden Rahmen und wirken als Sicherheitsnetz, wenn Eltern ihrer Aufgabe nicht ausreichend wirksam nachkommen. Aufgeklärte Eltern, die passgenaue Schutzmaßnahmen – im Idealfall im Dialog mit ihren Kindern – einsetzen, sind daher ein entscheidender Eckpfeiler im System des Jugendmedienschutzes.

Die **Gewichtung dieser vier Säulen** (technische Maßnahmen zum Zugangsschutz, Befähigung der Nutzerinnen und Nutzer, Vorsorge- und Risikominderungsmaßnahmen der Anbieter, Ausstattung der Eltern mit Wissen und Werkzeugen) kann nicht pauschal für alle Angebote oder Angebotsgattungen festgelegt werden, sondern muss sich stets an einer individuellen Risikoanalyse orientieren.¹ Eine bestimmte Kombination der angesprochenen Bausteine mag für den einen Dienst perfekt geeignet sein, um den erforderlichen Jugendmedienschutz unter Berücksichtigung des kinderrechtlichen Dreiecks aus Schutz, Befähigung und Teilhabe sicherzustellen. Bei einem anderen Dienst mag dasselbe Set an Maßnahmen nicht ausreichend wirksam sein – oder aber zu restriktiv und damit gleichermaßen ungeeignet.

¹ Vgl. 5C-Typologie der Online-Risiken für Kinder, Anhang zu den Leitlinien für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065 ([C/2025/5519](#)).

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:

Für die Beantwortung dieses Fragenkomplexes kommt es zunächst entscheidend auf dessen Zielrichtung an.

Wenn in Überschrift und Frage allgemein von **digitalen Diensten** die Rede ist und damit alle Dienste i.S.d. § 1 Abs. 4 Nr. 1 DDG gemeint sind, müsste eine fachlich angemessene Beantwortung ausgesprochen breit ausfallen. Dies ist – auch angesichts des sehr schmalen Zeitkorridors, der für die Beantwortung eingeräumt ist – herausfordernd.

Für den großen Bereich der **linearen digitalen Mediendienste** sowie der **digitalen Mediendienste auf Abruf** (vor allem Video on Demand) sei an dieser Stelle lediglich darauf verwiesen, dass durch die Regelungen vor allem im JMStV, aber auch im JuSchG, die u.a. die AVMD-Richtlinie umsetzen, bereits ein bewährtes Schutzkonzept regulatorisch ausgestaltet und in der Praxis etabliert ist. So gibt es – soweit erkennbar – von allen relevanten Akteuren akzeptierte Vorgaben, wie Inhalte hinsichtlich ihrer Jugendschutzrelevanz zu bewerten, zu kennzeichnen sowie gegen die Wahrnehmung durch (zu) junge Menschen abzusichern sind.

Ergänzend kann in diesem Zusammenhang auch auf die zentrale Rolle der Jugendschutzbeauftragten hingewiesen werden, die als Ansprechpersonen für Nutzerinnen und Nutzer fungieren und dafür Sorge tragen, dass Inhalte mit entsprechenden Altersfreigaben versehen werden, auf die sich Eltern und Familien verlassen können. Ein Pendant zu den in § 7 JMStV geregelten Jugendschutzbeauftragten findet sich nun sogar auch in Nr. 84 (b) der Leitlinien zu Art. 28 Digital Services Act (DSA). Auch wenn keine formelle Benennungspflicht besteht, erwarten die Leitlinien faktisch, dass bei Betreibern von Online-Plattformen klare interne Zuständigkeiten und ausreichende fachliche Expertise im Bereich Kinder- und Jugendschutz vorhanden sind.

Nicht zuletzt der Bereich der technischen Schutzmaßnahmen ist durch die Einbeziehung der Einrichtungen der Freiwilligen Selbstkontrolle wie der FSM praxistauglich, innovationsfördernd und risikoangemessen ausgestaltet und bedarf derzeit keiner weiteren Aufmerksamkeit durch den Gesetzgeber.

Auch leisten Medienhäuser und andere Inhaltenanbieter mit ihren kuratierten und jugendschutzkonform gestalteten Angeboten bereits einen wichtigen Beitrag zum Jugendmedienschutz in Deutschland.

Angemerkt sei an dieser Stelle gleichwohl, dass ein *Level Playing Field* unter Einbeziehung fast aller deutschen und der wichtigsten internationalen Anbieter angesichts des Herkunftslandprinzips primär deshalb erreicht wurde, weil die FSM im Rahmen freiwilliger Selbstverpflichtungen ein bestmögliches Heranrücken der Anbieter ohne Sitz in Deutschland an die hiesige Regulierung realisiert hat.

Lediglich der Vollständigkeit halber sei hier auf die Möglichkeit zur **Nutzung von Jugendschutzprogrammen** verwiesen. Nutzerautonome Filter (§ 11 Abs. 1 JMStV) können auf einzelnen Geräten oder für Netzwerke installiert werden und Eltern dabei helfen, ihre Kinder vor ungeeigneten Online-Inhalten zu schützen, indem sie diese altersdifferenziert blockieren bzw. filtern (z.B. JusProg²). Jugendschutzprogramme für geschlossene Systeme (§ 11 Abs. 2 JMStV) werden z.B. bei Video-on-Demand-Streaming-Diensten eingesetzt. Sie ermöglichen Familien, die verfügbaren Inhalte basierend auf Altersstufen zu filtern und nur für die jeweils passende Altersgruppe freizugeben. Jugendschutzprogramme müssen zur Beurteilung ihrer Eignung einer anerkannten Einrichtung der Freiwilligen Selbstkontrolle wie der FSM vorgelegt werden.

Seit dem 1. Dezember 2025 treten neben diese Maßnahmen zudem **Jugendschutzvorrichtungen auf Ebene der Betriebssysteme** (§ 12 JMStV). Zur praktischen Wirksamkeit dieser neuen regulatorischen Maßnahme liegen derzeit noch keine Erkenntnisse vor. Diese müssen jedoch abgewartet werden, bevor in dieses – nicht nur aus Elternsicht ohnehin komplexe – Konstrukt des technischen Jugendmedienschutzes erneut eingegriffen wird.

Aus diesem Grund konzentrieren sich die folgenden Ausführungen vor allem auf **Online-Plattformen i.S.d. DSA**, soweit dies nicht ausdrücklich anders angegeben ist.

Generell ist festzuhalten, dass **Anbieter von Online-Plattformen** über die Gestaltung ihrer Dienste einen **wichtigen Beitrag** leisten. Zudem müssen sie über sichere Nutzungsweisen und die Vermeidung von Risiken im Verhalten von Nutzerinnen und Nutzern transparent informieren. Als plattformseitige Maßnahmen kommen unter anderem in Betracht:

- das Anbieten besonderer Schutzmaßnahmen und Einstellmöglichkeiten für Minderjährige bzw. angepasster Nutzungsmöglichkeiten (z.B. über Teen-Profile)
- das Betreiben von Melde- und Moderationssystemen sowie die Beschäftigung von geschultem Personal, wobei angesichts der großen Anzahl zu bewertender Inhalte ein angemessener und sorgfältig überwachter Einsatz automatisierter Systeme unumgänglich ist

² <https://www.jugendschutzprogramm.de/>

- bei der Verwendung algorithmischer Empfehlungen nutzerseitige Anpassungen ermöglichen, die altersgerecht sind; der vollständige Ausschluss solcher Systeme bei minderjährigen Nutzerinnen und Nutzern würde dazu führen, dass es nicht möglich wäre, ausdrücklich altersgerechte bzw. für eine jugendliche Zielgruppe hilfreiche und relevante Inhalte bevorzugt auszuspielen
- das Anbieten von Melde- und Blockiermöglichkeiten gegen unangemessenes Verhalten Dritter bzw. zur Verhinderung unerwünschten Kontakts
- die Aufklärung über plattformspezifische Risiken auf eine Weise, die für junge Nutzerinnen und Nutzer nachvollziehbar ist³
- die Einbeziehung von Eltern und anderen Erziehenden, z.B. in den Registrierungsprozess, die Vorauswahl altersgerechter Einstellungen und Möglichkeiten einer begleitenden Nutzung („family pairing“)
- Möglichkeiten zur Regulierung von Bildschirmzeiten und Nutzungsdauer, Pausen-Funktionen, Digital Wellbeing

Diese sowie weitere Maßnahmen kommen zur Minimierung der in diesem Fragenkomplex aufgeworfenen Risikobereiche jeweils einzeln oder in Kombination miteinander in Betracht. Auf die **Leitlinien zu Art. 28 Abs. 4 DSA** (s.o. Fn. 1) ist an dieser Stelle ergänzend abermals zu verweisen. Sie enthalten zahlreiche instruktive, z.T. sehr spezielle Vorschläge für Maßnahmen zur Risikominderung insbesondere bei Online-Plattformen.

Grundsätzlich gilt aber: Wenn Jugendmedienschutz – zutreffend – als **Gesamtkonzept aus Schutz, Befähigung und Teilhabe** verstanden wird, so ist neben diesen Einzelmaßnahmen für individuelle Risikophänomene auch stets die große Bedeutung präventiven Schutzes durch Aufklärung und Medienbildung zu betonen, denn **es gibt keinen wirksamen Jugendmedienschutz ohne Medienkompetenz**. Medienbildung muss deshalb strukturell und nachhaltig gefördert werden. Kinder und Jugendliche müssen frühestmöglich befähigt werden, Risiken zu erkennen und souverän mit digitalen Medien umzugehen. Das beinhaltet eine altersgerechte Aufklärung über Risiken⁴, Handlungsoptionen im Falle negativer Erlebnisse, sichere und selbstbestimmte Nutzung von Angeboten und Diensten, kreative Medienproduktion und vieles mehr.

³ Auf die Ergebnisse des Kooperationsprojekts von FSM und JFF zu jugendgerechten AGB i.S.d. Art. 14 Abs. 3 DSA sei an dieser Stelle ergänzend hingewiesen: <https://www.jff.de/schwerpunkte/kinder-und-jugendmedienschutz/details/jugendgerechte-agb>

⁴ Vgl. oben Fn. 1.

Insbesondere **Eltern** müssen in ihrer Verantwortung bei der Medienerziehung in der Familie unterstützt werden. Aber auch Lehr- und pädagogische Fachkräfte benötigen Informationen, Ressourcen und praktische Tipps, um Kinder und Jugendliche im Umgang mit Online-Medien zu begleiten.

Medienbildung als grundlegender Bildungsauftrag braucht strukturelle Verankerung, langfristige Finanzierung sowie nachhaltige Förderung. Der Staat und seine Einrichtungen können in diesem Zusammenhang nicht nur durch finanzielle Unterstützung einen wertvollen Beitrag leisten, sondern sich auch an wirksamen Maßnahmen beteiligen, die die Sichtbarkeit vorhandener Angebote weiter erhöhen und damit ihre Auffindbarkeit für die angesprochenen Zielgruppen erleichtern.

Gleichzeitig können und sollen Plattformanbieter hier einen Beitrag leisten, indem sie über die Gestaltung ihrer Dienste, sichere Nutzungsweisen und die Vermeidung von Risiken im Verhalten von Nutzerinnen und Nutzern transparent informieren.

Die FSM engagiert sich seit vielen Jahren für die Medienkompetenzförderung. Wir unterstützen Eltern, Lehrkräfte und Heranwachsende mit vielfältigen Medienbildungsangeboten dabei, digitale Medien sicher und selbstbewusst zu nutzen, zum Beispiel:

- **Elternguide.online**⁵ unterstützt Eltern bei der Medienerziehung in der Familie und hilft ihnen dabei, ihre Kinder bei der Nutzung von Apps, Spielen, Websites und sozialen Netzwerken zu begleiten.
- **Medien in die Schule**⁶ bietet zahlreiche Unterrichtsmaterialien und mediendidaktische Werkzeuge, um die Chancen digitaler Medien, Online-Risiken und Handlungsmöglichkeiten für junge Menschen im Unterricht zu behandeln.
- Mit dem bundesweiten Fortbildungsprogramm **weitklick**⁷ unterstützt die FSM Lehr- und pädagogische Fachkräfte dabei, Jugendlichen einen verantwortungsbewussten und kritischen Umgang mit Desinformation, Hate Speech und KI zu vermitteln.

Viele Medienbildungsprojekte stellen bereits Informations- und Aufklärungsangebote für die Zielgruppen Kinder, Jugendliche, Eltern und Erziehende sowie Lehr- und pädagogische Fachkräfte zur Verfügung. Damit sie diese zielgerichtet und langfristig unterstützen können, benötigen Angebote der Medienbildung jedoch eine **strukturelle Verankerung, langfristige Finanzierung sowie nachhaltige Förderung**.

⁵ <https://www.elternguide.online/>

⁶ <https://www.medien-in-die-schule.de/>

⁷ <https://www.weitklick.de/>

a. digitale sexualisierte Gewalt (z.B. Cybergrooming, Sextortion, Missbrauchsdarstellungen),

Die angesprochenen Beispiele für sexualisierte Gewalt sind differenziert zu betrachten, auch wenn sie in gewisser Weise zusammenhängen.

Wirksamen Schutz bieten vor allem Kontakt- und Sichtbarkeitsbeschränkungen, altersangemessene Voreinstellungen, niedrigschwellige Meldewege und eine qualifizierte Reaktion auf entsprechende Hinweise von Nutzerinnen und Nutzern.

Um die Verbreitung von Darstellungen des sexuellen Missbrauchs von Minderjährigen (Child sexual abuse material – CSAM) zu erschweren und zu begrenzen, sind plattformspezifische Meldemöglichkeiten, aber auch gut ausgestattete unabhängige Meldestellen wie die FSM-Beschwerdestelle⁸ essenziell. Gemeinsam mit unseren Partnern sind wir der wichtigste Hinweisgeber für das BKA⁹. Durch die internationale Kooperation im INHOPE-Netzwerk¹⁰ sorgen wir für schnellstmögliche Entfernung solcher Inhalte weltweit.

Betreiber von Online-Plattformen können die Verbreitung von CSAM durch die Nutzung von Hash-Datenbanken und einer zielgerichteten Weiterentwicklung ihrer eigenen Entdeckungstechnologie einschränken. Maßnahmen zur branchenweiten Kooperation können dazu weiter ausgebaut werden.

b. suchtbegünstigende/hochgradig bindende Gestaltungspraktiken (z.B. Mikrotransaktionen, Lootboxen/Zufallsmechaniken, Dark Patterns),

Besonders relevant sind Designentscheidungen wie Endlos-Scrolls, variable Belohnungssysteme oder aggressive Push-Mechaniken. Wirksam sind transparente Mechaniken, Abschwächungen besonders bindender Elemente sowie nutzungsbezogene Hinweise und Pausen-Defaults.

Entsprechend umzusetzende Regelungen existieren bereits auf EU- und nationaler Ebene. So werden Dark Patterns im DSA reguliert: Art. 25 DSA verbietet es Online-Plattformen, ihre Benutzeroberflächen so zu gestalten, dass Nutzerinnen und Nutzer getäuscht, manipuliert oder in ihrer freien Entscheidung beeinträchtigt werden.

National regt der Gesetzgeber in § 14 Abs. 2a JuSchG und in § 5c Abs. 3 S. 2 JMStV den Einsatz von Deskriptoren im Bereich der Spielplattformen an, um Erziehungsberechtigte

⁸ <https://www.fsm.de/fsm/beschwerdestelle/>

⁹ Vgl. sog. Löschbericht der Bundesregierung für das Jahr 2024, abrufbar unter https://www.bmjbv.de/SharedDocs/Downloads/DE/Fachpublikationen/Loeschbericht_2024.html

¹⁰ <https://inhope.org/>

und Eltern auf Interaktionsrisiken, wie sie von Lootboxen ausgehen, hinzuweisen. Viele Anbieter nutzen bereits diese (freiwillige) Möglichkeit und setzen entsprechende Deskriptoren ein. Durch eine weitere Vereinheitlichung von Deskriptoren könnte ihr Einsatz noch attraktiver gemacht werden.

c. Hate Speech, Desinformation sowie verschwörungsideologische und extremistische Inhalte,

Sowohl bei staatlichem Handeln im Zusammenhang mit Desinformation, manipulativen Inhalten und Falschinformation als auch bei Maßnahmen von Online-Plattformen ist strikt zu differenzieren zwischen Eingriffen zur Sanktionierung rechtswidriger Inhalte einerseits und der Unterstützung von Aufklärungsmaßnahmen zur Befähigung im Umgang mit Desinformation, die nicht (klar) rechtswidrig ist, andererseits. Gerade im Bereich Aufklärung haben sich in den vergangenen Jahren starke zivilgesellschaftliche Akteure etabliert, durch deren finanzielle Förderung Bund und Länder einen wichtigen Beitrag leisten, ohne inhaltlich Einfluss zu nehmen.

Die Verbreitung von Desinformation und Verschwörungsmythen findet insbesondere über die sozialen Medien sowie Messenger-Dienste statt. Daher tragen auch die Betreiber von Online-Plattformen eine gewisse Verantwortung, sowohl aktiv Desinformation zu verhindern als auch sicherzustellen, dass sie nicht unbeabsichtigt zur Verbreitung von falschen Informationen beitragen. Gleichzeitig müssen sie jedoch die Balance zwischen der Bekämpfung von Desinformation und der Wahrung der Meinungsfreiheit gewährleisten. Die Zusammenarbeit mit externen Organisationen, die Förderung von Medienkompetenz und die Transparenz der angewandten Praktiken sind wichtige Aspekte dieser Verantwortung.

Im Kampf gegen Desinformation spielen auch Medienbildung und -erziehung eine wichtige Rolle für die Prävention und Intervention. Hier kann Kindern und Jugendlichen grundlegendes Wissen über die Merkmale, Motive und Verbreitungswege von Desinformationen sowie deren Formen und Wirkungsweisen vermittelt werden. Dies unterstützt sie dabei, desinformierende, manipulative Inhalte zu erkennen und mit ihnen umzugehen – Grundlagen für sichere Online-Erfahrungen, den Umgang mit Risiken sowie eine mündige Meinungsbildung.

d. Belästigung/Cybermobbing und weitere Interaktionsrisiken (z. B. Doxxing, Stalking, koordinierte Angriffe),

Effektiv sind Funktionen zum Blockieren und Filtern, um unerwünschte Kontaktaufnahmen zu unterbinden.

Viele Online-Plattformen bieten besondere Voreinstellungen für jüngere Nutzerinnen und Nutzer oder allgemeine Funktionseinschränkungen unterhalb bestimmter Altersstufen. Dazu gehört zum Beispiel, dass Dienste „unsichtbar“ genutzt werden können oder dass Standortdaten entweder gar nicht oder lediglich in einem sehr eng begrenzten Rahmen geteilt werden können.

Schnelle und verlässliche Abhilfeprozesse nach der Meldung unzulässigen Verhaltens oder problematischer Inhalte sind ebenso wichtig.

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

Wichtig sind frühe Signale an Nutzerinnen und Nutzer, sensible Empfehlungslogiken und Verweise auf Hilfsangebote. Pauschale Sperren sind regelmäßig weniger wirksam als kontextsensible Interventionen.

Hilfreich können neben Warnhinweisen bei der Suche nach entsprechenden Inhalten in sozialen Medien auch Verlinkungen zu spezialisierten Helplines wie der Nummer gegen Kummer¹¹ sein. Im Rahmen der Vorsorgemaßnahmen wird auch in den DSA-Leitlinien¹² ein Verweis auf externe und unabhängige Beratungsangebote angeregt.

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

Datensparsame Defaults, klare Kennzeichnung von Werbung und Beschränkungen personalisierter Ansprache sind zentrale Schutzinstrumente.

Auf europäischer Ebene sind große Online-Plattformen über Art. 28 Abs. 2 DSA direkt verpflichtet, Minderjährige vor irreführender Werbung und personalisiertem Tracking zu schützen. Ergänzend empfehlen die DSA-Leitlinien, dass Konten Minderjähriger standardmäßig als privat konfiguriert werden, um unbefugte Dateneinsicht und Profilbildung zu verhindern. Weitere Maßnahmen aus den Leitlinien dienen der Schaffung sicherer Interaktionsräume: etwa die Möglichkeit, andere Nutzer zu blockieren oder stummzuschalten, das Verbot, Inhalte Minderjähriger herunterzuladen oder Screenshots erstellen zu können, sowie Einschränkungen für manipulative Designpraktiken. Diese Vorgaben können dazu beitragen, die unerwünschte

¹¹ <https://www.nummergegenkummer.de/>

¹² Vgl. oben Fn. 1.

Weiterverbreitung persönlicher Inhalte und die kommerzielle oder kriminelle Ausnutzung von Minderjährigen einzudämmen.

Die deutschen Jugendschutzbestimmungen im JuSchG und im JMStV schaffen dazu einen ergänzenden Rahmen, vor allem mit § 6 Abs. 2 JMStV (jugendschutzkonforme Gestaltung von Werbung) sowie § 5 Abs. 1 S. 2 JMStV (Entwicklungsbeeinträchtigung) – letzterer umso mehr, seitdem mit der Novellierung des JMStV nun auch sog. Interaktionsrisiken außerhalb der medieninhaltlichen Wirkung mit erfasst werden.

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

Fast alle sozialen Netzwerke geben an, Nutzerinnen und Nutzern unterhalb einer bestimmten Altersstufe angepasste Funktionen zur Verfügung zu stellen und spezielle Sicherheitsfunktionen voreingestellt anzubieten. Die **DSA-Leitlinien¹³ enthalten zudem einen umfangreichen Katalog** für solche Optionen und Features. Technische Lösungen können als flexible Schutzmaßnahme Online-Inhalte für verschiedene Altersgruppen filtern und so altersgerechte Zugänge sicherstellen. Sie müssen im besten Interesse von Kindern und Familien gestaltet und viel **besser sichtbar** gemacht werden. Dienstespezifische und risikoangemessene Schutzmaßnahmen, die durch Anbieter bzw. Betreiber angeboten und eingesetzt werden, können Nutzerinnen und Nutzer unabhängig von deren Medienkompetenz erreichen. Sie spielen deshalb eine ganz zentrale Rolle.

Statt neue Verbote zu verhängen, sollte der Fokus der Diskussion deshalb auf diesen Einstellungen und Funktionen liegen sowie darauf, wie sie eine **sicherere Nutzung durch Jugendliche ermöglichen** können. Die EU-Kommission hat die Bedeutung der DSA-Leitlinien wiederholt betont, und so ist zu erwarten, dass die neuen Regeln auch in der Praxis Auswirkungen darauf haben werden, dass es diese Features überhaupt gibt und dass sie auch tatsächlich wie angegeben funktionieren und wirksam sind.

Offen bleibt derzeit auch in den Leitlinien, welche dieser Einstellmöglichkeiten verpflichtend und welche optional sein sollten.

Die FSM steht als staatlich anerkannte Selbstkontrollereinrichtung bereit und kann **mit ihrem branchenweiten Ansatz** eine entscheidende Rolle dabei spielen, die Relevanz und Praxistauglichkeit der Features zu bewerten. Das System der Regulierten Selbstregulierung, in dem die FSM seit über 20 Jahren gesetzlich abgesichert agiert, hat sich für den Jugendmedienschutz in Deutschland bewährt. Es schafft Verbindlichkeit

¹³ Vgl. oben Fn. 1.

und entlastet staatliche Stellen. Dieses flexible Konzept **fördert Innovation** und **lässt Spielraum für individuelle Lösungen**. Auf diese Weise kann auch die Perspektive der Anbieter einbezogen und kritisch begleitet werden. Dass dieses System über den Kernbereich des gesetzlichen Jugendmedienschutzes hinaus wirksam und beispielgebend sein kann, zeigen die Erfahrungen der FSM als Einrichtung der Regulierten Selbstregierung für die Zwecke des NetzDG.¹⁴

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

Maßnahmen zum Schutz von insbesondere jungen Nutzerinnen und Nutzern müssen auf Grundlage einer fortlaufenden Risikoanalyse **bereits bei der Produktentwicklung und vor der Einführung neuer Features** mitgedacht werden, und zwar ausdrücklich unter Einbeziehung unabhängiger Expertise aus Jugendmedienschutz, Medienforschung und Medienpädagogik. Sie müssen organischer Bestandteil digitaler Dienste sein und dürfen nicht lediglich nachträglich hinzugefügt werden.

Frühzeitig sollte zudem die **Perspektive der jungen Menschen** selbst einbezogen werden: Nur so kann verlässlich antizipiert werden, auf welche Weise (neue) Angebote von ihnen genutzt werden und welche Risiken sich möglicherweise daraus ergeben. Daneben tritt die **Perspektive der Eltern**, die für das Gelingen von Jugendmedienschutz in der Familie zwingend erforderlich ist.

Zusätzlich muss die **Wirksamkeit** bereits getroffener Maßnahmen **kontinuierlich** anhand der verfügbaren Daten (bezüglich aktueller Risikolagen sowie der Mediennutzung und Schutzbedürfnisse junger Menschen) **analysiert** werden, um ggf. Anpassungen vornehmen zu können. Praktische Erkenntnisse aus dem gesamtgesellschaftlichen Dialog, beispielsweise bezogen auf Nutzungstrends oder Umgehungsmechanismen, können hier einfließen, um sicherzustellen, dass die implementierten Schutzmaßnahmen nicht nur vorhanden sind, sondern nachweislich und nachhaltig funktionieren.

¹⁴ <https://www.fsm.de/fsm/netzdg/>

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)?

Es bestehen bereits hinreichend konkrete rechtliche und praktische Regelungen zur Verantwortung von Plattformen gegenüber Minderjährigen. Diese ergeben sich primär aus Art. 28 Abs. 1 DSA und den im Sommer 2025 dazu erlassenen Leitlinien¹⁵, die diese Anforderungen sehr präzise ausbuchstabieren.

Der DSA verpflichtet Online-Plattformen, die für Minderjährige zugänglich sind, „geeignete und verhältnismäßige Maßnahmen“ zum Schutz von Kindern zu implementieren – und zwar ausdrücklich in den Bereichen Privatsphäre, Sicherheit und Schutz vor Risiken. Die EU-Kommission hat diese Pflichten durch die Leitlinien in folgenden Punkten konkretisiert:

- Schutz durch Default-Settings (z.B. private Profile für Minderjährige)
- Risiken und Risikoanalysen (5C-Modell)
- Altersabsicherung, bspw. Altersverifikation (robust, datensparsam, zuverlässig)
- Moderations- und Meldewege für Kinder
- Transparenzpflichten, Anpassen von Empfehlungssystemen

Die Leitlinien stellen, auch wenn man sie als nicht rechtsverbindlich einordnet, quasi den operationalen Standard dar, den Plattformen beachten müssen. Sie können als entscheidende Grundlage für regulatorische Maßnahmen und die allgemeine Aufsichtspraxis herangezogen werden.

Damit ist das **Schutzniveau durch den Gesetzgeber hinreichend konkret definiert**. Die Herausforderung liegt nun primär in Implementierung, Aufsicht und Durchsetzung. Da die Leitlinien erst Mitte 2025 veröffentlicht wurden, sollte den Anbietern nun entsprechend Zeit zugestanden werden, die Sinnhaftigkeit der getroffenen Maßnahmen zu evaluieren.

¹⁵ Vgl. oben Fn. 1.

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

Eine umfangreiche Überprüfbarkeit ist bereits im DSA und in den DSA-Leitlinien¹⁶ berücksichtigt worden: Art. 15 DSA regelt die Anbieterpflicht zu **jährlichen Transparenzberichten** hinsichtlich der Inholdemoderation. Art. 34 und 35 DSA regeln die Vornahme jährlicher Risikoanalysen und Maßnahmen zur Risikominderung nebst deren Dokumentation. Eine unabhängige aufsichtsrechtliche Kontrolle erfolgt durch die nationalen *Digital Services Coordinators* einerseits und die EU-Kommission für VLOPs und VLOSEs andererseits. Jene sind verpflichtet, jedes Jahr Berichte über ihre Risikobewertungen des laufenden Jahres, ihre Risikominderungsmaßnahmen sowie ihre Prüfberichte und Prüfdurchführungsberichte in geeigneten Fassungen zu veröffentlichen. Auch ist bspw. Forschenden laut DSA der Zugriff auf Daten der Plattformen zu gewähren, wenn die Forschung geeignet ist, systemische Risiken zu finden oder besser zu verstehen.

Mittelbar ergibt sich die Überprüfbarkeit auch aus der Tätigkeit der vertrauenswürdigen Hinweisgeber (**Trusted Flagger**) i.S.d. Art. 22 DSA, die ihrerseits den Kontakt mit den Plattformen umfangreich und auditierbar dokumentieren müssen und ebenfalls einer jährlichen Berichtspflicht unterliegen.

Nicht zuletzt kommt auf nationaler Ebene dem System der regulierten Selbstregulierung eine herausragende Bedeutung zu, wenn es um die (Eigen-)Verantwortung der Plattformen geht. Die Beaufsichtigung durch eine anerkannte Selbstkontrollereinrichtung wie die FSM ermöglicht die unmittelbare Reaktion der Unternehmen auf festgestellte Verstöße gegen jugendmedienschutzrechtliche Vorschriften – anders als staatliche Aufsichtsverfahren, die Monate oder gar Jahre dauern können. Zudem können auch Anbieter, die aufgrund des Herkunftslandprinzips nicht der deutschen Regulierung unterliegen, durch den Anschluss an eine Selbstkontrolle an nationale Jugendschutzstandards bestmöglich herangeführt werden.

3. 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?

Das **System der regulierten Selbstregulierung** sollte weiter gestärkt werden, nicht zuletzt durch gesetzliche oder andere regulatorische Anreize für Unternehmen, sich einer Einrichtung der Freiwilligen Selbstkontrolle wie der FSM anzuschließen. Damit

¹⁶ Vgl. oben Fn. 1.

können sich Effizienz- und Umsetzungsvorteile im Hinblick auf die in Art. 28 DSA und in den Leitlinien geforderten Vorgaben ergeben. Da in den Leitlinien ein risikobasierter Ansatz gewählt wurde (Stichwort 5C-Risiken), sind pauschale Lösungen ungeeignet. Die Selbstkontrollen hingegen sind strukturell ideal aufgestellt, um differenzierte, plattformspezifische Maßnahmen zu entwickeln und zu begleiten. Durch die Beratung und die „kurzen Dienstwege“ zwischen Anbietern und Selbstkontrolle kann Jugendmedienschutz umfassend und effizient gestaltet werden. Bei der Umsetzung sollte der dialogische Ansatz, der sich in der Vergangenheit bewährt hat, auch vonseiten der Aufsicht weiterverfolgt werden. Die rechtliche Beratung und Beaufsichtigung der Unternehmen, die sich anerkannten Selbstkontrollen wie der FSM angeschlossen haben, sollte aber weiterhin primär durch diese erfolgen.

Hinsichtlich der Umsetzung des Bereichs Altersabsicherung haben die anerkannten Selbstkontrollen im neuen JMStV den gesetzlichen Auftrag erhalten, Kriterien für Altersverifikationssysteme und technische Mittel gemeinsam mit der Kommission für Jugendmedienschutz (KJM) zu erarbeiten. Die DSA-Leitlinien stellen hohe Anforderungen an Robustheit, Verhältnismäßigkeit und Datenschutz von Altersverifikationssystemen – die gemeinsame Kriterienentwicklung von KJM und Selbstkontrollen gemäß JMStV ist ein zentraler Baustein für die nationale Umsetzung dieser Erfordernisse.

Die Prämisse, die Kriterien hinsichtlich der ständig fortschreitenden Entwicklung **technologieoffen** zu gestalten, sollte auch für andere Umsetzungsbereiche gelten – zu starre Kriterien und zu eng gefasste Vorgaben würden fortschrittliche Lösungen schlimmstenfalls verhindern. Auch Pauschallösungen für die Umsetzung von Maßnahmen verbieten sich. Vielmehr muss jede Maßnahme passgenau auf diejenigen Risiken abgestimmt sein, die dem jeweiligen Dienst laut Risikoanalyse immanent sind.

Nicht zuletzt müssen präventive Maßnahmen weiter ausgebaut werden. Auch zuverlässige Meldewege sind essenziell. Meldestellen wie die **FSM-Beschwerdestelle**, die mit anerkannten Netzwerken wie INHOPE kooperieren, müssen auch aus Deutschland **staatliche Förderung** erhalten, um ihre Existenz nachhaltig zu sichern.

Im Ergebnis sichert eine Umsetzung als Zusammenspiel von EU-Regulierung und regulierter Selbstregulierung auf nationaler Ebene einen effizienten, innovationsfreundlichen Schutz von Minderjährigen.

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

Deutschland verfügt insgesamt über ein sehr gut etabliertes Jugendmedienschutz-System mit verschiedensten Akteuren, die bereits seit Jahren erfolgreich zusammenarbeiten. Dieses System wird für Online-Plattformen durch die Vorgaben aus DSA und den dazugehörigen Leitlinien umfangreich ergänzt. Regelungslücken existieren daher weniger im materiellen Recht, sondern eher auf der Stufe der Harmonisierung von nationalen und EU-Vorschriften. Notwendig ist eine Verzahnung der EU-Regelungen mit JMStV und JuSchG, um widersprüchliche Vorgaben und Doppelstrukturen zu vermeiden. Ein Beispiel für widersprüchliche Rechtsansichten zwischen der EU und Deutschland ist die Altersverifikation per *Facial Age Estimation*, die aufgrund ihrer Zuverlässigkeit von KJM und der nach § 4 Abs. 4 S. 2 JMStV nunmehr dafür zuständigen FSM auch für Angebote mit hohem Risiko anerkannt wird, in den DSA-Leitlinien hingegen als nicht grundsätzlich tauglich für die strikte Altersverifikation angesehen wird.

Der Bedarf zum Schließen von Lücken liegt weniger in zusätzlichen Regeln, sondern in einer kohärenten Umsetzung der bestehenden Vorgaben und Ziele, insbesondere im Bereich des technischen Jugendmedienschutzes.

6. 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?

Auf EU-Ebene unterliegen große App-Stores als VLOPs dem DSA mit strengen Pflichten zu Risikobewertung, Risikominderung, Altersverifikation und kindgerechten Default-Einstellungen. Die DSA-Leitlinien zum Schutz Minderjähriger¹⁷ konkretisieren diese Anforderungen.

In Deutschland wurde durch den novellierten JMStV mit der sog. **Jugendschutzvorrichtung** eine technische Schutzmöglichkeit auf Betriebssystemebene eingeführt, und auch die Betreiber von App-Stores werden in die Pflicht genommen. Dabei bleibt weiterhin unklar, inwieweit die relevanten Betriebssystemanbieter überhaupt dem deutschen Jugendmedienschutzregime unterfallen und die neuen Vorgaben des JMStV auch umsetzen werden, da sie ihren Sitz nicht in Deutschland haben. Durch den Vorrang des DSA ist zusätzlich fraglich, ob die Regelungen überhaupt wirksam sind, sofern sie eine Entsprechung im DSA haben.

¹⁷ Vgl. oben Fn. 1.

Wie oben (I.1.) ausgeführt, liegen zur praktischen Wirksamkeit dieser neuen regulatorischen Maßnahme derzeit noch keine Erkenntnisse vor. Diese müssen zunächst abgewartet werden.

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

Umfassender Jugendmedienschutz ist stets mit Kosten verbunden – sei es für die Implementierung von technischen Schutzmechanismen, die Beschäftigung von Jugendschutzbeauftragten oder die Weiterentwicklung von KI-Systemen zur Erkennung jugendschutzrelevanter Inhalte.

Die FSM tritt seit langem dafür ein, dass **Jugendmedienschutz** von Anfang an mitgedacht werden muss, idealerweise **bereits in der Produktentwicklung**. So können hohe Folgekosten, die durch eine nachträgliche Anpassung entstehen würden, vermieden werden. Mitgliedsunternehmen der FSM setzen dies seit Jahren erfolgreich um und schaffen echten Mehrwert für ihr Publikum.

Internationale Unternehmen, die sich einer Einrichtung der Freiwilligen Selbstkontrolle wie der FSM angeschlossen haben, werden bestmöglich an deutsche Jugendschutzstandards herangeführt. Jedoch besteht das Risiko, durch zu strikte und international nicht anschlussfähige Vorgaben eben jene Unternehmen abzuschrecken.

Bei der Prüfung neuer gesetzlicher Vorgaben ist zudem zu berücksichtigen, dass diejenigen Diensteanbieter, die bereits die gesetzlichen Schutzanforderungen erfüllen, durch neue Regelungen, welche insbesondere diejenigen Dienste erfassen soll, die bislang nicht ausreichend jugendschutzkonform agieren, zusätzlich wirtschaftlich belastet werden können. Insbesondere hinsichtlich journalistisch-redaktioneller Mediendienste ist entsprechende Sorgfalt erforderlich, um weiterhin einen möglichst niedrigschwelligen Zugang zu faktenbasierten und vertrauenswürdigen Informationen und Inhalten zu gewährleisten.

III. Altersgrenzen, Altersverifikation und spezifische Schutzräume

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

Strikte Altersgrenzen sind dort sinnvoll, wo sie sachlich geboten sind, zum Beispiel um den Zugriff auf pornografische und andere entwicklungsgefährdende Inhalte zu verhindern. Gleichfalls sind sie ein bewährtes Instrument zur Steuerung des Zugangs zu

individuell altersbewerteten Inhalten, die nicht für Nutzerinnen und Nutzer jeden Alters geeignet sind (z.B. Spiele, Serien und Filme).

Verbindliche Altersgrenzen eignen sich aber **nicht pauschal für bestimmte Gattungen digitaler Angebote**. Auch der europäische Gesetzgeber hat sich im DSA bewusst gegen starre Altersgrenzen oder pauschale Nutzungsverbote entschieden und stattdessen einen risikobasierten, an der konkreten Ausgestaltung des jeweiligen Dienstes orientierten Ansatz gewählt. Maßgeblich ist nicht allein das Alter, sondern die Frage, welche Risiken ein bestimmtes Angebot für Minderjährige birgt und wie diesen Risiken wirksam begegnet werden kann.

Starre Altersgrenzen für die Nutzung ganzer Dienstegattungen werden der sehr verschiedenen Entwicklung junger Menschen nicht gerecht.

Mediennutzungskompetenzen, soziale Reife und Unterstützungsbedarfe entwickeln sich nicht linear und lassen sich grundsätzlich nicht sinnvoll an einer einzelnen Altersmarke festmachen, die für eine Vielzahl verschiedener Dienste gelten würde.

Gerade für Jugendliche sind digitale Kommunikationsräume ein **wichtiger Ort sozialer Teilhabe, Meinungsbildung und Identitätsentwicklung**. Ein pauschaler Ausschluss von diesen Räumen birgt die Gefahr, Schutzdefizite eher zu vergrößern als zu verringern, etwa durch Ausweichbewegungen in weniger regulierte Angebote.

Pauschale Altersgrenzen für soziale Medien, wie sie derzeit diskutiert werden, sind kein geeignetes Mittel, um Minderjährige zu schützen. Vielmehr entlassen sie die Plattformanbieter aus ihrer Verantwortung, da diese sich dann darauf berufen können, dass keine Minderjährigen ihre Dienste nutzen (dürfen) und sie daher keine Vorkehrungen zu deren Schutz treffen müssen. Dies würde ein über die Jahre gewachsenes System von abgestimmten und funktionierenden Jugendschutzmaßnahmen zunichtemachen. Dass ein Wegfall oder Zurückfahren solcher individuellen Einstellmöglichkeiten auch nachteilig für erwachsene Nutzerinnen und Nutzer wäre, kommt erschwerend hinzu.

Auch aus rechtlicher Sicht sind solche Verbotsbestrebungen zumindest problematisch, da sie den **Vorrang des DSA** außer Acht lassen. Der DSA entfaltet vollharmonisierende Wirkung¹⁸: Sein Anwendungsvorrang hindert Mitgliedsstaaten, anders- (oder sogar gleich-) lautende Vorschriften im selben Regelungsbereich zu erlassen. Da der DSA kein pauschales Aussperren Minderjähriger von Online-Plattformen vorsieht, sind nationale Alleingänge diesbezüglich nicht möglich.

¹⁸ Gleichwohl lässt der DSA einzelne Vorschriften anderer EU-Rechtsakte unberührt, so z.B. die AVMD-RL (Art. 2 Abs. 4 lit. a DSA).

Etwas anderes ergibt sich auch nicht aus Punkt 37 (d) der DSA-Leitlinien. Im Grunde genommen regelt dieser Punkt lediglich den Zugang zu Waren und Dienstleistungen *auf* Plattformen, nicht den allgemeinen Zugang *zu* Plattformen. Sofern der letzte Halbsatz „(...) einschließlich eigens definierter Kategorien von Online-Diensten sozialer Medien“ als Rechtsgrundlage für Mitgliedsstaaten gesehen wird, auf nationaler Ebene altersbedingte Zugangsbeschränkungen einzuführen, so ist auch hier der laut Nr. 37 (d) ausdrücklich notwendige „Einklang mit Unionsvorschriften“ zu beachten. Dieser Einklang ist aufgrund des DSA-Vorrangs aber gerade nicht gegeben. Die Leitlinien als unverbindliche Auslegungshinweise der EU-Kommission sind im Übrigen nicht geeignet, ausdrückliche Abweichungen von den Bestimmungen des DSA selbst zu rechtfertigen oder zu ermöglichen.

Auf das **Positionspapier der FSM** („Social Media und junge Menschen: Jugendmedienschutz im Spannungsfeld von digitalen Lebenswelten und Forderungen nach einem neuen Mindestalter“) vom 15. Dezember 2025 wird ergänzend und vollumfänglich Bezug genommen.¹⁹

2. Wie sollte eine altersangemessene Altersverifikation rechtlich und praktisch ausgestaltet werden?

Auf begrifflicher Ebene wird im Jugendmedienschutz unter „Altersverifikation“ stets die **strikte Überprüfung der Volljährigkeit** verstanden, üblicherweise im Rahmen von Zugangsbeschränkungen für Inhalte i.S.d. § 4 Abs. 2 JMStV.

Daneben treten weitere Maßnahmen, für die das Alter von Nutzerinnen und Nutzern relevant ist, und die ein **geringeres Maß an Verlässlichkeit** erfordern. Technische Mittel wie die Überprüfung der Personalausweisnummer oder die Altersschätzung anhand von biometrischen Merkmalen (v.a. *Facial Age Estimation*) kommen hier in Betracht, wobei letztere bei Vorliegen einer entsprechenden Eignung auch für den Volljährigkeitsnachweis i.S.d. § 4 Abs 2 JMStV nutzbar sein können. Aber auch ein näherungsweise Bestimmen des Alters von Personen anhand ihrer Nutzungsweise von bestimmten Diensten kann ein angemessener Weg sein.

Eine altersangemessene Feststellung und ggf. Überprüfung des Alters von Nutzerinnen und Nutzern sollte **verhältnismäßig, datenschutzkonform und risikobasiert** ausgestaltet sein. Intensität und Form der Altersprüfung muss also vom Gefährdungspotenzial der Inhalte abhängen. Dies ist für den Regelungsbereich der AVMD-Richtlinie im Übrigen auch auf EU-Ebene seit langer Zeit anerkannt.²⁰ Dabei sind Grundrechte, insbesondere Informationsfreiheit und Datenschutz, zu wahren. Um

¹⁹ https://www.fsm.de/files/2026/01/20251215_positionspapier_social-media.pdf

²⁰ Vgl. Art. 6a Abs. 1 AVMD-RL.

gemäß den DSA-Leitlinien²¹ als wirksam zu gelten, sollten Methoden zur Altersüberprüfung genau, robust, zuverlässig und nicht diskriminierend sein. An den europäischen Prozessen sollte man sich orientieren, denn sie sind – für den Bereich des DSA – maßgeblich. Nationale Alleingänge innerhalb des koordinierten bzw. harmonisierten Rechtsrahmens sind hingegen wenig erfolgsversprechend.

Daneben sind aber nationale Entscheidungsspielräume außerhalb des Geltungsbereichs des DSA zu beachten, so z.B. für Video-Sharing-Plattformen, deren Jugendschutzvorgaben aus der AVMD-RL und den jeweiligen Umsetzungsgesetzen der Mitgliedsstaaten folgen, sowie für „klassische“ Websites, bei denen es sich nicht um Vermittlungsdienste bzw. Online-Plattformen i.S.d. DSA handelt.

KJM und FSM haben in der Vergangenheit für die Zwecke des JMStV zusammengekommen bereits weit mehr als 100 verschiedenster Systeme aus Deutschland und Europa geprüft und für vereinbar mit deutschem Recht erklärt. **Seit dem 1. Dezember 2025 liegt die gesetzliche Zuständigkeit dafür ausdrücklich bei der FSM** (§§ 4 Abs. 4 S. 2, 5 Abs. 8 S. 2 JMStV). Derzeit arbeiten KJM und FSM daran, gemeinsame Kriterien für Altersverifikationssysteme und andere technische Mittel zur Altersfeststellung aufzustellen.²²

Neben diese bekannten und bewährten Systeme treten künftig digitale Wallets, die u.a. staatliche Identitäts- und Altersnachweise einbeziehen. Sie werden, ebenso wie europarechtliche Entwicklungen und Sichtweisen, bei der Kriterienentwicklung in Deutschland angemessene Berücksichtigung finden.

Beachtenswert ist in diesem Zusammenhang, dass insbesondere jungen Menschen oft keine (digital nutzbaren) Ausweisdokumente zur Verfügung stehen, um ihr Alter verlässlich online nachzuweisen. Methoden zur Altersschätzung, die grundsätzlich altersgruppenunabhängig funktionieren und zum Teil gute und genaue Ergebnisse liefern, kommen zudem an ihre Grenzen, wenn ein präziser (im Zweifelsfall: taggenauer) Altersnachweis erforderlich sein sollte. Genau darum geht es aber, wenn eine starre Altersgrenze, deren Einhaltung zu verifizieren wäre, gefordert würde. Ohne die **Einbeziehung der Eltern** wird deshalb ein strikter Altersnachweis, unabhängig von der schließlich gewählten Altersstufe, nicht für alle jungen Menschen zu erbringen sein.

²¹ Vgl. oben Fn. 1.

²² Vgl §§ 4 Abs. 4 S. 1, 5 Abs. 8 S. 1 JMStV.

3. 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?

Die Altersabsicherung sollte sich am Risiko des jeweiligen Angebots orientieren. Die Geeignetheit einer Altersabsicherung ist damit in erster Linie an ihrer **Zuverlässigkeit und Verhältnismäßigkeit** zu messen. Dabei sollte das jeweilige System selbst technische und organisatorische Maßnahmen implementieren, um Manipulation (z.B. Lebenderkennung, Nutzung der Frontkamera etc.) und Umgehungsmöglichkeiten zu verhindern oder zu erschweren. Im Rahmen der Verhältnismäßigkeit ist beachtlich, wie strikt, aufwendig und verlässlich eine Altersüberprüfung angelegt ist: Nicht für jeden Einsatzzweck muss beispielsweise eine sichere Altersverifikation auf Basis staatlicher Dokumente oder Wallets gefordert werden.

Die individuellen Maßnahmen einer Anwendung zur Altersüberprüfung können dann bei einer **Zertifizierung durch die FSM** (z.B. im Rahmen von §§ 4 Abs. 4, 5 Abs. 8 JMStV) überprüft werden.

Um Over-Collection zu vermeiden, sollte stets nur die Altersaussage und nicht die Identität verarbeitet werden. Zu diesem Zwecke können beispielsweise *Zero-Knowledge-Proofs*²³ oder *Double Blindness*-Ansätze verwendet werden.

Die Gefahr einer Diskriminierung z.B. aufgrund von Alter, Geschlecht oder Ethnizität kann durch barrierefreie Zugänge und alternative Nachweismöglichkeiten reduziert werden. Idealerweise sollte auch mehr als eine Methode zur Altersabsicherung angeboten werden. Bei KI-basierten Anwendungen sollte zudem selbstverständlich auf diskriminierungsfreie und diverse Trainings- und Datensätze geachtet werden.

4. 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?

Kinder und Jugendliche bewegen sich in digitalen Räumen, die überwiegend für Erwachsene konzipiert, ökonomisch getrieben und öffentlich strukturiert sind. Kinder und Jugendliche benötigen jedoch **altersangemessene Schutzräume**, um ihre Identität und sozialen Rollen auszuprobieren. Geschlossene oder begrenzte digitale Räume können diese Entwicklungsbedingungen besser gewährleisten als offene Plattformen. Denn in gemischten digitalen Räumen für Nutzerinnen und Nutzer verschiedenster Altersstufen bestehen strukturelle Ungleichgewichte. Ein eingeschränkter Zugang für

²³ <https://de.wikipedia.org/wiki/Null-Wissen-Beweis>

Erwachsene zu Angeboten speziell für junge Menschen kann diese Asymmetrien verringern und das Sicherheitsgefühl junger Nutzerinnen und Nutzer stärken.

Wichtig ist, wie man diese Schutzräume für Kinder und Jugendliche verantwortungsvoll umsetzt, ohne neue Risiken zu schaffen. Dies kann technisch und organisatorisch sehr anspruchsvoll sein. Zudem sollten sie auch immer pädagogisch begleitet werden. Einen Ersatz für umfassende Medienbildung können sie aber nicht bieten.

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?

Die Zielrichtung dieser Frage bleibt zunächst dunkel.

Es kann aber davon ausgegangen werden, dass die heute ohnehin populären Online-Plattformen auch **in der Schule, im außerschulischen pädagogischen Bereich oder in der offenen Jugendarbeit** breiter genutzt werden könnten, wenn technisch-organisatorisch sicherzustellen wäre, dass die für die jeweilige Nutzerin oder den jeweiligen Nutzer am besten geeigneten und sichersten Einstellungen unveränderlich vorgewählt wären.

Welche Einstellungen das jeweils sind und wie sie idealerweise für die einzelnen Kinder und Jugendlichen aus- oder vorzuwählen sind, ist jedoch weniger eine Frage von „Jugendschutz by design“, sondern ergibt sich in der **Gesamtschau aller Maßnahmen** von Schutz, Befähigung und Teilhabe.

Unabhängig davon ist hier festzuhalten, dass in Deutschland niedergelassene Mediendienste diesen Schutz bereits umfassend gewähren (s.o. I.1.). Daher bieten **journalistisch-redaktionelle Mediendienste** Heranwachsenden hohe Chance in den Bereichen Information, Bildung, Beteiligung und Freizeit.

Zur Beantwortung wird ergänzend auf die obigen Ausführungen zur Leitfrage sowie in den Abschnitten I. bis III. verwiesen.

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)?

Die reine Dauer der Mediennutzung ist kein „klassisches“ Jugendschutzkriterium, aber die veränderten digitalen Angebote, insbesondere in Spielen und auf Online-Plattformen, und die damit einhergehenden Nutzungsgewohnheiten junger Menschen bringen neue Risikodimensionen mit sich.

Laut der repräsentativen FSM-Studie Jugendmedienschutzindex 2022 sorgen sich 50 Prozent der Eltern, dass ihr Kind zu viel Zeit online verbringt. Am stärksten ausgeprägt zeigte sich diese Sorge bei den Eltern der 11- bis 12-Jährigen (54%) sowie 13- bis 14-Jährigen (56%). 72 Prozent der Kinder und Jugendlichen äußerten selbst, dass es ihnen schon mal passiert sei, zu viel Zeit online verbracht zu haben, bei den 13- bis 16-Jährigen waren es sogar 79 Prozent.²⁴

Laut der repräsentativen JIM-Studie 2025 stimmen 68 Prozent der Jugendlichen (12 bis 19 Jahre) zu, dass sie viel mehr Zeit am Handy verbringen, als sie ursprünglich gewollt haben. 60 Prozent äußern, dass sie nachts bewusst das Handy ausschalten oder in den Ruhemodus versetzen würden.²⁵

Um die Bedürfnisse von jungen Menschen sowie ihrer Eltern und Erziehenden nach einer **gesunden Balance bei der Nutzung von Medien und Online-Plattformen** nachzukommen, bieten Anbieter von Diensten und Betriebssystemen hier vermehrt Einstellungen und Funktionen, die es Nutzenden individuell ermöglichen, ihre Bildschirmzeit und Nutzungsdauer zu regulieren, regelmäßige Pausen einzulegen und eine gesündere Mediennutzung zu fördern (z.B. Nicht-Nutzung während Schlafenszeiten). Konten für Minderjährige auf Social-Media-Plattformen halten teils entsprechende Default-Einstellungen (z.B. limitierte Nutzungszeit am Tag) vor. Zudem bieten Schutz- und Begleitfunktionen für Eltern („family pairing“) die Möglichkeit, entsprechende Einstellungen für das eigene Kind festzulegen, darunter bspw. auch Zeitlimits, Zeitphasen für Nicht-Nutzung, Schul-Modus o.ä.).

Darüber hinaus ist es auch hier essenziell, junge Menschen frühzeitig über problematische Mediennutzungsgewohnheiten aufzuklären und sie zu unterstützen, ihr **eigenes Verhalten kritisch zu hinterfragen**. Dazu gehört auch die Vermittlung von Warnsignalen, Erklärungen über die Mechanismen und Features von Diensten und Plattformen, welche exzessive Nutzung begünstigen können, und die Vermittlung von Handlungsstrategien für einen gesunden Umgang. Eltern, Erziehende, Lehr- und

²⁴ https://www.fsm.de/files/2023/01/fsm_jmsindex_2022_barrierefrei.pdf

²⁵ https://mpfs.de/app/uploads/2025/11/JIM_2025_PDF_barrierearm.pdf

pädagogische Fachkräfte benötigen hier Unterstützung und Bildungsangebote, um Kinder und Jugendliche entsprechen zu begleiten und zu stärken, aber auch, um sich ihrer eigenen **Vorbildrolle als Erwachsene** bewusst zu werden.

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?

Wenn Kinder sich und ihren Alltag auf sozialen Netzwerken wie YouTube, TikTok oder Instagram einer großen Menge an Menschen präsentieren, spricht man von Kinder-Influencing oder Kindern als Content Creator. Auch wenn Eltern Bilder oder Videos mit ihrem Kind online veröffentlichen, werden Kinder bereits in jungem Alter zu Akteurinnen und Akteuren im Netz (Sharenting, Family-Influencing). In beiden Fällen müssen Kinder vor Gefahren wie z.B. möglichen Privatsphäreverletzungen, sexueller Belästigung, Cybermobbing oder Cybergrooming geschützt und ihre Rechte gewahrt werden. Gleichzeitig haben Kinder ein Recht darauf, Teil des digitalen Alltags zu sein, Online-Angebote zu nutzen und sich Anderen auf digitalem Wege mitzuteilen. Es ergibt sich die Herausforderung, Jugendmedienschutz und Teilhabe gleichermaßen zu ermöglichen.

Sind Kinder im Internet zu sehen oder posten eigenen Content, **tragen die Eltern als volljährige und geschäftsfähige Personen die Verantwortung** für den Kanal. Sie müssen diesen entsprechend verwalten und sind dazu verpflichtet, rechtliche Vorgaben einzuhalten. Eltern stehen vor der Aufgabe, ihre Kinder im Netz zu begleiten und ihnen einen reflektierten und sicheren Umgang mit sozialen Medien zu ermöglichen.

Beim Erstellen von Content ist darauf zu achten, keine ungeeigneten Inhalte zu veröffentlichen. Die Inhalte dürfen weder das eigene noch andere Kinder schädigen oder ängstigen. Kinder sollten nicht in Badebekleidung, Unterwäsche oder Schlafsachen gefilmt werden. Szenen und Bilder, in denen Kinder in sexuell anzüglichen Posen dargestellt werden, sind absolut unzulässig (§ 4 Abs. 1 Nr. 9 JMStV). Das Veröffentlichen solcher Darstellungen kann auch strafrechtlich geahndet werden. Ungeeignet sind auch Inhalte, die Gewalt darstellen. Zudem sollten keine gefährlichen Situationen gefilmt werden, die andere Kinder zum Nachahmen animieren.

Die Beschäftigung von Kindern ist gemäß § 5 Abs. 1 Jugendarbeitsschutzgesetz (JArbSchG) grundsätzlich verboten. Nach § 2 Abs. 1 JArbSchG ist Kind im Sinne des Gesetzes, wer noch nicht 15 Jahre alt ist. Ausnahmen können für Kinder ab drei Jahren unter der Maßgabe der Regelungen des § 6 JArbSchG für Dreharbeiten auf Antrag bewilligt werden. Dabei ist zu beachten, dass für Kinder unter drei Jahren jede Form der Beschäftigung verboten ist. Eine Ausnahmegewilligung ist jedoch erst dann notwendig, wenn eine Beschäftigung des Kindes im Sinne des JArbSchG vorliegt. Einer

Ausnahmebewilligung bedarf es somit nicht, wenn nur eine geringfügige und gelegentliche Hilfeleistung oder ein Fall der erlaubten Beschäftigung nach § 5 Abs. 2 bis 4a JArbSchG vorliegt. Beschäftigung liegt i.d.R. vor, wenn das Kind mit seiner Contentproduktion Arbeit im wirtschaftlichen Sinne im Interesse eines Dritten leistet. Voraussetzung ist eine Weisungsgebundenheit des Kindes. Indizien für eine Beschäftigung im Sinne des JArbSchG sind eine gewisse Regelmäßigkeit, ein großer Umfang, längere Dauer der erfolgten Arbeitsleistung sowie eine Vergütungsvereinbarung. Ob eine genehmigungspflichtige Beschäftigung vorliegt, muss im Einzelfall entschieden werden. Sollten Kooperationen eingegangen werden, bei denen Vorgaben/Regieanweisungen o. ä. durch den Werbepartner erfolgen, sollten sich Eltern von den Jugendämtern bzw. den Gewerbeämtern beraten lassen.

Damit eine **sichere Teilhabe** gelingen kann, ist neben den rechtlichen Vorgaben zu Jugendmedien- und Arbeitsschutz auf einen sensiblen Umgang mit der Privatsphäre und den persönlichen Daten des Kindes und anderer Personen zu achten. Beispielsweise sollte es genug Rückzugsorte geben, an denen der Alltag nicht gefilmt wird. Persönliche Daten sind Daten, die Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person machen. Dazu gehören beispielsweise Namen, Telefonnummern, Kontodaten, die Anschrift und das Aussehen, aber auch Standortdaten (z. B. der Schulweg des Kindes). Diese Informationen sollten auf keinen Fall veröffentlicht werden.

Die Entscheidung, welche Inhalte unter Einhaltung der rechtlichen Rahmenbedingungen und dem Schutz der Privatsphäre hochgeladen werden, sollte immer beim Kind selbst liegen. In der Vergangenheit hochgeladene Inhalte sollten regelmäßig daraufhin überprüft werden, ob sich das Kind noch wohl damit fühlt, dass diese einer breiten Öffentlichkeit zugänglich sind.

Um Kinder vor den genannten Gefahren zu schützen und ihre Rechte zu wahren, bietet die Arbeitsgruppe „Kinder-Influencing“, die aus der FSM und sechs weiteren interdisziplinären Institutionen der Handlungsfelder Medienpädagogik, Jugendmedienschutz und Kindermedien besteht, [umfangreiche Handlungsempfehlungen](#)²⁶ sowie eine [Checkliste](#)²⁷ mit den wichtigen Aspekten. In Kürze werden ergänzend hierzu **Aufklärungsvideos für Kinder** veröffentlicht.

* * *

²⁶ https://www.fsm.de/files/2022/03/2020_handlungsempfehlungen_kinder-influencing.pdf

²⁷ <https://mediasmart.de/handlungsempfehlungen-kinder-influencing/>