

Online-Sicherheit von Kindern

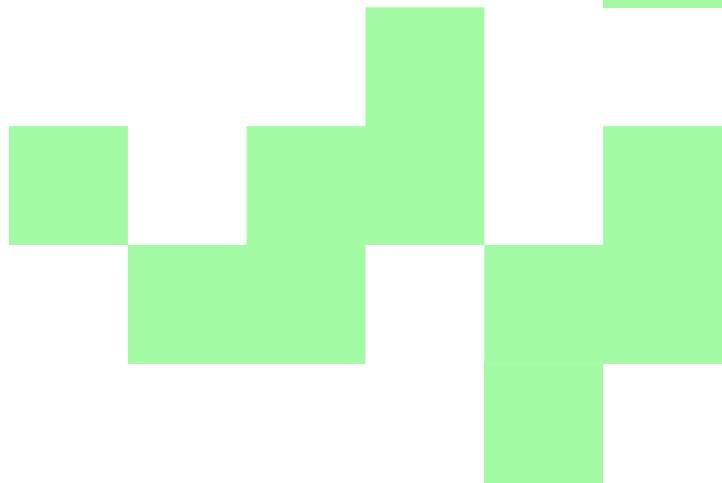
SCHUTZ UND STÄRKUNG VON MINDERJÄHRIGEN IN EINER DIGITALEN WELT

BERICHT DER KO-VORSITZENDEN DES SONDERAUSSCHUSSES

FÜR DIE ONLINE-SICHERHEIT VON KINDERN

Prof. Dr. Jörg M. Fegert und Dr. Maria Melchior





Vorbemerkung

Im März 2026 betraute die Präsidentin der Europäischen Kommission Ursula von der Leyen zwei Sonderberater – Prof. Dr. Jörg M. Fegert und Dr. Maria Melchior – mit dem Vorsitz des Sonderausschusses für die Online-Sicherheit von Kindern und mögliche Altersbeschränkungen für die Nutzung sozialer Medien. Die Ko-Vorsitzenden wurden beauftragt, einen Bericht über die Ergebnisse der Beratungen des Ausschusses zu verfassen und Empfehlungen dazu abzugeben, wie Europa die Online-Welt für Kinder sicherer machen kann.

In dem Ausschuss, den die Kommissionspräsidentin erstmals in ihrer Rede zur Lage der Union 2025 angekündigt hatte, kamen hochrangige Wissenschaftlerinnen und Wissenschaftler, Praktikerinnen und Praktiker, Jugend- und Elternvertreterinnen und Vertreter sowie andere Fachleute aus verschiedenen Bereichen aus ganz Europa zusammen, um die Auswirkungen sozialer Medien auf Minderjährige zu prüfen.

Der Sonderausschuss trat dreimal zusammen, wobei jeweils unterschiedliche Fachleute an den Gesprächen teilnahmen. Die erste Sitzung des Sonderausschusses fand am 5. März 2026 statt und hatte die aktuellen wissenschaftlichen Erkenntnisse über die Auswirkungen sozialer Medien und des digitalen Umfelds im weiteren Sinne auf Kinder und Jugendliche zum Thema.

In der zweiten Sitzung des Sonderausschusses, die am 16. April 2026 stattfand, wurden die bestehenden Rechtsvorschriften und Instrumente der EU sowie die nationalen politischen Ansätze für den Umgang mit der Online-Sicherheit von Kindern erörtert. In der dritten Sitzung des Sonderausschusses am 16. Juni 2026 ging es vor allem um nationale Konzepte und mögliche Empfehlungen zum Schutz und zur Stärkung von Kindern und Jugendlichen in der digitalen Welt.

„[Wir werden] uns vor allem zum Ziel setzen, die Eltern zu stärken und ein sichereres Europa für unsere Kinder aufzubauen. Denn wenn es um die Sicherheit unserer Kinder im Internet geht, glaubt Europa an Eltern, nicht an Gewinne.“

— URSULA VON DER LEYEN,
PRÄSIDENTIN DER EUROPÄISCHEN
KOMMISSION, REDE ZUR LAGE
DER UNION 2025

ZU DEN WICHTIGSTEN THEMEN, DIE IN DEN SITZUNGEN DES

SONDERAUSSCHUSSES DEBATTIERT WURDEN, GEHÖRTEN FOLGENDE:

- // die positiven und negativen Auswirkungen der Einführung spezifischer Altersbeschränkungen für die Nutzung sozialer Medien und anderer digitaler Dienste,
- // maßgeschneiderte Ansätze zum Schutz und zur Stärkung Minderjähriger entsprechend den Altersgruppen, dem sozioökonomischem Hintergrund und altersspezifischen Risiken,
- // Sicherheit durch Technikgestaltung/Voreinstellungen und Verantwortung der Anbieter sozialer Medien und anderer digitaler Dienste,
- // Aufklärungs- und Sensibilisierungsmaßnahmen zur Förderung einer verantwortungsvollen Internetnutzung durch Kinder und Jugendliche, Eltern und Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte,
- // Möglichkeiten, Eltern und pädagogische Fachkräfte zu unterstützen und Kinder und Jugendliche in die Lage zu versetzen, die Chancen der digitalen Welt zu nutzen.

Die Analyse und die Empfehlungen dieses Berichts stützen sich auf wichtige Beiträge einer vielfältigen Gruppe von Sachverständigen, die zu den einzelnen Ausschusssitzungen eingeladen wurden; sie stützen sich auch auf Beiträge aus zahlreichen zusätzlichen Sitzungen mit Vertreterinnen und Vertretern der Mitgliedstaaten, insbesondere denjenigen, die vom irischen Vorsitz des Rates der EU und Luxemburg (D9+-Ministertagung) ausgerichtet wurden, von Drittländern (einschließlich Australien und Brasilien), des Europäischen Parlaments und von dessen Mitgliedern, insbesondere der interfraktionellen Arbeitsgruppe für die Rechte des Kindes, der Industrie, der Zivilgesellschaft sowie von Denkfabriken und anderen Organisationen, einschließlich des OHCHR der Vereinten Nationen und des Europäischen Datenschutzausschusses (EDSA).

Im Anschluss an diese Begegnungen arbeiteten die Ko-Vorsitzenden auf der Grundlage der gesammelten Erkenntnisse ihre Empfehlungen aus. Zwar liegt die Verantwortung für die Empfehlungen ausschließlich bei den Ko-Vorsitzenden, doch beruht ihre Arbeit in hohem Maße auf den Beiträgen anderer renommierter Sachverständiger sowie von Eltern- und Jugendvertreterinnen und -vertretern und auf dem Fachwissen der Europäischen Kommission.

Der Bericht soll als Grundlage für künftige Maßnahmen dienen, welche die Europäische Kommission und die EU-Mitgliedstaaten zur Stärkung der Online-Sicherheit von Kindern vorschlagen werden. Die vorliegende unabhängige analytische Bewertung enthält Empfehlungen und Anregungen für Kinder und Jugendliche, Eltern und Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte sowie Anbieter sozialer Medien und anderer digitaler Dienste dazu, wie Minderjährige online besser geschützt und gestärkt werden können.

GEGENSTAND UND TERMINOLOGIE

Die von Präsidentin von der Leyen vorgegebene Hauptaufgabe des Sonderausschusses bestand darin, die Online-Sicherheit von Kindern und mögliche Altersbeschränkungen für die Nutzung sozialer Medien zu erörtern. Zwar entspricht der Gegenstand dieses Berichts dieser Aufgabenstellung, doch haben die fortschreitenden Diskussionen während der Sitzungen des Sonderausschusses und andere politische Entwicklungen (z. B. der Appell der Führungsspitzen der G7 vom 17. Juni 2026 für einen sichereren digitalen Raum für Minderjährige) deutlich gemacht, dass die in diesem Bericht verwendete Terminologie präzisiert werden sollte.

Unbeschadet internationaler, EU- oder nationaler Rechtsakte werden im vorliegenden Bericht die folgenden Begriffe und die entsprechenden Begriffsbestimmungen verwendet:

Soziale Medien und andere digitale Dienste (kurz: soziale Medien+)

Im Rahmen dieses Berichts werden die Begriffe „soziale Medien+“ und „soziale Medien und andere digitale Dienste“ verwendet, um im weitesten Sinne Dienste zu definieren, die Minderjährigen zur Verfügung stehen und altersunangemessene und/oder riskante Merkmale (z. B. suchterzeugende und schädliche Merkmale, darunter unendliches Scrollen, das automatische Abspielen von Medieninhalten, Empfehlungsalgorithmen und ständige Benachrichtigungen) und/oder Inhalte enthalten können. Zu den Anbietern sozialer Medien und anderer digitaler Dienste gehören Online-Plattformen, die als Vermittler von Inhalten Dritter fungieren, z. B. soziale Medien, sowie App-Stores. Auch KI-Systeme, die Risiken für die Sicherheit und Entwicklung von Minderjährigen bergen, darunter KI-Gefährten, Videospiele, bei denen Kinder schädlichen Geschäftspraktiken oder gefährlichen Kontakten ausgesetzt sind, und Video-Sharing-Plattformen, die Minderjährigen einen nicht altersgerechten Zugang ermöglichen, fallen in diese Kategorie.

Minderjährige, Kinder und Jugendliche

Unbeschadet der gesetzlich festgelegten Bedeutung des Begriffs „Kinder“ (z. B. im Übereinkommen der Vereinten Nationen über die Rechte des Kindes) wird in diesem Bericht für einen notwendigen entwicklungsorientierten Ansatz zum Schutz Minderjähriger online plädiert, der den spezifischen Risiken und Anfälligkeiten Rechnung trägt, denen sie je nach Alter ausgesetzt sind. Für die Zwecke der vorliegenden Analyse verwenden die Autoren den Begriff „Minderjährige“ für alle Kinder und Jugendlichen unter 18 Jahren (dem Alter der Volljährigkeit). Der Begriff „Jugendliche“ bezeichnet alle Minderjährigen im Alter von 13 bis 18 Jahren. Der Begriff „Kinder“ erstreckt sich auf alle Minderjährigen unter 13 Jahren. Der Begriff „Kinderrechte“ bezeichnet in diesem Bericht die in Rechtstexten definierten Rechte aller Kinder und Jugendlichen unter 18 Jahren. Der im Mandat für die Tätigkeit des Sonderausschusses genannte Begriff „Online-Sicherheit von Kindern“ wird als Oberbegriff für den Schutz und die Stärkung von Minderjährigen in der digitalen Welt verwendet.

VORWORT

Sicheres Aufwachsen in der Welt der sozialen Medien+

Der rasche Fortschritt der digitalen Technologien hat die Art und Weise, wie Kinder und Jugendliche aufwachsen und mit Gleichaltrigen, Eltern, Lehrkräften und der Welt um sie herum interagieren, radikal verändert. Gleichzeitig sind Aktivitäten in der Offline-Welt nach wie vor von entscheidender Bedeutung für das Lernen, die Entstehung tiefergehender Beziehungen und Erfahrungen, die die Entwicklung von Minderjährigen prägen.

Die Welt der sozialen Medien+ bietet Kindern und Jugendlichen viele Möglichkeiten zu lernen, Kontakte zu knüpfen, sich zu beteiligen und kreativ zu sein. Minderjährige müssen jedoch geschult und befähigt werden, diese Chancen zu nutzen, um ihr Potenzial voll auszuschöpfen.

Gleichwohl **bergen die sozialen Medien+ auch eine Reihe von Risiken** für die gesunde Entwicklung und das Wohlbefinden von Minderjährigen. Dazu gehören das Risiko einer durch suchterzeugende Funktionen begünstigten übermäßigen Nutzung, die Substituierung entwicklungsfördernder Tätigkeiten, die Konfrontation mit schädlichen Inhalten und unangemessene Kontakte im Internet. Diese Risiken werden durch das Aufkommen neuer Technologien noch verstärkt und erfordern mutige, aber wohlüberlegte Entscheidungen zum Schutz von Kindern und Jugendlichen online.

Die breite Nutzung sozialer Medien und anderer digitaler Dienste hat **bei politischen Entscheidungsträgern und Eltern große Besorgnis über die Bedrohungen ausgelöst, denen Kinder und Jugendliche online ausgesetzt sind**. Altersbeschränkungen für den Zugang zu sozialen Medien und anderen digitalen Diensten werden zwar kritisiert, doch **können sie eine notwendige Vorsichtsmaßnahme sein**, bis nachgewiesen ist, dass der Zugang zu sozialen Medien+ für Kinder und Jugendliche sicher ist, oder bis sichere Alternativen entwickelt werden.

Bei Altersbeschränkungen geht es nicht darum, Eltern und Betreuungspersonen oder Kinder und Jugendliche selbst in erster Linie für die Online-Sicherheit Minderjähriger verantwortlich zu machen. Ebenso wenig geht es darum, die Anbieter von ihrer Verantwortung zu entbinden. **Anbieter sozialer Medien und anderer digitaler Dienste tragen weiterhin die Hauptverantwortung für die Sicherheit der Dienste, die sie entwickeln und anbieten.**

Die Beweislast muss bei den Anbietern liegen, nicht bei den Regulierungsbehörden, Eltern und Kindern. **Solange die Anbieter sozialer Medien und anderer digitaler Dienste nicht nachweisen, dass ihre Dienste inhärent sicher ("safe by design") sind, sollten sie nur eingeschränkten Zugang zu Kindern unter 13 Jahren in der EU erhalten.** Zusätzlich zu den EU-weiten Beschränkungen können die Mitgliedstaaten weitere vorsorgliche Altersbeschränkungen für Jugendliche über 13 Jahren einführen.

Vorsorgliche Altersbeschränkungen sind Sofortmaßnahmen, um das langfristige Ziel zu erreichen, durch die Förderung des kulturellen Wandels sicherzustellen, dass Räume in den sozialen Medien+ für Minderjährige sicher sind. Erste Ergebnisse aus Ländern, die pauschale Altersbeschränkungen für den Zugang zu sozialen Me-

dien eingeführt haben, zeigen, dass die meisten Minderjährigen einen Weg finden, diese Maßnahmen zu umgehen. Gleichzeitig haben sich einige Minderjährige aus riskanten sozialen Medien und digitalen Diensten zurückgezogen und haben nun mehr Zeit für Offline-Aktivitäten (wie Sport und persönliche soziale Begegnungen). Dies zeigt, dass ein schrittweiser Wandel bei den Normen für die Nutzung sozialer Medien+ durch Minderjährige möglich ist und anerkannt werden muss.

Der Wandel braucht jedoch Zeit. So haben sich beispielsweise die gesellschaftlichen Einstellungen in Bezug auf das gesetzliche Verbot körperlicher Züchtigung in der Erziehung über mehr als eine Generation hinweg weiterentwickelt (z. B. in Deutschland und Schweden). Mit dem Verbot der körperlichen Züchtigung wurden die Erwartungen an Eltern, Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte präzisiert und das Engagement Außenstehender gestärkt, um die gewaltfreie Erziehung Minderjähriger sicherzustellen. Der Erfolg dieser Maßnahme wurde durch die positiven Trends und die kontinuierliche Bewertung seit ihrer Einführung nachgewiesen.

Auch die Wirksamkeit von Altersbeschränkungen würde eine Änderung gesellschaftlicher Einstellungen erfordern. Kontinuierliche Bewertung und langfristige Beobachtung können den politischen Entscheidungsträgern dabei helfen, zu erkennen, ob sich die Gewohnheiten von Minderjährigen und ihren Eltern, Betreuungspersonen und pädagogischen Fachkräften im Laufe der Zeit ändern.

Kinder und Jugendliche, die in der heutigen Welt der sozialen Medien+ aufwachsen, müssen in die Lage versetzt werden, ein gesundes und erfülltes Leben zu führen und die Möglichkeiten, die soziale Medien und andere digitale Dienste bieten, zu nutzen. **Die Kinderrechte gelten im Internet genauso wie im realen Leben** – vom Recht auf Sicherheit und Schutz vor wirtschaftlicher Ausbeutung und Kriminalität in allen Formen (insbesondere sexueller Gewalt) bis hin zum Recht auf Zugang zu Informationen, Bildung und Freizeit.

Kinder haben das Recht, in einer Umgebung aufzuwachsen, die sicher ist und ihre Entwicklung fördert, und zwar sowohl online als auch offline. Natürlich sollten Minderjährige offline weiter unterstützt werden, doch müssen wir auch anerkennen, dass Online-Umgebungen zu einem immer wichtigeren Bestandteil ihres täglichen Lebens geworden sind. Deshalb muss in allen sozialen Medien und anderen digitalen Diensten standardmäßig für Schutz gesorgt werden.

Die Kinderrechte müssen die Grundlage für Online-Maßnahmen zur Sicherheit von Kindern bilden. Mögliche Altersbeschränkungen müssen unter uneingeschränkter Achtung der Rechte des Kindes umgesetzt werden, verhältnismäßig sein und gegen das Wohl des Kindes abgewogen werden. Die Mittel, mit denen dies erreicht werden soll, müssen mit den technologischen Entwicklungen Schritt halten.

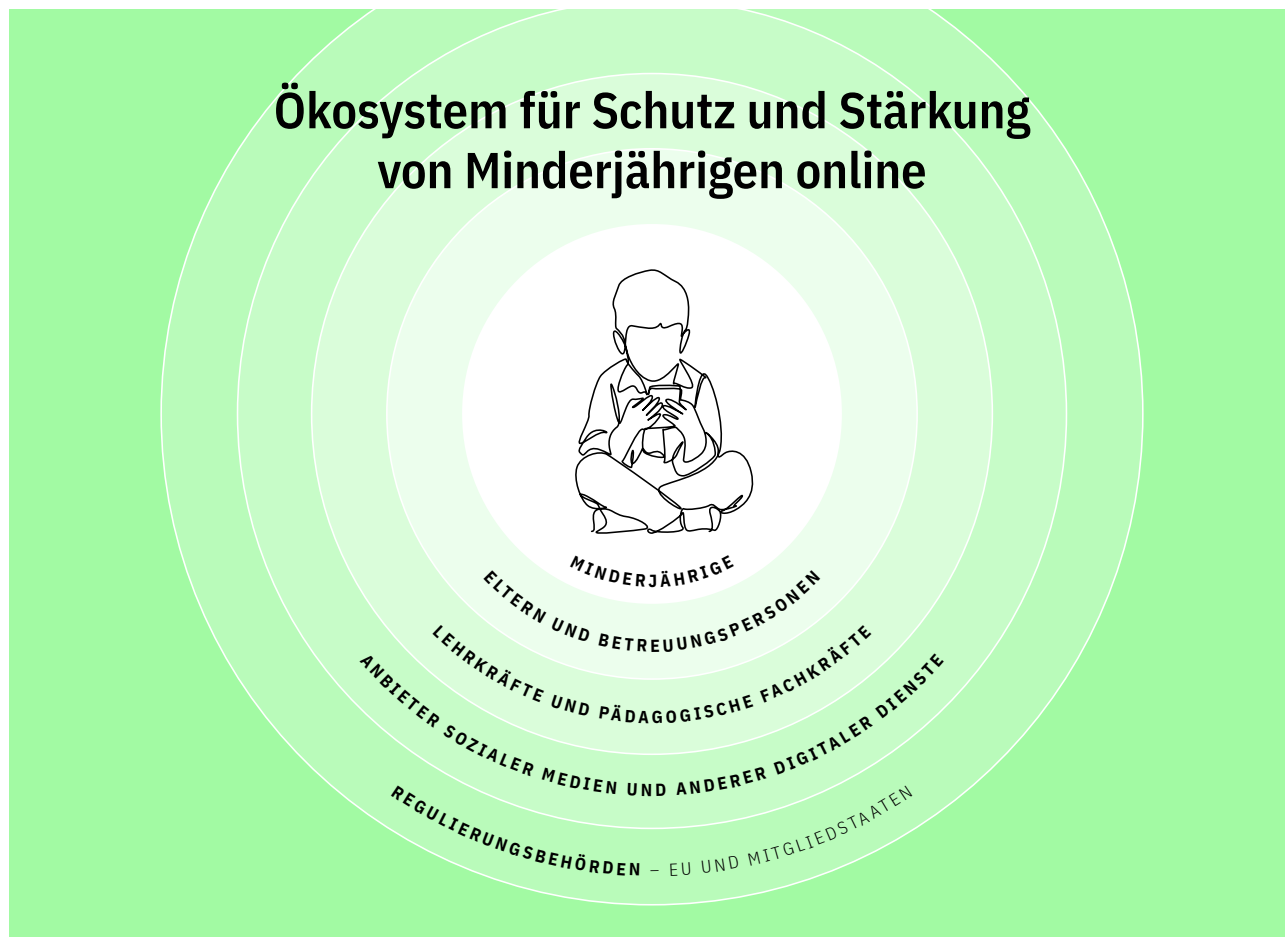
Zwar tragen nach wie vor die Anbieter sozialer Medien und anderer digitaler Dienste die Hauptverantwortung für die Sicherheit ihrer Dienste, insbesondere für Minderjährige, doch **bedarf es eines Ökosystems von Akteuren, um Kinder und Jugendliche in der Welt der sozialen Medien+ zu schützen und zu stärken.** Von den Regulierungsbehörden, die die erforderlichen Maßnahmen ergreifen müssen, über die Anbieter, die sichere und altersgerechte Dienste anbieten, bis hin zu Eltern, Betreuungspersonen, Lehrkräften und pädagogischen Fachkräften, die eine Schlüsselrolle bei der Überwachung und Anleitung der Online-Nutzung durch Minderjährige spielen. Da Minder-

„Seit Jahrzehnten arbeiten wir daran, die reale Welt für Kinder sicherer zu machen, und das Gleiche müssen wir auch in der digitalen Welt tun. Die Chancen, die uns die Technologie bietet, dürfen nicht auf Kosten der Sicherheit, Gesundheit oder des Glücks unserer Kinder gehen.“

— URSULA VON DER LEYEN, PRÄSIDENTIN DER EUROPÄISCHEN KOMMISSION

jährige reifer werden und sich die sozialen Medien+ rasch verändern, **hängt der Erfolg des Ökosystems von den miteinander verknüpften Maßnahmen aller Akteure ab**, die dieselbe Vision haben: Kinder und Jugendliche, die in einer digitalen Welt sicher aufwachsen.

Abbildung 1: Ökosystem zum Schutz und zur Stärkung von Minderjährigen online



Zunehmende politische Dynamik zugunsten einer Stärkung der Online-Sicherheit von Kindern

Die vergangenen Monate haben gezeigt, dass die Online-Sicherheit von Kindern weltweit immer größeres Gewicht in der Politik erhält. Die **Einführung, Umsetzung und kontinuierliche Evaluation des Hinauszögerns des Zugangs zu den sozialen Medien durch Australien hat der übrigen Welt wichtige Erkenntnisse geliefert**. Andere Länder wie das Vereinigte Königreich und Kanada sind dem Beispiel gefolgt und haben ebenfalls Legislativvorschläge geplant, und Indonesien hat bereits ein Verbot erlassen.

Einem aktuellen Bericht zufolge sind 92 % der Europäerinnen und Europäer der Ansicht, dass die Stärkung des Online-Schutzes von Kindern und Jugendlichen eine Priorität für die EU sein sollte^a.

a. Europäische Kommission, „Digitale Dekade – Eurobarometer-Bericht – Februar-März 2026“ (nur auf Englisch abrufbar), 2026.

Auch die politisch Verantwortlichen in Europa haben damit begonnen, sich mit diesem Thema zu befassen. Die Erklärung von Jütland^b vom September 2025 und die Entschließung des Europäischen Parlaments, in der ein EU-weites digitales Mindestalter gefordert wird^c, die Einsetzung des Sonderausschusses für die Online-Sicherheit von Kindern durch Präsidentin von der Leyen und die jüngsten Schlussfolgerungen des Europäischen Rates^d sind klare Anzeichen dafür, dass die politische Dynamik für konkrete Maßnahmen zur Bewältigung der zunehmenden Risiken, denen Kinder online ausgesetzt sind, zunimmt.

Im Juni 2026 einigten sich die G7 – Deutschland, Frankreich, Italien, Japan, Kanada, das Vereinigte Königreich, die Vereinigten Staaten und die Europäische Union – erstmals auf höchster politischer Ebene auf gemeinsame Grundsätze zum Schutz Minderjähriger vor digitalen Diensten, die Risiken bergen^e.

Darüber hinaus **erlassen mehrere EU-Mitgliedstaaten Rechtsvorschriften zur Festlegung eines Mindestalters für den Zugang zu sozialen Medien und anderen digitalen Diensten**, durch die Kinder und Jugendliche Schaden erleiden können. So schlägt Frankreich beispielsweise aktuell eine Altersgrenze von 15 Jahren auf der Grundlage einer schwarzen Liste zu beschränkender Dienste vor. Griechenland plant eine Altersgrenze von 15 Jahren für soziale Online-Netzwerke. Dänemark erwägt eine Beschränkung für Minderjährige unter 16 Jahren mit der Option, das Alter mit Zustimmung der Eltern zu senken. Schweden sieht eine Beschränkung auf der Grundlage des Jahres vor, in dem das Kind 15 Jahre alt wird, wobei mehrere Arten von Dienstleistungen ausgenommen sind. Viele andere, von Portugal und Spanien bis hin zu Deutschland und Polen, erwägen, Rechtsvorschriften zu diesem Thema zu erlassen.

Vor diesem Hintergrund stellt die Fragmentierung des europäischen Binnenmarkts für digitale Dienste ein echtes Risiko dar. Angesichts dessen fordern viele Mitgliedstaaten, dass dieses Thema auf EU-Ebene geregelt werden sollte. Es sollte anerkannt werden, dass die Mitgliedstaaten unterschiedliche kulturelle und nationale Herangehensweisen in Bezug auf Erziehung, digitale Kompetenz und den Schutz Minderjähriger haben. Eine Fragmentierung könnte dazu führen, dass Minderjährige je nach EU-Mitgliedstaat unterschiedliche Schutzniveaus genießen. Dies würde auch bedeuten, dass die Regulierungsbehörden mit praktischen Schwierigkeiten bezüglich der Durchsetzung und die Anbieter mit höheren Befolgungskosten konfrontiert sein könnten. Dies wiederum hätte Folgen für die Entwicklung sichererer sozialer Medien und anderer digitaler Dienste und für die Wirksamkeit der Rechtsvorschriften zur Online-Sicherheit.

Die EU hat bereits konkrete Maßnahmen zum Schutz von Minderjährigen ergriffen. Die jüngsten Beschlüsse der Europäischen Kommission haben nur unterstrichen, dass das Vorgehen gegen die Bedrohungen, denen Kinder und Jugendliche online ausgesetzt sind, auf konkreten Fakten beruhen muss. Die vorläufigen Feststellungen gegen Meta und TikTok wegen mutmaßlicher Nichteinhaltung der hohen Standards für den Online-Schutz Minderjähriger, die nach dem Gesetz über digitale Dienste erforderlich sind, und wegen der nicht erfolgten Bereitstellung leicht zugänglicher Mechanismen für die Meldung von sexuellem Kindesmissbrauch darstellenden Inhalten sind deutliche Beispiele. Darüber hinaus haben die jüngsten wegweisenden Urteile US-amerikanischer Gerichte einen historischen Wendepunkt in der Debatte über die Haftung von Plattformen markiert.

- b.** [Dänischer Vorsitz, Rat der Europäischen Union, „Die Erklärung von Jütland: Gestaltung einer sicheren Online-Welt für Minderjährige“ \(nur auf Englisch abrufbar\), 2026.](#)
- c.** [Europäisches Parlament, „Schutz von Minderjährigen im Internet – Entschließung des Europäischen Parlaments vom 26. November 2025 zu dem Schutz von Minderjährigen im Internet“ \(2025/2060\(INI\)\), 2025.](#)
- d.** [Europäischer Rat, Schlussfolgerungen des Europäischen Rates, 19. März 2026.](#)
- e.** [G7, „Leaders' call on a safer digital space for minors“ \(„Staats- und Regierungschefs fordern einen sichereren digitalen Raum für Minderjährige“, nur auf Englisch abrufbar\), 2026.](#)

Eine kurze Geschichte des Online-Schutzes von Minderjährigen

Die Bemühungen um den Schutz von Kindern und Jugendlichen im Internet sind so alt wie das Internet selbst und stammen aus einer Zeit vor sozialen Medien, Smartphones und KI. Die Grundlagen der heutigen Vorschriften zum Schutz von Minderjährigen im Internet wurden in den 1990er-Jahren und Anfang der 2000er-Jahre mit Rechtsakten geschaffen, die es Diensten und Unternehmen ermöglichen sollten, grenzüberschreitend tätig zu sein und Informationen auszutauschen. Obwohl diese Vorschriften nicht ausschließlich zum Schutz von Kindern und Jugendlichen im Internet konzipiert wurden, wurden darin viele der Grundsätze festgelegt, die den aktuell geltenden Rechtsvorschriften in drei Bereichen nach wie vor zugrunde liegen.

Erstens wurden mit der Regulierung von Medien und digitalen Diensten im Binnenmarkt gemeinsame Vorschriften für Fernsehprogramme in ganz Europa eingeführt, unter anderem Schutzvorkehrungen gegen Inhalte, die für Minderjährige schädlich sein könnten. Der erste harmonisierte Rahmen für Online-Dienste oder „Dienste der Informationsgesellschaft“ (im Rahmen der Richtlinie über den elektronischen Geschäftsverkehr) förderte auch die Entwicklung grenzüberschreitender Online-Dienstleistungen innerhalb der EU.

Der zweite Bereich sind die Vorschriften zum Datenschutz und zum Schutz der Privatsphäre, beginnend mit den gemeinsamen Normen der Datenschutzrichtlinie von 1995 für die Erhebung und Nutzung personenbezogener Daten in den Mitgliedstaaten.

Der dritte Bereich ist der Verbraucherschutz. Durch gemeinsame EU-Vorschriften werden irreführende und aggressive Geschäftspraktiken bekämpft. Mit diesen Vorschriften wird anerkannt, dass schutzbedürftige Verbraucherinnen und Verbraucher zusätzlichen Schutz benötigen, was ein wichtiger Grundsatz im digitalen Umfeld ist. Dies gilt auch für Fälle, in denen Kinder und Jugendliche Geschäftspraktiken ausgesetzt sind, die sie möglicherweise anders betreffen als Erwachsene.

Als die digitalen Technologien mit der Zeit ein immer größerer Bestandteil des alltäglichen Lebens wurden, hat die EU diese Rechtsrahmen immer wieder auf den neuesten Stand gebracht, um auf neue Herausforderungen zu reagieren. Mit der Datenschutz-Grundverordnung (DSGVO) wurden spezifische Schutzmaßnahmen zum Schutz der personenbezogenen Daten und der Einwilligung von Kindern im Internet eingeführt. Die Richtlinie über audiovisuelle Mediendienste wurde auf neue Formen audiovisueller Inhalte und Video-Sharing-Plattformen ausgeweitet. Schließlich wurden mit dem Gesetz über digitale Dienste Vorschriften für Online-Vermittlungsdienste festgelegt, unter anderem für den besonderen Zweck des Schutzes Minderjähriger.

Diese Entwicklung spiegelt einen allgemeinen Trend wider: Digitale Technologien lassen sich nicht mehr eindeutig in eine einzige regulatorische oder rechtliche Kategorie einordnen. Soziale Medien und andere digitale Dienste kombinieren Elemente von Medien, Kommunikation, Handel und Datenverarbeitung, häufig innerhalb derselben Plattform. Folglich muss ein wirksamer Ansatz für den Online-Schutz von Minderjährigen ganzheitlich sein und sich auf Instrumente in mehreren Bereichen des EU-Rechts stützen, einschließlich der Regulierung von Plattformen, des Datenschutzes, des Verbraucherschutzes und der Regulierung audiovisueller Medien.

Mit der raschen Entwicklung und Verbreitung von KI vervielfachen sich die Risiken für Minderjährige online. Parallel dazu werden soziale Medien und andere digitale Dienste kontinuierlich weiterentwickelt, um die Aufmerksamkeit der Nutzer in der heutigen „Aufmerksamkeitsökonomie“ zu wecken und aufrechtzuerhalten. Es ist wichtiger denn je, dass die Regulierungsbehörden tätig werden, um den Schutz von Minderjährigen zu stärken und sie in die Lage zu versetzen, sich in der Welt der sozialen Medien+ sicher zurechtzufinden.

Die Erkenntnisse über die Risiken und Chancen für Minderjährige online

Der rasche technologische Wandel hat Kindern außerordentliche Möglichkeiten eröffnet, sich mit Gleichaltrigen auszutauschen, ihre Kreativität zum Ausdruck zu bringen und Zugang zu Wissen und Hilfe zu erhalten. Kinder sind jedoch keine Erwachsenen, und in der Umgebung der sozialen Medien+ sind sie je nach ihrem Alter unterschiedlichen Risiken für ihre körperliche und psychische Gesundheit und Entwicklung ausgesetzt. Sozioökonomische und individuelle Faktoren wie der familiäre Hintergrund und das Geschlecht sowie die Gestaltung sozialer Medien und anderer digitaler Dienste haben ebenfalls prägenden Einfluss.

Solide Erkenntnisse darüber, wie Risiken und Schäden mit sozialen Medien und anderen digitalen Diensten zusammenhängen, sind unerlässlich, um geeignete Maßnahmen zum Schutz und zur Stärkung Minderjähriger online ergreifen zu können. Spezifische Merkmale, Funktionen oder Formate, die in sozialen Medien+ implementiert werden, können je nach den sozialen und persönlichen Umständen eines Kindes oder Jugendlichen in unterschiedlichem Maße schädlich sein. Minderjährige, die ethnischen und religiösen Minderheiten angehören, Teil der LGBTIQ+-Gemeinschaft sind oder besondere pädagogische Bedürfnisse oder bereits bestehende psychische Erkrankungen haben, können besonders anfällig für Gefahren im digitalen Raum sein. Diese Anfälligkeit wird natürlich durch soziale Medien und andere digitale Dienste mit schädlichen, manipulativen oder suchterzeugenden Inhalten oder Designs noch verstärkt. Die Forschungsarbeit und die Sammlung von Erkenntnissen sollten in jedem Fall mit der Weiterentwicklung dieser Merkmale Schritt halten.

Minderjährige sind durch die sozialen Medien und andere digitale Dienste weitreichenden Risiken für ihre körperliche und psychische Gesundheit ausgesetzt. Was die körperliche Gesundheit betrifft, so verdrängt übermäßige Bildschirmzeit das Spielen im Freien und den Sport und kann sich auf die Gesundheit, die körperliche Leistungsfähigkeit und den Schlaf von Kindern auswirken. Die Nutzung von sozialen Medien+ und Endgeräten im frühen Kindesalter tritt an die Stelle des eigenständigen Erkundens und persönlicher sozialer Interaktionen. Auswirkungen auf die sozial-emotionale Entwicklung und die Anfälligkeit für psychische Probleme sind möglich. Werden Endgeräte über längere Zeiträume hinweg genutzt, kann dies auch zu Problemen wie Muskel-Skelett-Erkrankungen oder einer Überanstrengung der Augen durch digitale Medien führen.

Die Nutzung sozialer Medien und anderer digitaler Dienste ist für Kinder aber auch mit erheblichen Risiken für ihre psychische Gesundheit verbunden. Dabei besteht sowohl das Risiko, dass die sozialen Medien+ der psychischen Gesundheit von Kindern unmittelbar schaden, als auch die Gefahr, dass durch sie bestehende psychische Probleme wie Depressionen oder Ängste verschärft werden. Auch hier bestimmen soziale und individuelle Faktoren, wie stark Kinder und Jugendliche gefährdet sind.

Im Allgemeinen wird eine ausgeprägte Nutzung sozialer Medien und anderer digitaler Dienste durch Kinder und Jugendliche mit Schlaf- und Konzentrationsproblemen sowie mit einem erhöhten Auftreten von Depressionen und Ängsten in Verbindung gebracht. Durch suchterzeugende Gestaltungsmerkmale werden diese Effekte verstärkt, da sie das zwanghafte Nachsehen, die Angst, etwas zu verpassen ("fear of missing out"), und das vermehrte Vergleichen mit anderen fördern. Mögliche Folgen für Minderjährige sind ein vermindertes Selbstwertgefühl und erhöhter Stress. Algorithmische Verstärkung und Empfehlungssysteme können Desinformation und Hetze fördern. Besonders schädlich sind diese Effekte im Internet für schutzbedürftige Gruppen.

Es besteht ein beträchtliches Risiko, dass Minderjährige online mit kriminellen und illegalen Inhalten konfrontiert werden. Sowohl Erwachsene als auch Minderjährige nutzen gezielt soziale Medien und andere digitale Dienste, darunter auch Spieleplattformen, um mit Kindern und Jugendlichen in Kontakt zu treten. Dabei umfasst das Gefahrenpotenzial unter anderem sexuellen Kindesmissbrauch (oder Darstellungen davon), Grooming, Cybermobbing, Radikalisierung sowie die Anstiftung zu illegalen Handlungen, Gewalttaten oder Terrorismus. Aus der weitverbreiteten Nutzung von KI-Systemen ergibt sich eine ernsthafte Gefahr für Kinder und Jugendliche, da Darstellungen sexuellen Kindesmissbrauchs künstlich erzeugt werden können (z. B. Deepfakes). Die hier beschriebenen Arten des Missbrauchs wirken sich verheerend auf die Entwicklung sowie die psychische und körperliche Gesundheit von Minderjährigen aus und können sie im schlimmsten Fall das Leben kosten.

In erster Linie sind die Anbieter sozialer Medien und anderer digitaler Dienste dafür verantwortlich, dass bei der Nutzung ihrer Dienste die Sicherheit Minderjähriger gewährleistet ist. Darüber hinaus ist es wichtig, dass Eltern und Betreuungspersonen im Blick behalten, wie viel Zeit Kinder und Jugendliche online verbringen, und dass sie ihnen Hilfestellung bieten, um die Risiken, denen sie in den sozialen Medien+ ausgesetzt sind, gemeinsam mit ihnen zu bewältigen. Unabhängig vom Alter ist es von entscheidender Bedeutung, für angemessene Offline-Aktivitäten und persönliche Begegnungen zu sorgen.

Trotz der zahlreichen Gefahren – **die Welt der sozialen Medien+ bietet Kindern und Jugendlichen viele Möglichkeiten.** Wenn Minderjährige in die Lage versetzt werden, sich sicher online zu bewegen, und mit soliden digitalen Kompetenzen ausgestattet sind, kann die Nutzung sozialer Medien und anderer digitaler Dienste dem Wohlbefinden und der sozialen Vernetzung zugutekommen, einen unterstützenden Kontakt zu Gruppen von Gleichaltrigen ermöglichen und Chancen für Selbstentfaltung, gesellschaftliches Engagement und unabhängiges Lernen bieten. Es hat sich gezeigt, dass gezielte Initiativen für digitale Kompetenzen – wie die EU-Strategie „Besseres Internet für Kinder“, die Safer-Internet-Zentren sowie auf nationaler Ebene die Verankerung von Medienkompetenz in den Lehrplänen für die allgemeine und berufliche Bildung – kritisches Denken fördern, die Widerstandsfähigkeit gegenüber Desinformation erhöhen und Minderjährige in die Lage versetzen können, sich sicher im Internet zu bewegen.

Soziale Medien und andere digitale Dienste, die „safe by design“ sind, könnten die Position von Kindern und Jugendlichen im Internet stärken und ihnen mehr Teilhabe ermöglichen, indem sie den Erwerb von digitalen Kompetenzen und Medienkompetenz fördern. Durch eine altersgerechte digitale Bildung in den Schulen und mit der Unterstützung von Eltern und Betreuungspersonen könnten Minderjährige außerdem dazu befähigt werden, die Chancen der Online-Welt zu nutzen und mögliche Risiken und Gefahren zu bewältigen.

Altersspezifische Risiken müssen adressiert werden

Je älter und unabhängiger Kinder werden, desto weniger können Eltern sie bei ihren Online-Aktivitäten beaufsichtigen. Der Einfluss Gleichaltriger spielt eine immer wichtigere Rolle. Jugendliche können sich, je näher sie der Volljährigkeit kommen, zunehmend eigenständig online bewegen und die Risiken, denen sie dort ausgesetzt sind, besser verstehen und bewältigen. Es steht außer Frage, dass sich die Bedürfnisse eines 3-Jährigen von denen eines 16-Jährigen unterscheiden. Daher ist es wichtig, **in Bezug auf die Online-Sicherheit von Kindern einen entwicklungssensiblen Ansatz zu verfolgen, der sich im vorliegenden Bericht in der Unterscheidung verschiedener Altersgruppen** niederschlägt:

Kinder **unter 3 Jahren** sind durch passive Internetnutzung vor allem Risiken mit Blick auf den Beziehungsaufbau und „Technoferenz“^f ausgesetzt. Diese Risiken entstehen in erster Linie, wenn Betreuungspersonen versuchen, kleine Kinder mithilfe von Bildschirmen zu „beruhigen“ oder abzulenken, anstatt sich direkt mit ihnen zu beschäftigen. Dies kann sich auf die Aufmerksamkeitsspanne, den Spracherwerb und die sozial-emotionale Entwicklung von Kindern auswirken.

Kinder **zwischen 3 und 5 Jahren** sind im Rahmen einer zunehmend unabhängigen Nutzung unter Aufsicht zunehmend den Risiken in der digitalen Welt und einer längeren Bildschirmnutzung ausgesetzt. Soziale Medien und andere digitale Dienste sind mit ihrer Auslegung auf sofortige und wiederkehrende Belohnung sowie kontinuierliche externe Stimulation dem Entwicklungsstand von Kindern grundsätzlich nicht angemessen und können deren langfristige Entwicklung beeinträchtigen.

Kinder **zwischen 6 und 9 Jahren** nutzen soziale Medien und andere digitale Dienste in stark zunehmendem Umfang. Die Bewertung von außen in der Online-Welt (z. B. Likes, Punktzahlen und Bestenlisten) vermischt sich mit dem entstehenden Selbstwertgefühl, das auf der Entwicklung von Fähigkeiten in der realen Welt beruht. Dadurch können leistungsbezogene Ängste sowie der Vergleich mit Gleichaltrigen verstärkt und die Anfälligkeit für Cybermobbing, Hetze und Belästigung durch Gleichaltrige erhöht werden.

^f Die Unterbrechung der Interaktionen zwischen Eltern und Kindern durch Technologie.

Für Kinder **zwischen 10 und 12 Jahren** ist der Zugang zu sozialen Medien+ eine zentrale Voraussetzung für die Teilnahme am Sozialleben. In diesem Alter sind Kinder am stärksten dem Zusammenspiel von entwicklungsbedingten Anfälligkeiten und plattformgesteuerter Verstärkung ausgesetzt. Algorithmische Empfehlungssysteme fördern den sozialen Vergleich sowie die Konfrontation mit gefährlichen oder illegalen Inhalten (einschließlich Darstellungen sexuellen Kindesmissbrauchs, extremistischer Propaganda und Desinformation) und mit suchterzeugenden Gestaltungsmustern, die das Auftreten von Depressionen und Ängsten begünstigen. Jüngste prospektive Untersuchungen deuten darauf hin, dass bei Kindern, die mit 12 Jahren (statt mit 13) ihr erstes Smartphone bekommen, nach einem Jahr ein erhöhtes Risiko für Depressionen und andere psychische Probleme bestehen könnte^g. Anhand dieses Beispiels zeigt sich, dass Kinder unter 13 Jahren im Allgemeinen besonders schutzbedürftig sind.

Bei Jugendlichen **zwischen 13 und 15 Jahren** findet mit Blick auf soziale Medien und andere digitale Dienste ein Übergang von einer Nutzung unter Aufsicht zu einer zunehmend eigenständigen Nutzung statt. In diesem Alter nimmt die Wirksamkeit herkömmlicher Aufsicht durch Betreuungspersonen und Schulpersonal ab. Die Risiken ergeben sich zunehmend aus den Strukturen der sozialen Medien und anderen digitalen Dienste und nicht mehr nur aus dem individuellen Verhalten. Eine zentrale Herausforderung besteht im Umgang mit algorithmischen Systemen, die angezeigte Inhalte vorgeben und das Verhalten beeinflussen, gleichzeitig aber nur begrenzt transparent sind.

Eine zunehmende Eigenständigkeit gehört heutzutage nicht nur offline, sondern auch in der Online-Welt zum Aufwachsen dazu. Es geht also nicht darum, Jugendliche in ihrem Übergang zur Eigenständigkeit zurückzuhalten, sondern vielmehr dafür zu sorgen, dass sie in einer mit großer Verwundbarkeit einhergehenden Entwicklungsphase weniger Gefahren ausgesetzt sind. Ein wirksamer Schutz erfordert einen entwicklungsorientierten, vielschichtigen Ansatz, bei dem die Regulierung sozialer Medien und anderer digitaler Dienste, Bildungsmaßnahmen sowie Unterstützung zur Selbstregulierung und kritischen Mediennutzung ineinandergreifen.

Jugendliche **zwischen 16 und 18 Jahren** befinden sich in einer Phase, in der sich ihre Identität zunehmend festigt und ihre Eigenständigkeit zunimmt. Ihre Fähigkeiten entwickeln sich weiter, sodass sie die Risiken, denen sie im Internet ausgesetzt sind, besser verstehen und bewältigen können. Ihre neurobiologische Entwicklung ist jedoch bei Weitem noch nicht abgeschlossen, und die Nutzung sozialer Medien und anderer digitaler Dienste geht mit einem erhöhten Risiko für Sucht, Ängste und psychische Probleme einher. In diesem Alter müssen Jugendliche Kompetenzen (z. B. kritisches Denken und Bewerten) erwerben, die sie benötigen, um sich erfolgreich und sicher in der digitalen Welt zu bewegen und die sich dort bietenden Möglichkeiten voll auszuschöpfen.

g. [Children's Hospital of Philadelphia, „Age Limits Alone Won't Fix Smartphone Risks, Suggests Children's Hospital of Philadelphia Study“, 2026, abgerufen am 12. Juli 2026.](#)

Sechs Leitprinzipien für den Schutz und die Stärkung Minderjähriger online

Da die sozialen Medien+ für Kinder und Jugendliche sowohl Risiken als auch Chancen bergen können, bedarf es eines umfassenden politischen Rahmens, durch den Minderjährige online geschützt und gestärkt werden. Die folgenden **sechs von den Ko-Vorsitzenden ausgearbeiteten Leitprinzipien dienen als Richtschnur für die Arbeit des Sonderausschusses** und bilden das Gerüst für den vorliegenden Bericht. Als Grundlage für Maßnahmen sollten eine solide Datenlage und Analyse in Bezug auf die Herausforderungen und Chancen für Kinder in der digitalen Welt dienen. Damit die Maßnahmen Wirkung zeigen, müssen sie effektiv umgesetzt und evaluiert werden.

LEITPRINZIP 1

Entwicklungsorientierter Ansatz (siehe Kapitel 1)

Regulierung muss altersgerecht sein und Orientierungshilfen müssen differenziert sein. Da die Entwicklung von Kindern und Jugendlichen in Phasen verläuft, sollten Schutzmaßnahmen so gestaltet und umgesetzt werden, dass sie den für die jeweiligen Altersgruppen relevanten Risiken Rechnung tragen. Nach Möglichkeit sollte bei diesen Maßnahmen der persönliche und soziale Hintergrund der Kinder berücksichtigt werden, der sich verstärkend auf die Risikoanfälligkeit auswirken kann.

LEITPRINZIP 2

Gleichstellung und Diversität (siehe Kapitel 2)

Ungleichheiten zwischen Altersgruppen und sozioökonomischen Gruppen mit Blick auf die Risiken und die Anfälligkeit für Gefahren im Internet sollten anerkannt werden. Geschlecht, Sexualität, ethnischer und religiöser Hintergrund, sonderpädagogischer Förderbedarf und bereits bestehende psychische Probleme sind ausschlaggebend dafür, wie anfällig Minderjährige für Online-Gefahren sind. Diese Faktoren beeinflussen auch, welche Ressourcen und Kapazitäten Eltern und Betreuungspersonen zur Verfügung stehen, um Kinder und Jugendliche auf ihrem Weg zur Eigenständigkeit zu unterstützen.

LEITPRINZIP 3

Schutz Minderjähriger (siehe Kapitel 3)

Kinder und Jugendliche müssen die Vorteile sicherer sozialer Medien+ nutzen können. Der Schutz Minderjähriger vor schädlichen Inhalten, suchterzeugenden Funktionen, digitaler Vernachlässigung^h und Internetkriminalität (z. B. sexuellem Missbrauch) sollte in die Gestaltung sozialer Medien und anderer digitaler Dienste einfließen. Schädliche Inhalte oder Funktionen sollten für Minderjährige leicht zu melden sein. Die Anbieter sollten solche Meldungen vorrangig behandeln und schädliche Inhalte oder Funktionen unverzüglich entfernen.

h. Das wiederholte Versäumnis einer Betreuungsperson, ein dem Entwicklungsstand angemessenes Maß an Aufmerksamkeit, Zugewandtheit, Aufsicht oder Schutz zu bieten, da wesentliche Betreuungsaufgaben durch digitale Technologien gestört, ersetzt oder beeinträchtigt werden.

LEITPRINZIP 4**Rechenschaftspflicht digitaler Dienste und Verbraucherrechte (siehe Kapitel 3)**

Die Anbieter sozialer Medien und anderer digitaler Dienste müssen die Hauptverantwortung dafür tragen, dass der Zugang zu Online-Räumen und deren Nutzung für Minderjährige sicher sind. Digitale Dienste sollten dazu angelegt werden, Maßnahmen für „safety by design“ umzusetzen, und eine inhaltsbezogene Regulierung sollte schnell durchgesetzt werden. Die Beweislast muss auf den Anbietern sozialer Medien und anderer digitaler Dienste liegen, nachzuweisen, dass die Funktionen ihrer Dienste nicht schädlich sind, bevor sie Zugang zu Kindern und Jugendlichen erhalten.

LEITPRINZIP 5**Stärkung und Vermittlung von Medienkompetenz (siehe Kapitel 4)**

Eltern und Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte sollten in die Lage versetzt werden, Kinder und Jugendliche bei ihrem schrittweisen Übergang zu einer sicheren und eigenständigen Online-Nutzung zu unterstützen. Es sollten ausreichend Möglichkeiten (z. B. Schulungen zur digitalen Kompetenz und Medienkompetenz) und eine angemessene Infrastruktur geschaffen werden, um Eltern dazu zu befähigen, über ihr eigenes Handeln nachzudenken und Minderjährige bei ihren Online-Aktivitäten anzuleiten. Die entsprechenden Maßnahmen müssen auf die Rollen der Betreuungspersonen und pädagogischen Fachkräfte zugeschnitten sein, die sich mit zunehmendem Alter der Kinder und Jugendlichen verändern.

LEITPRINZIP 6**Rechte und Teilhabe von Kindern (siehe Kapitel 4)**

Das Recht von Kindern auf sichere Teilhabe, Interaktion und gemeinsame Gestaltung sollte online wie offline geschützt werden. Die in den einschlägigen internationalen Rahmenwerkenⁱ verankerten Rechte von Kindern sollten stets als Grundlage für Kinderschutzmaßnahmen dienen. Altersbezogene Zugangsbeschränkungen müssen die Rechte des Kindes online achten und verhältnismäßig, zeitlich begrenzt sowie auf das Wohl des Kindes abgestimmt sein. Dies unterstreicht die Notwendigkeit, Offline-Aktivitäten für Minderjährige aller Altersgruppen finanziell zu fördern und zu bewerben.

Sonderberater/Sonderberaterin der Präsidentin und Ko-Vorsitzende des Sonderausschusses für die Online-Sicherheit von Kindern



Prof. Dr. Jörg M. Fegert

Ärztlicher Direktor der Klinik für
Kinder- und Jugendpsychiatrie,
Psychosomatik und Psychotherapie
am Universitätsklinikum Ulm



Dr. Maria Melchior

Forschungsdirektorin am
französischen Institut für
Gesundheit und medizinische
Forschung (INSERM)

- i. Insbesondere das Übereinkommen der Vereinten Nationen über die Rechte des Kindes und die Allgemeinen Bemerkungen des Ausschusses für die Rechte des Kindes, die Charta der Grundrechte der Europäischen Union und die EU-Kinderrechtsstrategie.

SECHS LEITPRINZIPIEN für den Schutz und die Stärkung Minderjähriger online

ONLINE - SICHERHEIT VON KINDERN

ANALYSE DER SITUATION

ENTWICKLUNGSORIENTIERTER ANSATZ

altersgerechte Regulierung und differenzierte Leitlinien
sicherstellen

GLEICHSTELLUNG UND DIVERSITÄT

Ungleichheiten zwischen verschiedenen Gruppen mit Blick auf Risiken,
Anfälligkeit und digitale Gefahren anerkennen

SCHUTZ MINDERJÄHRIGER

vor schädlichen Inhalten, suchterzeugenden Gestaltungsmerkmalen, digitaler
Vernachlässigung und Kriminalität (z. B. sexuellem Missbrauch, Mobbing) schützen

RECHENSCHAFTSPFLICHT DIGITALER DIENSTE UND VERBRAUCHERRECHTE

inhärente Sicherheit und inhaltsbezogene Regulierung durchsetzen

STÄRKUNG UND VERMITTLUNG VON MEDIENKOMPETENZ

Eltern und Betreuungspersonen in die Lage versetzen, die digitalen Kompetenzen
und die Medienkompetenz von Kindern und Jugendlichen im Sinne einer
verantwortungsvollen Nutzung zu fördern

RECHTE VON KINDERN UND TEILHABE

das Recht auf sichere Teilhabe und gemeinsame Gestaltung
online schützen

MAßNAHMEN

EVALUIERUNG

Zentrale Empfehlungen zum Schutz und zur Stärkung Minderjähriger online

Das übergeordnete Ziel der in diesem Bericht enthaltenen Empfehlungen, die auf einem entwicklungssensiblen Ansatz und den sechs Leitprinzipien beruhen, besteht darin, sowohl die Notwendigkeit, Kinder und Jugendliche online zu schützen, als auch ihr Recht auf Teilhabe in den sozialen Medien+ und auf Nutzung der sich dort bietenden Chancen in ausgewogener Weise zu berücksichtigen.

Empfehlungen zur altersgerechten Nutzung sozialer Medien und anderer digitaler Dienste

0 BIS 2 JAHRE

Bildschirme und soziale Medien+ vermeiden

Längere Bildschirmnutzung in der frühen Kindheit zu vermeiden, bedeutet kein vollständiges Verbot. Vielmehr bedeutet es, die entwicklungsbedingten Bedürfnisse von Kindern in Bezug auf Bindung, Entwicklung der Sinne und frühkindlichen Spracherwerb zu respektieren. Eltern und Betreuungspersonen sollten vor allem auf persönliche Interaktion setzen und ihre eigene Nutzung digitaler Endgeräte im Auge behalten, um eine Vorbildfunktion zu übernehmen und „Technoferenz“ zu vermeiden. Dieser Ansatz steht im Einklang mit den Empfehlungen der Weltgesundheitsorganisation zur Vermeidung von Störungen der neurobiologischen und kognitiven Entwicklung und der Bildung emotionaler Bindungen sowie körperlicher Probleme (z. B. Beeinträchtigungen des Sehvermögens) bei Kindern.

3 BIS 12 JAHRE

Nutzung altersgerechter sozialer Medien+ und von Endgeräten unter Aufsicht

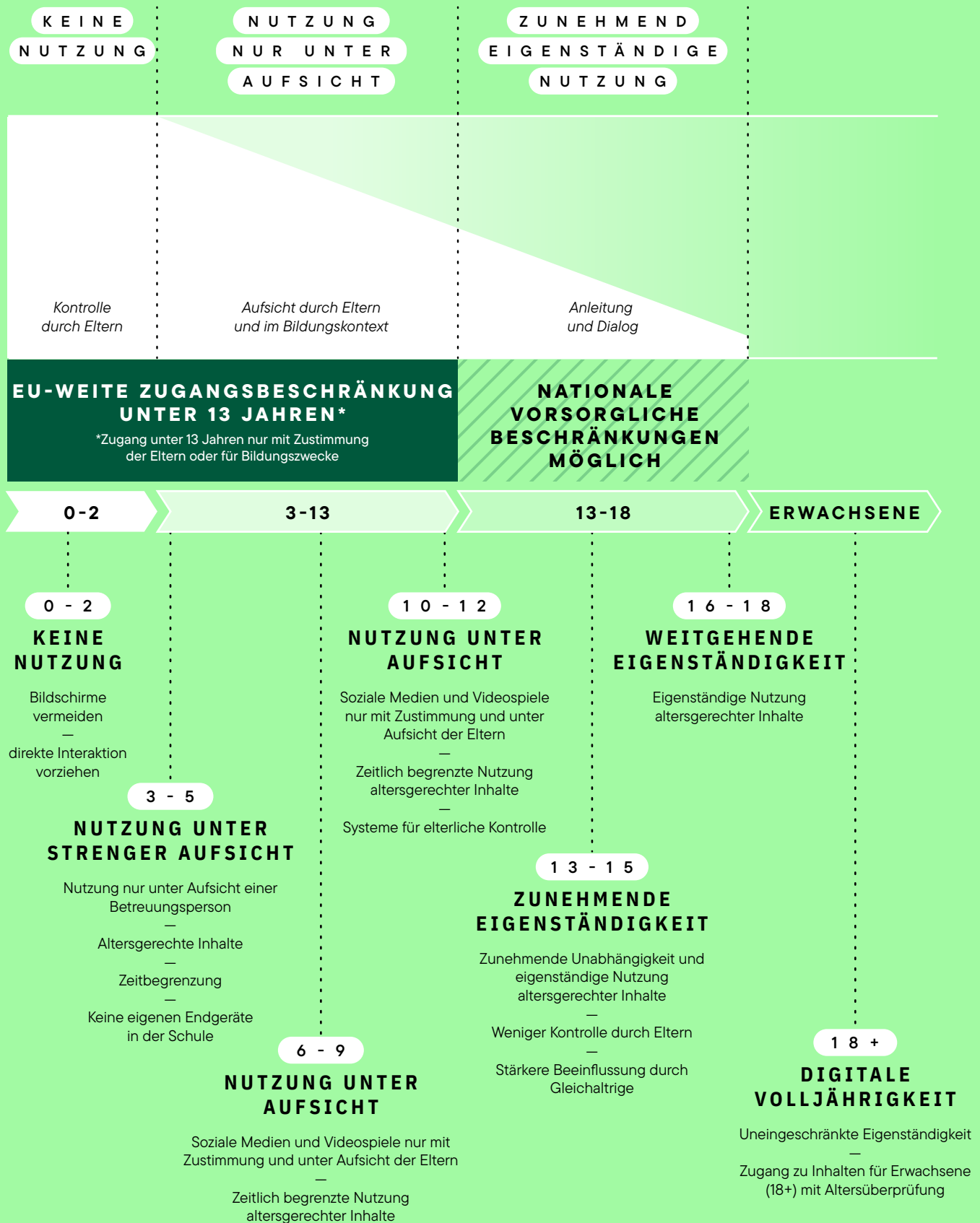
Kindern sollte nicht erlaubt werden, internetfähige Endgeräte unbeaufsichtigt zu nutzen. Schulen sollten die Gegebenheiten für eine beaufsichtigte und begrenzte Nutzung von internetfähigen Endgeräten für Bildungszwecke schaffen und digitale Kompetenzen, Medienkompetenz, emotionale Resilienz und die kritische Auseinandersetzung mit den Risiken fördern. Eltern und Betreuungspersonen sollten Kinder beaufsichtigen und ihre digitale Autonomie schrittweise mit altersgerechten sozialen Medien und anderen digitalen Diensten unterstützen. Sie sollten außerdem regelmäßig mit Kindern über die Chancen und Risiken sprechen, die sich für Minderjährige aus der Online-Nutzung ergeben. Betreuungspersonen und pädagogische Fachkräfte sollten Kinder in diesem Alter weiter dazu ermuntern, sich an Offline-Aktivitäten zu beteiligen.

13 BIS 18 JAHRE

Zunehmend eigenständige Nutzung altersgerechter sozialer Medien+

Im Alter von 13 bis 18 Jahren sollten Jugendliche nur Zugang zu altersgerechten und auf „safety by default“ beruhenden sozialen Medien und anderen digitalen Diensten haben, bei denen zentrale Sicherheitsfunktionen aktiv umgesetzt wurden (z. B. Beschränkungen für endloses Scrollen und Empfehlungssysteme). Bis solche auf „safety by default“ beruhenden sozialen Medien und anderen digitalen Dienste zur Verfügung stehen, spielt die individuelle und altersgerechte Kontrolle und Aufsicht durch die Eltern weiterhin eine wichtige Rolle. Zusätzliche Vorsichtsmaßnahmen vonseiten der Regulierungsbehörden sind denkbar. Auch mit zunehmender digitaler Autonomie bestehen bei Jugendlichen über 16 Jahren weiterhin Risiken im Zusammenhang mit schädlichen Online-Inhalten. Daher sollten Eltern und Betreuungspersonen weiter mit ihnen über ihre Online-Erfahrungen sprechen. Jugendliche sollten beim Zugang zu Hilfsdiensten und Beschwerdesystemen Vorrang haben und außerdem von unterstützenden Netzwerken Gleichaltriger („peer support networks“) profitieren, wodurch eine verantwortungsvolle Nutzung sozialer Medien und anderer digitaler Dienste gefördert würde.

Altersgerechte Nutzung sozialer Medien+ durch Minderjährige



Empfehlungen zum Schutz von Kindern und Jugendlichen online

// Eine harmonisierte EU-weite Zugangsbeschränkung für soziale Medien und andere digitale Dienste für Kinder unter 13 Jahren vorschlagen.

Eine harmonisierte EU-weite Zugangsbeschränkung für soziale Medien und andere digitale Dienste, einschließlich KI-Gefährten, für Kinder unter 13 Jahren ist notwendig. Eine solche harmonisierte Zugangsbeschränkung würde einerseits die Umsetzung einer verhältnismäßigen, rechtskonformen Altersfeststellung erleichtern und andererseits die Festlegung von Anforderungen an die Anbieter sozialer Medien und anderer digitaler Dienste hinsichtlich „safety by design“ begünstigen. Kinder unter 13 Jahren sollten nur mit Zustimmung und unter Aufsicht der Eltern oder im Bildungskontext zeitlich begrenzten Zugang zu altersgerechten sozialen Medien+ haben. Ab dem Alter von 13 Jahren sollten Jugendliche die Vorteile einer zunehmend eigenständigen Nutzung altersgerechter und sicherer sozialer Medien und anderer digitaler Dienste genießen können.

Harmonisierte Vorschriften über ein EU-weites Mindestalter von 13 Jahren würden zum reibungslosen Funktionieren des Binnenmarkts beitragen, indem ein einheitlicher Rahmen geschaffen würde, an den sich die Anbieter halten müssten. Durchsetzung und Aufsicht würden den Regulierungsbehörden sowohl auf nationaler Ebene als auch auf EU-Ebene durch harmonisierte Vorschriften erleichtert. Außerdem würde so dafür gesorgt, dass alle Minderjährigen in der EU dasselbe Maß an Schutz genießen, unabhängig von sozioökonomischen, kulturellen und einzelstaatlichen Faktoren.

// Funktionierende Systeme zur Altersfeststellung einführen, damit auf „safety by design“ beruhende und altersgerechte Systeme zum Schutz und zur Stärkung Minderjähriger online ihre Wirkung entfalten können.

Methoden der Altersfeststellung – Altersüberprüfung und Altersschätzung – müssen verhältnismäßig sein und Mindestanforderungen unterliegen, insbesondere in Bezug auf die Grundrechte der Nutzerinnen und Nutzer, wozu auch Kinderrechte und die damit verbundenen Schutzvorkehrungen zählen. Alle zur Altersfeststellung genutzten Methoden sollten höchsten Anforderungen in Bezug auf den Schutz der Privatsphäre und den Datenschutz genügen und auf die Verarbeitung von Ausweisdokumenten oder biometrischen Daten zum Zwecke der Altersschätzung verzichten. Es sollten technische Normen wie der „Null-Wissen-Beweis“ angewandt werden, um sicherzustellen, dass sowohl die zur Altersfeststellung verpflichtete Plattform als auch der Anbieter, der die Altersüberprüfung durchführt, keine Informationen erhalten, die das Tracking oder die Identifizierung der Nutzerinnen und Nutzer erlauben.

Die Methoden zur Altersfeststellung sollten das Alter oder Altersgruppen entsprechend den Anforderungen präzise bestimmen können, und für eine einfache und zuverlässige Praxisanwendung unter realen Bedingungen geeignet sein. Die Methoden sollten robust sein, um einer Umgehung sowie Sicherheitsbedrohungen entgegenzuwirken, sie sollten inklusiv (und diskriminierungsfrei) sein und allen, die sie benötigen, gleichermaßen zur Verfügung stehen. Anbieter sozialer Medien und anderer digitaler Dienste müssen ihrer Verpflichtung nachkommen, zu verhindern, dass Minderjährige Dienste mit hohem Risikopotenzial nutzen oder mit Personen in Kontakt kommen, die sich als Kinder oder Jugendliche ausgeben.

// Vorschriften für zentrale Sicherheitsfunktionen bei der Gestaltung sozialer Medien und anderer digitaler Dienste erweitern und harmonisieren.

Eine klar definierte „safety by design“-Sicherung sowie altersgerechte Schutzvorkehrungen (z. B. potenzielle Beschränkungen für endloses Scrollen, automatische Wiedergabe, Push-Benachrichtigungen und problematische Systeme für personalisierte Empfehlungen) sollten in soziale Medien und andere digitale Dienste integriert werden. Soziale Medien und andere digitale Dienste sollten durch entsprechende integrierte Standardeinstellungen Schutz vor suchterzeugenden Gestaltungsmerkmalen, Dark Patterns, unerwünschter Kontaktaufnahme und dem Rabbit-Hole-Effekt bieten. Eine Erweiterung und Harmonisierung der Vorschriften über zentrale Sicherheitsfunktionen würde für Gewissheit und Einheitlichkeit im Bereich der sozialen Medien+ sorgen. Aufgrund der raschen technologischen Entwicklung sollten die Vorschriften über zentrale Sicherheitsfunktionen anpassbar sein, damit kontinuierlich auf neue schädliche Gestaltungsmerkmale reagiert werden kann.

// Beweislast, dass Produkte und Dienste für Minderjährige sicher sind, auf Anbieter sozialer Medien und anderer digitaler Dienste verlagern.

Spezifische Altersbeschränkungen sollten gelten, bis die Anbieter sozialer Medien und anderer digitaler Dienste zentrale Sicherheitsfunktionen zum Schutz von Kindern und Jugendlichen einführen. Nur wenn Anbieter nachweisen können, dass sie sichere und altersgerechte Funktionen eingeführt haben und somit den von der EU und den Mitgliedstaaten ergriffenen Maßnahmen entsprechen, sollten sie ihre Dienste Minderjährigen anbieten dürfen. Wenn eine „safety by default“-Version vorhanden ist, sollten nicht altersgerechte Funktionen (Funktionen für Erwachsene) nur nach einer erfolgreichen Altersfeststellung aktiviert werden können.

// Durchsetzungs- und Evaluierungskapazitäten stärken.

Angesichts der zahlreichen Vorschriften, die inzwischen in Bezug auf die Online-Sicherheit von Kindern gelten (Gesetz über digitale Dienste, DSGVO, Verordnung über Künstliche Intelligenz usw.), sollten die Aufsichtsbehörden aus unterschiedlichen Rechtsfeldern intensiver zusammenarbeiten und Informationen austauschen. So können Unstimmigkeiten vermieden und kohärente, verlässliche und wirksame rechtliche Rahmenbedingungen gewährleistet werden, deren Fundament der Schutz der Grundrechte bildet. Die Europäische Kommission sollte prüfen, durch welche Mechanismen eine nahtlose Zusammenarbeit zwischen den Aufsichtsbehörden ermöglicht werden kann, um bestehende Strukturen für die Rechtsdurchsetzung zu nutzen. Darüber hinaus muss beurteilt werden, ob die für die Durchsetzung und Evaluierung zuständigen Regulierungsbehörden zusätzliche Ressourcen oder Umstrukturierungen benötigen. Es sollten Maßnahmen in Betracht gezogen werden, durch die die Zivilgesellschaft eine wichtigere Rolle bei der Durchsetzung einnehmen und einen größeren Beitrag zur Erweiterung der Durchsetzungskapazitäten leisten kann, was auch innerhalb bestehender Strukturen erfolgen kann. Die Durchsetzungsmechanismen sollten ergänzend ineinandergreifen und Überschneidungen sollten vermieden werden.

// Rasche Maßnahmen ergreifen, um Anbietern sozialer Medien und anderer digitaler Dienste klare Verpflichtungen aufzuerlegen, sexuellen Missbrauch von Kindern im Internet, auch im Rahmen interpersoneller Kommunikation, zu verhindern, aufzudecken, zu melden und zu stoppen.

Die Lücke im Bereich der Sicherheit von Kindern, die sich infolge des Auslaufens der Übergangsverordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern aufgetan hat, muss rasch geschlossen werden. Der EU-Gesetzgeber sollte die vorgeschlagene langfristige Verordnung für die Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern rasch beschließen. Mehr als 80 % der Ermittlungen im Zusammenhang mit sexuellem Missbrauch von Kindern gehen auf Meldungen von Anbietern sozialer Medien und anderer digitaler Dienste zurück. Kinder haben oft zu große Angst, um Missbrauch zu melden. Die Aufdeckung von Material über sexuellen Missbrauch von Kindern, einschließlich im Rahmen interpersoneller Kommunikation ausgetauschten Materials, ist häufig die einzige Möglichkeit, den Missbrauch zu stoppen.

// Mitgliedstaaten können zusätzliche vorsorgliche Zugangsbeschränkungen für soziale Medien und andere digitale Dienste für Kinder ab 13 Jahren einführen.

Zusätzliche vorsorgliche Zugangsbeschränkungen sollten als Ergänzung zu der EU-weit gültigen Zugangsbeschränkung für soziale Medien und andere digitale Dienste für unter 13-Jährige dienen. Jugendliche dürfen nur Zugang zu sozialen Medien+ haben, die in Bezug auf Inhalte und Gestaltung sicher und altersgerecht sind und bei deren Gestaltung ihre Rechte und Bedürfnisse berücksichtigt wurden. Die Situation hat sich in den Mitgliedstaaten von Land zu Land unterschiedlich entwickelt, und manche Mitgliedstaaten ziehen vielleicht eine Altersgrenze von mehr als 13 Jahren in Betracht. Alle auf nationaler Ebene erlassenen zusätzlichen vorsorglichen Zugangsbeschränkungen sollten laufend evaluiert und gegebenenfalls neu bewertet werden, sobald soziale Medien und andere digitale Dienste für Kinder und Jugendliche „safe by default“ gemacht wurden.

// Vorschriften über den Zugang der Forschung zu Daten und über die Kontrolle stärker durchsetzen.

Mit der delegierten Verordnung über Datenzugang nach Artikel 40 des Gesetzes über digitale Dienste vom Juli 2025 wurde zugelassenen Forschenden grundsätzlich ein neuer Weg eröffnet, Zugang zu Daten von Online-Plattformen zu erhalten. Diese Daten können für Forschungsarbeiten verwendet werden, die dabei helfen werden, systemimmanente Risiken zu erkennen, festzustellen und zu verstehen sowie Risikominderungsmaßnahmen zur Förderung der Sicherheit von Kindern online zu bewerten.

Ob die verfolgten Ziele erreicht werden, hängt davon ab, ob die Vorschriften von den Anbietern sozialer Medien und anderer digitaler Dienste eingehalten und von den Regulierungsbehörden wirksam durchgesetzt werden. Der Erfolg ist auch von der Bandbreite der abgedeckten Dienste und von der Qualität und der Kontinuität der zur Verfügung gestellten Daten abhängig. Die Kommission sollte die praktische Wirksamkeit des Artikels 40 über Datenzugang und Kontrolle unter Berücksichtigung der ersten Erfahrungen von Forschenden mit der delegierten Verordnung prüfen. Nur so kann sichergestellt werden, dass Online-Plattformen Anträgen auf Datenzugang aus Compliance-Gründen, für Risikobewertungen und zu Forschungszwecken nachkommen.

Die Verpflichtungen zur Datenauskunft sind nicht nur ein zentraler Bestandteil der Transparenzvorschriften nach dem Gesetz über digitale Dienste, sondern fallen auch unter die umfassendere Verantwortung der Anbieter sozialer Medien und anderer digitaler Dienste für Risikominderung. Angesichts der Risiken, die kleinere Plattformen für Minderjährige darstellen, und der Rolle einer unabhängigen Kontrolle bei der Bewältigung dieser Risiken sollten auch diese Plattformen ermutigt werden, der Forschung Zugang zu Daten zu gewähren. Bei der Umsetzung von Artikel 40 sollten standardmäßig die FAIR-Prinzipien^j für das Forschungsdatenmanagement angewandt werden.

Empfehlungen zur Stärkung von Kindern und Jugendlichen online

// Minderjährigen mehr Möglichkeiten bieten, die Welt der sozialen Medien+ in einem geschützten Rahmen aktiv mitzugestalten.

Kinder und Jugendliche sollten die Möglichkeit erhalten, Rechtsvorschriften, Strategien und Bildungsinitiativen zur Förderung der Sicherheit und Stärkung von Kindern im Internet aktiv und wirksam mitzugestalten. Dementsprechend sollten mehr Maßnahmen für die Beteiligung von Kindern und Jugendlichen an einschlägigen Vorhaben ergriffen werden. So sollten Kinder beispielsweise bei der Gestaltung von Sicherheitsstrategien, Lernprogrammen, Evaluierungen und Leitfäden einbezogen werden. Die Auswirkungen dieser Maßnahmen auf die Sicherheit und die Rechte von Kindern sollten kontinuierlich beobachtet und evaluiert werden.

Bei Verfahren zur Beteiligung von Kindern sollte sichergestellt werden, dass die Kinder klare Informationen erhalten, dass sie verstehen, wie ihre Beiträge weiterverwendet werden, und dass sie über die weiteren Entwicklungen am Laufenden gehalten werden. Insbesondere sollten auch Kinder aus benachteiligten, marginalisierten und schutzbedürftigen Gruppen einbezogen werden. Für alle Aktivitäten, an denen Kinder beteiligt sind, müssen geeignete Schutzmaßnahmen vorgesehen werden.

// Beschwerdemechanismen und Verbraucherrechte von Kindern und Jugendlichen ausweiten.

Meldungen und Beschwerden von Kindern und Jugendlichen sollten bei der Moderation von Inhalten durch Anbieter sozialer Medien und anderer digitaler Dienste vorrangig behandelt werden. Die Anbieter müssen intensiver

j. Die FAIR-Prinzipien für das Forschungsdatenmanagement wurden erstmals 2016 in einem Artikel in der Zeitschrift *Scientific Data* vorgestellt. Ziel ist es, die Infrastruktur für die Nachnutzung von Forschungsdaten zu verbessern, indem Maschinen und Menschen das Auffinden und Nutzen von Daten erleichtert wird. Siehe: Wilkinson, M.D., et al., [The FAIR Guiding Principles for scientific data management and stewardship](#), *Scientific Data*, 3, 2016.

in die Pflicht genommen werden, damit für Beratungs- und Hilfsangebote und Beschwerdemechanismen ausreichende Mittel zur Verfügung stehen. Diese Mechanismen müssen altersgerecht, benutzerfreundlich, zugänglich und wirksam sein und die Privatsphäre wahren.

// Programme für digitale Bildung und zur Förderung digitaler Kompetenzen für Minderjährige, Eltern und Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte etablieren.

Digitale Bildung und digitale Kompetenz sollten auf allen Bildungsebenen als zentrale Grundfertigkeit für Minderjährige, Eltern und Lehrkräfte verankert werden. Wohlbefinden im digitalen Raum sollte Teil der digitalen Bildung für alle sein.

Bildung sollte Kinder und Jugendliche in die Lage versetzen, Informationen und Quellen online kritisch zu bewerten und Manipulationstechniken wie z. B. Desinformation, Deepfakes und personalisierte Werbung zu erkennen. Außerdem sollten Minderjährige, Eltern und Lehrkräfte darüber aufgeklärt werden, wie digitale Inhalte erstellt und geteilt werden und wie Algorithmen das Wahrnehmen und Erleben in der Welt der sozialen Medien+ beeinflussen.

Durch strukturierte Bildungsangebote für Sicherheit im Internet sollten praktische Kompetenzen in Bezug auf den Schutz personenbezogener Daten, die Verwaltung von Datenschutzeinstellungen, die Wahrung sicherer digitaler Identitäten und die Ermittlung von Risiken insbesondere in sozialen Medien, bei Nachrichtenübermittlungsdiensten und in Spielumgebungen aufgebaut werden. Diese Kompetenzen sollten laufend ausgebaut werden, ausgehend von einfachen Verhaltensweisen für mehr Sicherheit hin zu einem Verstehen komplexerer Konzepte wie digitaler Fußabdruck, Einwilligungserklärungen und Risiken auf Plattformen. Für ein gesundes Bildschirmverhalten sollten Kinder angeleitet werden, eine ausgewogene Nutzung zu erlernen, ihre Aufmerksamkeit zu regulieren und übermäßiges oder schädliches Nutzungsverhalten zu erkennen.

// Mehr Angebot und geeignete Infrastruktur für Offline-Aktivitäten schaffen.

Die Mitgliedstaaten und die lokalen Behörden sollten das Angebot an erschwinglichen Sport-, Kunst- und Kulturstätten, Jugendclubs, Bibliotheken und Gemeinschaftsräumen erhalten und erweitern und den Zugang dazu erleichtern, um Minderjährige verstärkt für gesunde Offline-Aktivitäten zu gewinnen und attraktive Alternativen zur übermäßigen Bildschirmnutzung zu schaffen. Dafür bedarf es Investitionen in sichere, inklusive und altersgerechte Räume, in denen Minderjährige miteinander in Kontakt treten, lernen, spielen und positive Beziehungen in ihrem Umfeld aufbauen können.

// Gemeinsam Leitfäden für Eltern ausarbeiten.

Gemeinsam mit Elternvereinigungen sollten sich die EU und die Mitgliedstaaten dafür einsetzen, dass Leitfäden für Eltern ausgearbeitet werden. Die Leitfäden würden Eltern und Betreuungspersonen als klare und leicht zugängliche Ratgeber dabei unterstützen, Minderjährige im sicheren, verantwortungsvollen und positiven Umgang mit den sozialen Medien+ zu begleiten. Die Leitfäden sollten praktische Hilfestellungen zu wichtigen Themen wie Sicherheit im Internet und Datenschutz, digitales Wohlbefinden, ethische und verantwortungsvolle Nutzung und Hilfsangeboten bieten.

// Ausreichende öffentliche Finanzierung und gemeinsame Standards für Organisationen der Zivilgesellschaft und Peer-Beratung sichern.

Die EU und die Mitgliedstaaten sollten sicherstellen, dass die Safer-Internet-Zentren und ähnliche Organisationen der Zivilgesellschaft auch künftig mit ausreichenden finanziellen Mitteln ausgestattet werden und dass ihre Arbeit sich nach gemeinsamen, von Fachleuten entwickelten Standards richtet. Nur so können sie weiter Sensibilisierungs-, Schulungs- und Unterstützungsdienste anbieten und ihr Angebot weiterentwickeln. Öffentliche Mittel sind von entscheidender Bedeutung, damit sie weiter unabhängig agieren können und das Angebot kohärent bleibt.

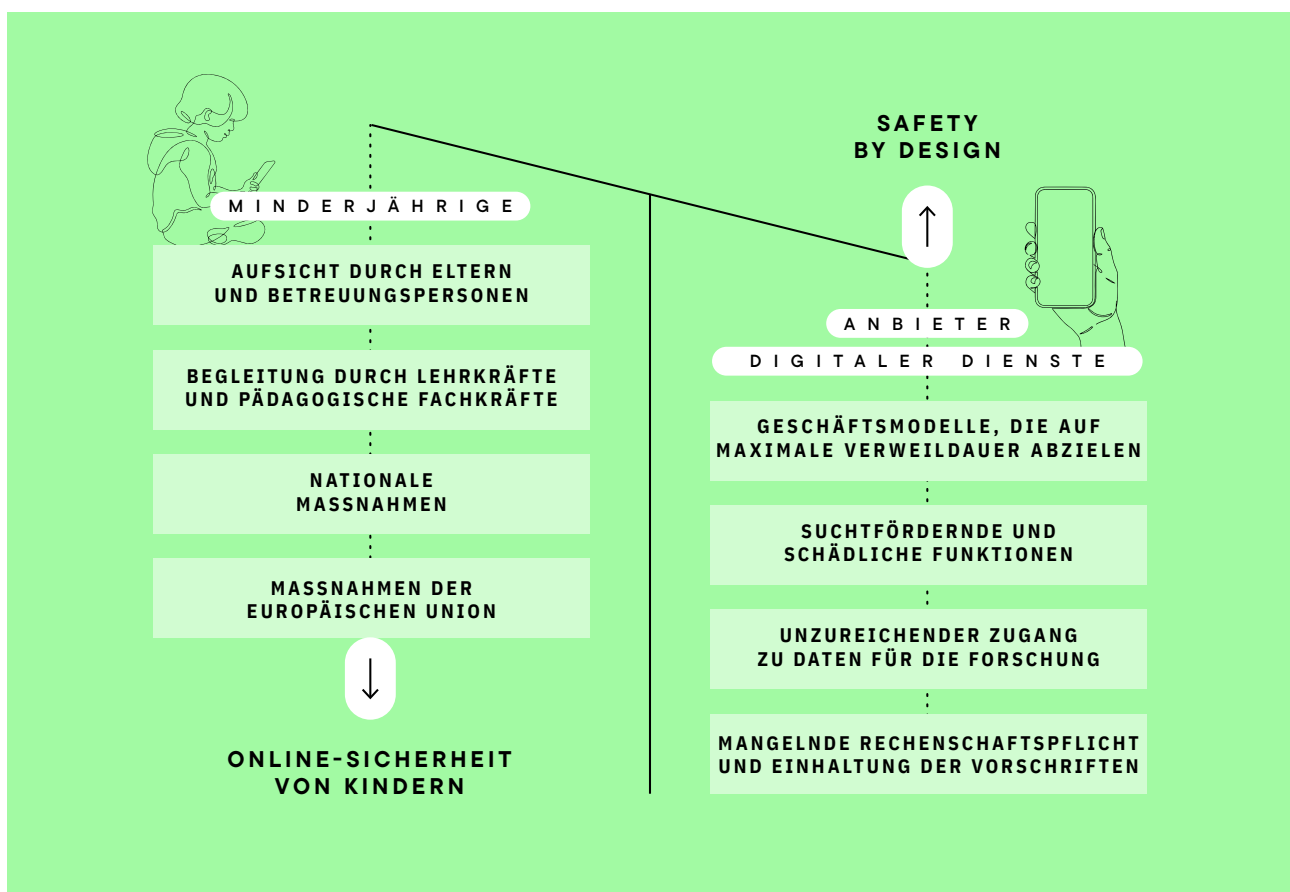
Auch Peer-Beratung, Beratungs- und Hilfsangebote, Bildungsressourcen, Sensibilisierungskampagnen und Maßnahmen für Kapazitätsaufbau sollten von der öffentlichen Hand finanziert werden. Mit weiteren Investitionen sollten die Sichtbarkeit, Zugänglichkeit und Reichweite dieser Einrichtungen – auch für schutzbedürftige Minderjährige – erhöht und Initiativen zur Förderung sichererer Umgebungen in den sozialen Medien+ unterstützt werden.

// Langfristige Finanzierung für groß angelegte europäische Langzeitstudien bereitstellen und randomisierte kontrollierte Studien weiter fördern.

Groß angelegte europäische Langzeitstudien zur Sicherheit von Kindern im Internet könnten sich beispielsweise an der nordamerikanischen Langzeitstudie zur Gehirnentwicklung und Gesundheit von Kindern (Adolescent Brain Cognitive Development (ABCD)-Studie) orientieren. Um bei Fragen der Sicherheit von Kindern im Internet einen entwicklungsorientierten und neurobiologischen Ansatz verfolgen zu können, braucht es umfassende europäische Langzeitdaten (die einen Zeitraum von zehn Jahren oder mehr abdecken). So könnten Lücken in den weitgehend korrelierenden Forschungsergebnissen im europäischen Kontext zu den Auswirkungen der Nutzung sozialer Medien und anderer digitaler Dienste auf die Entwicklung, die körperliche und psychische Gesundheit von Minderjährigen und Gefahren im Internet geschlossen werden.

Auch randomisierte kontrollierte Studien sind wichtige Werkzeuge, um die faktengesicherten Grundlagen für die evidenzbasierte Politik zu stärken. Die Forschungsförderung sollte ausdrücklich entwicklungsorientierte und psychopathologische Ansätze zur Untersuchung der Anfälligkeiten von Minderjährigen für Risiken im Internet unterstützen, wobei auch soziale und individuelle Faktoren in Kindheit und Jugend berücksichtigt werden sollten.

Abbildung 2: Das Ökosystem in die Balance bringen: „Safety by Design“ in sozialen Medien+



- k. Die ABCD-Studie ist die größte Langzeitstudie zur Gehirnentwicklung und Gesundheit von Kindern in den Vereinigten Staaten. Die Studie verfolgt die Verhaltensentwicklungen von mehr als 11 000 Kindern im Alter von 9 bis 10 Jahren von der frühen Jugend bis ins junge Erwachsenenalter. Anhand der gesammelten Daten werden grundlegende Standards für Gehirnentwicklung von Jugendlichen erarbeitet und die Auswirkungen von biologischem und sozialem Geschlecht, Schlaf, körperlicher Aktivität und Bildschirmzeit auf die Entwicklung von Jugendlichen untersucht. Die Ergebnisse werden auch ein besseres Verständnis der Entwicklung psychischer Probleme im Kindes- und Jugendalter und des Zusammenhangs mit Alkohol- und Drogenmissbrauch ermöglichen.

Sicher online

TIPPS FÜR KINDER UND JUGENDLICHE



Kenn deine Rechte – denk dran, du hast das Recht auf Sicherheit und respektvollen Umgang im Internet.



Sei nett zu anderen im Internet – soziale Medien und Spiele sollten für alle eine gute Erfahrung sein. Behandle andere so respektvoll, wie du selbst behandelt werden möchtest.



Denk nach, bevor du postest – Fotos, Videos und Kommentare können für immer im Internet bleiben. Teile jetzt nur Inhalte, bei denen du auch Jahre später kein Problem hast, wenn andere sie sehen.



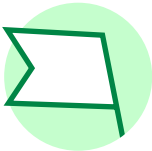
Schütze private Informationen – gib online keine privaten Informationen wie deinen vollständigen Namen, deine Wohnadresse, deine Schule, deine Telefonnummer, deine Passwörter oder deinen Live-Standort weiter.



Denk dran, dass KI ein Hilfsmittel ist und keine echte Person – KI kann Fehler machen und falsche Informationen, gefälschte Bilder, Videos, Stimmen und Nachrichten generieren.



Prüf nach, bevor du vertraust oder teilst – nicht alles im Internet ist wahr. Hinterfrage Informationen, insbesondere verwunderliche Geschichten, Videos oder Nachrichten, und vergewissere dich bei zuverlässigen Quellen, bevor du sie teilst.



Erkenne Gefahren – halte inne und denk nach, wenn du seltsame Anfragen von „Freunden von Freunden“ erhältst, Angebote, die „zu gut, um wahr zu sein“ sind, oder Nachrichten, die dich zu einer Entscheidung drängen.



Nimm keine Bilder oder Chat-Anfragen von Fremden an – wenn du nicht sicher bist, wie alt jemand ist oder wer dich kontaktiert, bitte einen Erwachsenen, zu überprüfen, wer die Person ist (oder sag der Person, „mein Vater/meine Mutter sitzt neben mir“ und schau, wie die Person reagiert).



Aktiviere Datenschutz- und Sicherheitseinstellungen – halte deine Konten privat, verwende sichere Passwörter und aktiviere nach Möglichkeit zusätzliche Sicherheitseinstellungen.



Teile keine intimen Aufnahmen – teile niemals intime Fotos oder Videos, selbst wenn dich jemand unter Druck setzt (vor allem wenn du jünger als 18 Jahre bist). Sind sie einmal geteilt, hast du keine Kontrolle mehr darüber.



Blockiere, melde und sichere Beweise – wenn du im Internet gemobbt, betrogen oder bedroht wirst oder du dich unwohl fühlst, melde und blockiere die Konten und speichere Screenshots oder Nachrichten.



Sprich mit einem Erwachsenen, dem du vertraust, wenn sich etwas falsch anfühlt – es ist nicht albern und du kommst nicht in Schwierigkeiten, wenn du um Hilfe bittest.



Hilf dabei, das Internet sicherer zu machen – lerne, wie Apps, Spiele, Websites, Algorithmen und KI funktionieren, und hilf auch anderen, auf sich aufzupassen.



Werde aktiv – engagiere dich und gestalte die Zukunft der digitalen Welt mit.



Sicher online

TIPPS FÜR ELTERN UND BETREUUNGSPERSONEN



Helfen Sie Ihrem Kind dabei, ein gesundes Bildschirmverhalten zu entwickeln – begrenzen Sie die Bildschirmzeit: gar keine Bildschirmzeit für Kinder im Alter von 0 bis 2 Jahren und altersgerechte Zeitbeschränkungen für Kinder bis ins Alter von 10 bis 12 Jahren; Nutzung unter Ihrer Aufsicht. Ob Beschränkungen der Bildschirmzeit für Jugendliche im Alter von 13 bis 18 Jahren eingeführt werden sollen, damit sie genügend Zeit haben, um zu lernen und Freunde im echten Leben zu treffen, ist noch zu erörtern.



Vergewissern Sie sich, dass Apps und Spiele altersgerecht für Ihr Kind sind.



Jüngere Kinder (bis zu 12 Jahre) sollten **Konsolen und Geräte nur nutzen, wenn eine erwachsene Person anwesend ist.**



Erlauben sie nicht, dass Geräte im Badezimmer, im Schlafzimmer oder während der Mahlzeiten genutzt werden.



Achten Sie auf den Tonfall bei Online-Gesprächen und Videospielen. Geben Sie Acht auf Warnsignale.



Verbringen Sie zusammen Zeit im Internet – bitten Sie Ihr Kind, seine Lieblingsinhalte gemeinsam anzusehen.



Kritisieren Sie nicht, womit sich Ihr Kind beschäftigt – helfen Sie Ihrem Kind, sich ein eigenes Urteil zu bilden (so bekommen Sie auch einen Eindruck davon, welche Inhalte der Algorithmus ihnen vorschlägt).



Ermutigen Sie Ihr Kind dazu, mit Ihnen zu sprechen, wenn es sich wegen etwas im Internet Sorgen macht – versichern Sie ihm, dass Sie ihm helfen werden, es nicht tadeln oder bestrafen und das Gerät nicht wegnehmen werden.



Sprechen Sie weiter über Sicherheit im Internet, wenn Ihr Kind älter wird – auch mit Kindern über 16 und über 18-Jährigen.



Teilen Sie keine Kinderfotos im Internet – Stichwort Sharenting: Denken Sie gut darüber nach, bevor Sie Fotos oder Videos von Ihren Kindern oder Teenagern online teilen. Fremde und KI können diese Informationen auf verschiedenste Arten nutzen.



Gehen Sie mit gutem Beispiel voran – kleben sie nicht an Ihrem Gerät, wenn Ihre Kinder anwesend sind. Geben Sie ihnen die Aufmerksamkeit, die sie verdienen, und verpassen Sie keine wichtigen Momente und Gespräche mit Ihrem Kind.



Liste aller Empfehlungen der Ko-Vorsitzenden nach Kapitel

KAPITEL 1

Ein entwicklungsorientierter Ansatz für die Online-Sicherheit von Kindern

- // Maßnahmen für altersgerechten Schutz von Kindern online erarbeiten und einführen
- // Sichere Online-Räume für Minderjährige gewährleisten
- // Minderjährige und ihr Umfeld stärken
- // (0 bis 2 Jahre) – Betreuungspersonen dafür sensibilisieren, wie wichtig direkte menschliche Interaktion ab der frühen Kindheit für die Entwicklung ist
- // (0 bis 2 Jahre) – Nutzung sozialer Medien und anderer digitaler Dienste vermeiden und für minimale Bildschirmnutzung sorgen, insbesondere bei Kindern unter 3 Jahren
- // (0 bis 2 Jahre) – Verbreitung von Daten von Kindern über Profile in den sozialen Medien begrenzen
- // (3 bis 12 Jahre) – Nutzung nach klaren Regeln unter Aufsicht
- // (3 bis 12 Jahre) – Kindern und ihrem Umfeld hochwertige Bildungsinhalte für den Erwerb digitaler Kompetenzen und für Wohlbefinden bereitstellen
- // (13 bis 18 Jahre) – Zunehmend eigenständige Nutzung für Jugendliche

KAPITEL 2

Forschung zu Risiken, denen Minderjährige online ausgesetzt sind

- // Evidenz-basierte Politik stärken, indem Evidenz in wenig erforschten Bereichen erarbeitet wird
- // Soziale Medien und andere digitale Dienste sollten unabhängige wissenschaftliche Fachleute aktiv in die Gestaltung von Risikominderungsstrategien und -instrumenten einbeziehen
- // Langfristige Finanzierung für groß angelegte europäische Langzeitstudien bereitstellen und randomisierte kontrollierte Studien weiter fördern
- // In eine geschützte, gemeinsame europäische Forschungsinfrastruktur investieren, um sicheren Zugang zu den Daten von Minderjährigen zu ermöglichen
- // Vorschriften über den Zugang der Forschung zu Daten und über die Kontrolle stärker durchsetzen

KAPITEL 3

Minderjährige in der sich rasch wandelnden Welt der sozialen Medien+ schützen

- // Eine harmonisierte EU-weite Zugangsbeschränkung zu sozialen Medien und anderen digitalen Diensten für Kinder unter 13 Jahren vorschlagen
- // Funktionierende Systeme zur Altersfeststellung einführen, damit auf "safety by design" beruhende und altersgerechte Systeme zum Schutz und zur Stärkung Minderjähriger online ihre Wirkung entfalten können
- // Vorschriften für zentrale Sicherheitsfunktionen bei der Gestaltung sozialer Medien und anderer digitaler Dienste erweitern und harmonisieren

- // Beweislast, dass Produkte und Dienste für Minderjährige sicher sind, auf Anbieter sozialer Medien und anderer digitaler Dienste verlagern
- // Durchsetzungs- und Evaluierungskapazitäten stärken
- // Rasche Maßnahmen ergreifen, um sicherzustellen, dass für Anbieter sozialer Medien und anderer digitaler Dienste klare Verpflichtungen gelten, sexuellen Missbrauch von Kindern im Internet, auch im Rahmen interpersoneller Kommunikation, zu verhindern, aufzudecken, zu melden und zu stoppen
- // Mitgliedstaaten können zusätzliche vorsorgliche Zugangsbeschränkungen für soziale Medien und andere digitale Dienste für Kinder ab 13 Jahren einführen
- // Verbraucherschutzvorgaben zum Schutz Minderjähriger im Internet nachschärfen
- // Auswirkungen der umgesetzten Maßnahmen laufend beobachten und bewerten
- // Bei der Verarbeitung von Daten von Kindern im Rahmen der DSGVO durch Anbieter sozialer Medien und anderer digitaler Dienste sollte das Wohl der Kinder an erster Stelle stehen
- // Wirksame Umsetzung der Produkthaftungsrichtlinie sicherstellen
- // Programme für digitale Bildung und zur Förderung digitaler Kompetenzen für Minderjährige, Eltern und Betreuungspersonen, Lehrkräfte und pädagogische Fachkräfte etablieren
- // Mehr Angebot und geeignete Infrastruktur für Offline-Aktivitäten schaffen
- // Gemeinsam Leitfäden für Eltern ausarbeiten
- // Eltern und Betreuungspersonen mit den modernsten Hilfsmitteln für Kontrolle und Aufsicht unterstützen, die laufend an den neuesten Stand der Technik angepasst werden
- // Ausreichende öffentliche Finanzierung und gemeinsame Standards für Organisationen der Zivilgesellschaft und Peer-Beratung sichern
- // Das Gesundheitssystem in die Lage versetzen, Suchterkrankungen und andere psychische Erkrankungen im Zusammenhang mit der Nutzung sozialer Medien und anderer digitaler Dienste zu diagnostizieren und zu behandeln
- // Aus- und Weiterbildung von Lehrkräften im Bereich digitaler Kompetenzen und Medienkompetenz fördern und Eltern einbeziehen
- // KI-Kompetenz als integralen Bestandteil der digitalen Bildung aufnehmen
- // Schulen sollten strukturierte Möglichkeiten zur Verbesserung der psychischen Gesundheit und des digitalen Wohlbefindens anbieten
- // Bei bildungspolitischen Maßnahmen besonderes Augenmerk auf schutzbedürftige Gruppen legen
- // In eine sichere, präventive, robuste und vertrauenswürdige digitale Bildungsinfrastruktur investieren

KAPITEL 4

Minderjährige befähigen, sich sicher in der digitalen Welt zu bewegen

- // Minderjährigen mehr Möglichkeiten bieten, die Welt der sozialen Medien+ in einem geschützten Rahmen aktiv mitzugestalten
- // Beschwerdemechanismen und Verbraucherrechte von Kindern und Jugendlichen ausweiten
- // Aufbau und Nutzung von sozialen Medien und anderen digitalen Diensten, die auf den Werten der EU aufbauen, und wo Minderjährige sicher miteinander in Kontakt treten können, finanzieren und bewerben

