

Stellungnahme zur Konsultation der Unabhängigen Expertenkommission "Kinder- und Jugendschutz in der digitalen Welt" Hearing 2 – Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste

26. Februar 2026

Meta begrüßt die Arbeit der deutschen Expertenkommission "Kinder- und Jugendschutz in der digitalen Welt". Wir bedanken uns für die Möglichkeit zur Stellungnahme.

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?

Übersicht

Die EU und insbesondere Deutschland haben mit dem Digital Services Act (DSA), dem kürzlich geänderten Jugendmedienschutz-Staatsvertrag (JMStV) sowie dem Jugendschutzgesetz (JuSchG) eine starke Grundlage für die Online-Sicherheit von Jugendlichen geschaffen. Dennoch gibt es weiteren Handlungsbedarf – insbesondere bei der Frage einer konsistenten Altersverifikation und bei der Frage, welche Rolle Eltern spielen sollten.

Unterstützung für weitere Maßnahmen im Jugendschutz

Fragmentierung und sich überschneidende Regulierungsregime oder aber zu eng gefasste regulatorische Maßnahmen, die nur für eine kleine Anzahl von Anbietern sozialer Medien gelten, bergen das Risiko, dass sich Jugendliche im Ergebnis in nicht oder wenig geschützten Bereichen des Internets bewegen. Die Erfahrung aus Australien hat gezeigt, dass die Ausgestaltung der dort eingeführten Altersbeschränkungen zu einer Abwanderung junger Menschen in weniger sicherere, unregulierte Bereiche - zu Diensten ohne robuste Schutzmaßnahmen - geführt hat.

Die Online-Aktivitäten junger Menschen umfassen ein komplexes Ökosystem aus Apps und Diensten. Der durchschnittliche Teenager nutzt mindestens 40 verschiedene Apps pro Woche, jeweils mit unterschiedlichen Altersanforderungen und Sicherheitsstandards.

Regierungen, die die Einführung von Altersbeschränkungen erwägen, sollten darauf achten, Jugendliche nicht ungewollt in weniger sichere unregulierte Bereiche zu drängen.

Erfahrungen aus Australien zeigen:

- die Abwanderung zu weniger sicheren Plattformen: Wenn Gesetze nicht klar definiert sind und der Anwendungsbereich zu eng gewählt wird, wechseln Jugendliche schnell zu ähnlichen, aber weniger bekannten und weniger regulierten Apps (z. B. Coverstar, Yope, RedNote) und Gaming-Plattformen, die vom Verbot nicht erfasst werden ([The Guardian](#)).
- den Wegfall von Unterstützungsangeboten für gefährdete Jugendliche: Der Telefonseelsorge Anbieter “Kids Helpline” berichtet von einem Anstieg an Anrufen von Jugendlichen, die den Zugang zu Online-Unterstützungsnetzwerken verloren haben; insbesondere Jugendliche in abgelegenen Regionen und marginalisierte Jugendliche sind von Isolation bedroht ([The West Australian](#)).
- Weitverbreitete Umgehung: 27 % der australischen Internetnutzer verwenden VPNs, und 75 % der Jugendlichen geben an, trotz des Verbots soziale Medien weiterhin nutzen zu wollen ([ABC](#)).

Der australische Ansatz versuchte, eine begrenzte Liste von Diensten zu regulieren. Im Ergebnis wichen Jugendliche einfach auf nicht regulierte Apps aus. Jugendliche nutzten außerdem auf einmal vermehrt algorithmisch gesteuerte Social-Media-Dienste, die auch ohne das Einloggen in ein Nutzerkonto zugänglich sind – und umgingen so die altersgerechten Schutzmechanismen für registrierte Nutzer. Daraus sollten wir lernen, dass effektiver Jugendschutz bedeutet, den Geltungsbereich von Gesetzen von Anfang an richtig zu wählen.

Altersverifikation – eine entscheidende Lücke

Obwohl die EU bereits einen umfassenden regulatorischen Rahmen für Jugend-bezogene Risiken (DSA, DSGVO und weitere Gesetze) hat, bleibt eine entscheidende Lücke - bei der Feststellung des Alters der Nutzer. Jugendliche nutzen wöchentlich Dutzende Apps mit unterschiedlichen Standards. Aktuelle Lösungen (ID-Checks, biometrische Analyse, eID) stoßen auf Herausforderungen in den Bereichen Datenschutz, Zugänglichkeit und Effektivität. Meta hat einen mehrstufigen Ansatz zur Altersverifikation entwickelt, der die Elemente Altersangabe, Meldung von Minderjährigen, Sprachanalyse-Technologie und KI-basierte Altersvorhersage kombiniert. Ergänzt wird dies durch die Verifikation via Ausweis oder Gesichtserkennung, z. B. wenn ein Nutzer sein Alter von unter 18 auf über 18 ändern

möchte. Dieser Ansatz ist robust und datenschutzfreundlich. Er minimiert zusätzliche Datenerhebungen proportional zum Risiko und erschwert Umgehung.

Die besten Ergebnisse werden erreicht, wenn die Akteure im Internet-Ökosystem zusammenarbeiten. Ein vielversprechender Ansatz ist die Altersverifikation über Betriebssysteme oder App-Stores. Diese Lösung ist datenschutzfreundlich, genießt elterliche Unterstützung und setzt auf bereits bestehende Freigabe Systeme. Mehrere US-Bundesstaaten sowie Brasilien haben bereits diese Lösung eingeführt.¹ Der neue Jugendmedienschutz-Staatsvertrag in Deutschland etabliert ebenfalls Jugendschutz auf Ebene der Anbieter der Betriebssysteme.

Das Betriebssystem oder der App-Store würden als erste Verteidigungslinie im gesamten Dienste-Ökosystem dienen, da Nutzer dort zunächst interagieren und Altersinformationen bereits erfasst werden. Das Betriebssystem oder der App-Store könnte dieses Signal dann mit Diensten wie etwa Instagram teilen. Dienste wie etwa Instagram würden weiterhin eine Rolle bei der Altersprüfung spielen, indem die Altersangabe mit eigenen Alters-Signalen verglichen werden: wenn wir Hinweise auf eine fehlerhafte Altersangabe finden, würden wir diese an das Betriebssystem/App-Store zurückspiegeln, um das System zu verbessern und einen positiven Feedback-Kreislauf zu schaffen.

Die zentrale Altersverifizierung und die anschließende Verpflichtung von Diensten wie Instagram und Facebook zur zusätzlichen Absicherung über Altersschätzungen ermöglichen einen verhältnismäßigen Ansatz bei der Altersverifikation (bei dem sensiblere Daten nur bei Bedarf erhoben werden) und führen insgesamt zu einem sicheren Online-Umfeld mit weniger Möglichkeiten zur Umgehung.

Ein weiterer Vorteil eines zentralen Systems ist, dass verhindert wird, dass ein Jugendlicher auf einem Dienst als 18 gilt (mit schwachen Standards), während er auf einem anderen als 14 verifiziert ist.

Wir sind außerdem überzeugt, dass dieser Ansatz gut mit der eID funktionieren kann – und die Effektivität eines Systems verbessert, indem jede App das Alter der Nutzer selbst per eID verifizieren muss. Die eID kann ein wertvolles Instrument sein, um das Alter zunächst zentral auf Betriebssystem- oder App-Store-Ebene zu überprüfen – für alle Apps und Dienste auf dem Gerät in einem Schritt. So werden die Datenschutzvorteile der eID mit der Effektivität einer zentralen Verifikation kombiniert.

Für Nutzerinnen ohne Zugang zum eID-System könnten andere verfügbare Maßnahmen zur Altersverifikation eingesetzt werden, wobei dennoch sichergestellt wird, dass alle Apps das gleiche, von der vertrauenswürdigen Quelle (Betriebssystem/App-Store) bereitgestellte, verifizierte Signal nutzen.

¹ Baker McKenzie, (17 September 2025). *Digital ECA (Brazil's Child and Adolescent Statute) - A new framework for online protection of children and adolescents*
https://insightplus.bakermckenzie.com/bm/data-technology/brazil-digital-eca-brazils-child-and-adolescent-statute-a-new-framework-for-online-protection-of-children-and-adolescents_2 (Accessed: 20 Jan 2026).

Meta arbeitet aktiv mit der EU und den Mitgliedstaaten zusammen, um technische Lösungen zu entwickeln, damit die eID als gültige Methode zur Altersverifikation im Rahmen des eIDAS-Systems eingeführt werden kann.

Deshalb unterstützt Meta Deutschlands Vorstoß für eine robuste, universelle Altersverifikation. Wir befürworten Lösungen, die einfach zu nutzen sind, Grundrechte schützen und für alle regulierten Dienste gelten. Verbesserte Altersverifikation ist die Grundlage, um altersgerechte Erlebnisse bei Inhalt, Kontakt und Nutzungsdauer zu ermöglichen.

Metas Ansatz für Jugendschutz

Meta investiert seit über einem Jahrzehnt erheblich in die Online-Sicherheit von Jugendlichen. 2024 haben wir “Teen Accounts” auf Instagram eingeführt, bevor sie 2025 auf Facebook und Messenger ausgeweitet wurden. Altersverifikation ist die Grundlage, um altersgerechte Erlebnisse zu bieten. Ein sicheres Umfeld für Minderjährige ist die oberste Priorität für Meta.

Instagram Teen Accounts ist ein spezielles Angebot für Nutzer von 13 bis 17 Jahren, entwickelt in Zusammenarbeit mit Eltern, Expertinnen und Jugendlichen. Diese Konten bieten integrierte Schutzmaßnahmen, die per default gelten: automatisch hohe Privatsphäre-Standards, eingeschränkte Kontaktmöglichkeiten, Filter für sensible Inhalte und Zeitmanagement-Features sowie den Ruhemodus. In Europa wird Jugendlichen keine Werbung angezeigt. Eltern müssen nichts tun, die Schutzmaßnahmen gelten automatisch. Unser Ziel ist es, Jugendlichen eine sichere, altersgerechte Umgebung zu bieten und Eltern durch Tools wie Family Center und elterliche Aufsicht zu ermöglichen, ihre jugendlichen Kinder bei der Nutzung unserer Dienste zu begleiten und zu unterstützen. Jugendliche unter 16 benötigen die Zustimmung eines Elternteils, wenn sie die Einstellungen weniger restriktiv gestalten möchten. Jugendliche von 16 bis 17 können dies selbst ändern, sofern ihr Konto nicht von einem Elternteil überwacht wird.

Hundert Millionen Jugendliche weltweit nutzen inzwischen Teen Accounts. Die überwiegende Mehrheit (97 % der 13- bis 15-Jährigen) lässt die voreingestellten, besonders schützenden Einstellungen unverändert. Das Feedback der Eltern ist überwältigend positiv: 94 % der befragten Eltern sagen, Teen Accounts erleichtern die Unterstützung ihrer Kinder.

Im Oktober 2025 haben wir angekündigt, dass sich die angezeigten Inhalte in Teen Konten künftig an Altersfreigaben für Filme ab 13 orientieren. Das bedeutet, dass Jugendliche auf Instagram Inhalte sehen, die vergleichbar mit altersgerechten Filmen sind. Jugendliche unter 18 werden automatisch in die aktualisierte 13+ Einstellung versetzt und können diese nur mit Zustimmung eines Elternteils ändern. Da Familien unterschiedlich sind, führen wir auch eine neue, strengere Einstellung für Eltern ein, die eine restriktivere Erfahrung für ihr Kind bevorzugen. Dies wird seit Februar 2026 in Deutschland und der EU ausgerollt. Die Teen Konten werden von uns kontinuierlich weiterentwickelt.

Ein digitales Mindestalter

2025 hat Meta sich für die Einführung eines Digitalen Mindestalters in allen EU-Mitgliedstaaten ausgesprochen, bei der Eltern die Zustimmung für den Zugang ihrer jüngeren Teenager zu digitalen Diensten geben müssen, einschließlich sozialer Medien. Ohne elterliche Zustimmung können Jugendliche diese Apps nicht herunterladen. Eine aktuelle [Umfrage von Morning Consult](#) zeigt, dass drei Viertel der EU-Eltern elterliche Zustimmung für App-Downloads von Jugendlichen unter 16 befürworten. Wir stimmen zu: Eltern kennen ihre Kinder am besten und sollten entscheiden, welche Online-Dienste für ihre Kinder geeignet sind. Regulierung sollte dies ermöglichen und die Entscheidungsfreiheit der Eltern stärken. Ein durchdachtes, EU-weit geltendes Digitales Mindestalter – basierend auf elterlicher Zustimmung, starker Altersverifikation und einem konsistenten Ansatz in der Branche – kann zu mehr Sicherheit für Jugendliche im Netz beitragen.

Wir freuen uns darauf, mit den politischen Entscheidungsträgern in Deutschland und der EU zusammenzuarbeiten, um die Arbeit an unseren Produkten durch unterstützende Gesetzgebung zu ergänzen, die dem gesamten Ökosystem zugutekommt.

Im Folgenden finden Sie weitere Details als Antwort auf die spezifischen Fragen der Expertenkommission.

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:

Wir sind überzeugt, dass die meisten der in diesem Abschnitt angesprochenen Risiken bereits durch den Digital Services Act (DSA) sowie durch andere Rechtsakte effektiv adressiert werden. Der DSA bietet einen sehr umfassenden Rechtsrahmen für Online-Plattformen. Insbesondere die DSA Art. 28 Guidelines sehen detaillierte Empfehlungen dafür vor, wie Plattform Provider die DSA-Vorgaben im Bereich Jugendschutz erreichen können. Darüber hinaus haben Provider wie Meta umfangreiche eigene Richtlinien und Programme definiert, um spezifische Risiken zu adressieren. Mehr Details dazu finden Sie in den Antworten zu den folgenden Fragen.

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

Wir nutzen derzeit einen mehrschichtigen Ansatz, um Grooming und sexuelle Ausbeutung von Kindern auf Facebook und Instagram zu bekämpfen. Zu den wichtigsten Strategien und Tools, die Meta einsetzt, gehören:

- KI und maschinelles Lernen: Meta verwendet künstliche Intelligenz, um Inhalte zu erkennen und zu entfernen, die gegen die Community-Standards von Meta verstoßen – darunter kinderpornografisches Material (CSAM) und Grooming-Verhalten, z. B. in Instagram Direct Messages und Facebook Messenger.
- Proaktive Erkennung & Hashing: Meta setzt Technologien wie PhotoDNA, PDQ und TMK+PDQF ein, um bekannte Missbrauchsbilder zu identifizieren. Jährlich melden wir Millionen Verdachtsfälle von sexuellem Kindesmissbrauch an das National Center for Missing and Exploited Children (NCMEC).
- Schützende Default-Konto-Einstellungen für Jugendliche: Um zu verhindern, dass Erwachsene mit schlechten Absichten Minderjährige finden, hat Meta Beschränkungen eingeführt, die es Erwachsenen untersagen, Jugendlichen Nachrichten zu senden, die ihnen nicht folgen.
- Standard-Datenschutzeinstellungen: Meta hat für Nutzerinnen unter 18 Jahren auf Facebook, Instagram und Messenger standardmäßig private Kontoeinstellungen eingeführt, um ihre Konten zu schützen und unerwünschte Kontakte zu begrenzen.

Wir möchten, dass Menschen – insbesondere junge Menschen – ihre Online-Beziehungen in einem Umfeld pflegen, in dem sie sich sicher fühlen. Wir haben strenge Richtlinien gegen Inhalte oder Aktivitäten, die Kinder ausbeuten oder gefährden, zum Beispiel im Bereich des Postens intime Bilder.

Unser Ziel ist es, identifizierte Konten von Sextortionist-Tätern (Täter sexueller Online-Erpressung) so schnell wie möglich zu entfernen. Wir führen gezielte Untersuchungen durch und löschen regelwidrige Konten, um Netzwerke von Tätern zu stören, die versuchen, Minderjährige auszubeuten oder finanziell zu erpressen. Wir melden diese auch an das NCMEC. Sextortion-Täter geben oft einen falschen Wohnort an, um Jugendliche zu täuschen. Um dem entgegenzuwirken, testen wir neue Sicherheitshinweise in Instagram-Direktnachrichten und im Messenger, die Jugendlichen anzeigen, wenn sie mit jemandem chatten, der sich möglicherweise in einem anderen Land befindet. Sextortion-Täter nutzen häufig die Follower- und Gefolgt-Listen ihrer Opfer, um sie zu erpressen. Konten, bei denen wir betrügerisches oder scammy Verhalten feststellen, können keine Follower- oder Gefolgt-Listen mehr einsehen und verlieren so die Möglichkeit, diese Funktion auszunutzen. Diese potenziellen Sextortionist-Täter können auch nicht mehr sehen, wer Beiträge geliked hat, in welchen Fotos jemand markiert wurde oder welche anderen Konten in Fotos markiert sind.

Instagram und Facebook sind außerdem Gründungsmitglieder von „Take It Down“ – einer Plattform des NCMEC, die verhindern soll, dass intime Bilder junger Menschen, einschließlich KI-generierter Inhalte, online veröffentlicht werden. „Take It Down“ weist dem Bild oder Video einen einzigartigen Hash-Wert – einen Zahlencode – zu, und zwar privat und direkt vom eigenen Gerät. Nach der Übermittlung des Hashes an das NCMEC können Unternehmen

wie Meta diese Hashes nutzen, um Kopien des Bildes zu finden, sie zu entfernen und zu verhindern, dass der Inhalt künftig auf unseren Apps veröffentlicht wird.

Wir arbeiten mit gemeinnützigen Organisationen zusammen, um Informationsmaterialien zu schaffen, die sowohl das Bewusstsein für Sextortion stärken als auch das Stigma rund um intime Bilder abbauen, damit Jugendliche Hilfe suchen und die Kontrolle zurückgewinnen können, wenn sie Sextortion erleben. Gemeinsam mit Thorn und deren Marke NoFiltr haben wir [Bildungsmaterialien](#) entwickelt, die das Schamgefühl und Stigma rund um intime Bilder reduzieren und Jugendliche dazu ermutigen, Hilfe zu suchen und die Kontrolle zurückzugewinnen, wenn sie solche Bilder geteilt haben oder von Sextortion betroffen sind.

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

Im DSA und in anderen Teilen des EU-Rechts besteht bereits Regulierung für die genannten Themenfelder. Das EU-Recht sieht bereits robuste Regelungsansätze zur Bekämpfung von hochgradig nutzerbindenden Designmustern vor.

So betonen die DSA-Richtlinien zu Artikel 28, dass sich Dienste wesentlich in ihrer Art, Nutzung und ihrem Risiko unterscheiden und empfehlen eine dokumentierte, kinderrechtsorientierte Risikoanalyse, um angemessene und verhältnismäßige Maßnahmen auszuwählen. Die Richtlinien enthalten zudem Empfehlungen für Maßnahmen, um manipulative oder persuasive Designtechniken zu vermeiden, die zu übermäßigem, impulsivem oder unerwünschtem Konsum oder zu Suchtverhalten führen könnten. Ziel dieser Vorgaben ist, dass Minderjährige nicht Praktiken ausgesetzt werden, die zu übermäßiger Nutzung führen, wie etwa bezahlte Lootboxen oder Glücksspiel-ähnliche Funktionen.

Die Industrie hat ebenfalls Schutzmechanismen entwickelt. Meta stellt Tools für elterliche Aufsicht, Datenschutzeinstellungen, Inhaltsbeschränkungen und Hinweise für gesundes Nutzungsverhalten bereit (z. B. Bildschirmzeit-Erinnerungen). Wir weisen außerdem darauf hin, dass Präferenzen sich mit Reife, Kontext und Zweck ändern.

Speziell im Bereich Gaming existiert eine robuste Governance durch Inhalte-Standards (z. B. PEGI, ESRB).

Abschließend sehen Verbraucherschutzgesetze (UCPD, Verbraucherrechte-Richtlinie, Richtlinie über digitale Inhalte und Dienste) ebenfalls spezifische Schutzmaßnahmen vor, die sogenannte „Dark Patterns“ adressieren.

Wir warnen daher vor pauschalen Verboten bestimmter Funktionen, da diese bestehende EU-Regelungen und etwa auch die Rolle von In-App-Käufen zur Unterstützung von Free-to-Play-Modellen und Spieleentwicklung außer Acht lassen. Ein ausgewogener Ansatz ist erforderlich. „Dark Patterns“ werden bereits heute durch mehrere EU-Gesetze adressiert.

Wir empfehlen, den Austausch über „Bright Patterns“ zu fördern. Es besteht in diesem Bereich keine Regelungslücke.

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

Metas Ansatz zur Bekämpfung von Hassrede, Desinformation und anderen extremistischen Inhalten basiert sowohl auf unseren eigenen Richtlinien als auch auf EU- und deutschem Recht.

Inhalte, die gegen unsere Richtlinien verstoßen, werden weltweit entfernt, sobald wir davon Kenntnis erlangen. Wenn wir Kenntnis über Inhalte erlangen, die zwar nicht gegen unsere Richtlinien verstoßen, aber nach lokalem Recht (z. B. deutschem Recht) rechtswidrig sind, sperren wir diese für die jeweilige Region, in der sie rechtswidrig sind (Geoblocking).

Wir arbeiten mit globalen Expert*innen aus den Bereichen Technologie, öffentliche Sicherheit und Menschenrechte zusammen, um unsere [Richtlinien](#) zu erarbeiten und regelmäßig zu aktualisieren. Diese definieren, was auf den Meta-Diensten erlaubt ist und was nicht. Wenn Inhalte gegen unsere Richtlinien verstoßen, ergreifen wir entsprechende Maßnahmen. Wir entwickeln Sicherheitsfunktionen, damit Menschen Inhalte melden sowie Konten blockieren, ausblenden oder entfolgen können. Wir setzen unsere Richtlinien sowohl mit Technologie als auch mit menschlicher Überprüfung durch. Mithilfe von Technologie und Review-Teams erkennen, prüfen und bearbeiten wir täglich Millionen von Inhalten auf Facebook und Instagram. Weitere Informationen darüber, wie wir unsere Richtlinien durchsetzen, finden Sie im [Transparency Center](#). Wir veröffentlichen regelmäßig [Transparenzberichte](#), um zu zeigen, wie wir bei der Durchsetzung unserer Richtlinien vorankommen.

Es gibt eine große Überschneidung zwischen Inhalten, die gegen unsere Richtlinien verstoßen, und solchen, die nach deutschem Recht rechtswidrig sind. Wir sind überzeugt, dass dieser mehrschichtige Ansatz zu starken Ergebnissen für unsere Nutzer führt.

Wir möchten im Folgenden unsere Ansätze zu den verschiedenen in der Frage angesprochenen Phänomenen darlegen:

Unser Ansatz gegen Hasserfülltes Verhalten:

Wir verbieten hasserfülltes Verhalten auf Facebook, Instagram und Threads, um sicherzustellen, dass sich Menschen sicher fühlen, wenn sie sich äußern. Hasserfülltes Verhalten ist definiert als direkte Angriffe auf Personen aufgrund geschützter Merkmale (z. B. Rasse, Religion, Geschlecht usw.). Weitere Details finden Sie [hier](#).

Misinformation versus Desinformation:

Wir unterscheiden zwischen Misinformation und Desinformation und wenden unterschiedliche Methoden zur Bekämpfung dieser Phänomene an:

Misinformation: wird oft unbeabsichtigt geteilt, der Fokus liegt auf dem Inhalt. Wir wenden diesbezüglich eine 3-teilige Strategie an aus den Elementen: Entfernen, Reduzieren, Informieren. Mehr Details dazu weiter unten.

Desinformation: ist durch ein Element der bewussten Täuschung oder Manipulation gekennzeichnet. Der Fokus liegt auf dem Verhalten. Wir begegnen Desinformation über unsere Richtlinie gegen koordiniertes irreführendes Verhalten (coordinated inauthentic behavior) (weitere Infos unten).

Unser Ansatz gegen Misinformation:

Unsere Richtlinien unterscheiden zwischen verschiedenen Kategorien von Fehlinformationen, mit denen wir unterschiedlich umgehen. Wir entfernen Fehlinformationen, wenn sie wahrscheinlich direkt zur Gefahr von Gewalt bzw. Körperverletzung beitragen. Wir entfernen auch Inhalte, die wahrscheinlich direkt zur Beeinträchtigung des Funktionierens politischer Prozesse beitragen. Bei allen anderen Fehlinformationen konzentrieren wir uns darauf, ihre Verbreitung zu verringern und unseren Nutzern hilfreiche Informationen bereitzustellen. Wir arbeiten außerhalb der USA mit externen Organisationen für Faktenprüfung zusammen, um die Richtigkeit der am häufigsten verbreiteten Inhalte auf unseren Plattformen zu überprüfen und zu bewerten ([hier](#) und [hier](#) erfahren Sie mehr über unseren Ansatz in den USA). Außerdem fördern wir Medienkompetenz. Wir verlangen von unseren Nutzern, dass sie KI-generierte Inhalte mithilfe unseres KI-Melde-Tools offenlegen, und wir können irreführende digitale Inhalte markieren oder sanktionieren. Schließlich verbieten wir Inhalte und Verhaltensweisen in anderen Bereichen, die sich oft mit der Verbreitung von Fehlinformationen überschneiden. So verbieten wir etwa gefälschte Konten, Betrug und koordiniertes irreführendes Verhalten.

Unser Ansatz gegen koordiniertes irreführendes Verhalten (coordinated inauthentic behavior):

Koordiniertes irreführendes Verhalten bezeichnet eine Vielzahl komplexer Formen der Täuschung, die durch ein Netzwerk irreführender Assets vorgenommen werden, die von derselben Person oder denselben Personen kontrolliert werden, mit dem Ziel, Meta oder unsere Community zu täuschen oder sich der Durchsetzung unserer Gemeinschaftsstandards zu entziehen. Wenn feindliche Akteure falsche Identitäten verwenden, um sich an ausgeklügelten Formen von irreführendem Verhalten zu beteiligen, sprechen wir von koordiniertem irreführendem Verhalten. Wir entfernen Netzwerke von Fake-Accounts, Seiten oder Gruppen, die darauf abzielen, Nutzer oder Meta zu täuschen. Wenn authentische Communities betroffen sind, entfernen wir nur die Akteure, die sich an dem regelwidrigen Verhalten beteiligen. Unsere Erkenntnisse werden in [Adversarial Threat Reports](#) veröffentlicht.

Unser Ansatz gegen gefährliche Organisationen und Einzelpersonen:

Wir verbannen Organisationen oder Einzelpersonen mit gewalttätigen Zielen von unseren Plattformen und bewerten diesbezüglich sowohl deren Online- als auch Offline-Verhalten.

- Tier 1: Akteure mit direkten Verbindungen zu Gewalt gegen Zivilisten (z. B. Terror- oder Hassgruppen). Wir entfernen jegliche Unterstützung, Verherrlichung oder Darstellung, einschließlich zugehöriger Ereignisse oder Ideologien.
- Tier 2: Gewaltbereite nichtstaatliche Akteure, die sich gegen staatliche Akteure richten oder Gewalt vorbereiten. Auch hier entfernen wir Unterstützung und Darstellung.

Weitere Informationen finden Sie [hier](#) und in unserer [Corporate Human Rights Policy](#).

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

Mobbing und Belästigung können an vielen Orten und in unterschiedlichen Formen auftreten – von Drohungen und der Veröffentlichung personenbezogener Daten bis hin zu bedrohlichen Nachrichten und unerwünschtem, böswilligem Kontakt. Wir tolerieren solches Verhalten nicht, da es Menschen daran hindert, sich auf unseren Apps sicher und respektiert zu fühlen.

Wir unterscheiden zwischen öffentlichen Personen und Privatpersonen, weil wir Diskussionen ermöglichen möchten, die oft auch kritische Kommentare über Personen beinhalten, die in den Nachrichten stehen oder ein großes öffentliches Publikum haben. Bei in der Öffentlichkeit stehenden Personen entfernen wir Angriffe, die schwerwiegend sind, sowie bestimmte Angriffe, bei denen die Person direkt im Beitrag oder Kommentar markiert wird.

Für Privatpersonen gehen unsere Schutzmaßnahmen weiter: Wir entfernen Inhalte, die darauf abzielen, jemanden herabzuwürdigen oder zu beschämen – zum Beispiel Behauptungen über das Sexualleben einer Person. Uns ist bewusst, dass Mobbing und Belästigung besonders für Minderjährige emotional belastend sein können. Deshalb bieten unsere Richtlinien einen erhöhten Schutz für Nutzer*innen im Alter von 13 bis 18 Jahren.

Wir bieten unseren Nutzern außerdem Zugang zu fachlich geprüften Leitfäden und Informationsmaterialien. Zum Beispiel bietet der [Meta Bullying Prevention Hub](#) eine umfassende Information, die gemeinsam mit dem [Yale Center for Emotional Intelligence](#) für Jugendliche, Eltern und Lehrkräfte entwickelt wurde. Er bietet Schritt-für-Schritt-Anleitungen zur Erkennung, Prävention und zum Umgang mit Mobbing und erklärt Tools zum Blockieren, Einschränken und Melden auf Facebook und Instagram. Zu den wichtigsten Funktionen und Informationsmaterialien gehören:

- Schutz für Minderjährige: Spezielle Richtlinien und erweiterte Schutzmaßnahmen für Nutzer im Alter von 13–18 Jahren.

- Melde-Tools: Nutzer können Mobbing, Belästigung oder missbräuchliche Inhalte melden, damit diese entfernt werden, wenn sie gegen die Gemeinschaftsstandards verstoßen.
- Sicherheits-Tools: Funktionen wie das Blockieren von Profilen, das Einschränken von Interaktionen und das Filtern von Kommentaren.
- Unterstützungsangebote: Der Hub bietet Ratschläge, wie man Gespräche über Mobbing beginnt, Anzeichen erkennt und Aktionspläne erstellt.
- Spezialisierte Informationsmaterialien: Enthält Tools zum Umgang mit Missbrauch intimer Bilder, z. B. [StopNCII.org](#) und [Stop Sextortion](#).

Für sofortige, praktische Schritte gegen Mobbing auf Meta-Plattformen können Nutzer den Bullying Prevention Hub direkt über das [Meta Safety Center](#) aufrufen.

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

Wir konsultieren regelmäßig Experten für Suizid, Selbstverletzung und Essstörungen, um unsere Richtlinien und deren Durchsetzung zu verbessern, und arbeiten mit Organisationen weltweit zusammen, um Menschen in akuten Krisen zu unterstützen.

Wir erlauben es nicht, dass Menschen absichtlich oder unabsichtlich Suizid, Selbstverletzung oder Essstörungen feiern oder fördern. Wir erlauben jedoch, dass über diese Themen gesprochen wird, weil wir möchten, dass unsere Dienste ein Raum sind, in dem Menschen ihre Erfahrungen teilen, das Bewusstsein für diese Themen stärken und sich gegenseitig unterstützen können. Wir können die Sichtbarkeit solcher Inhalte auf Erwachsene ab 18 Jahren beschränken.

Wir entfernen jegliche Inhalte, die zu Suizid, Selbstverletzung oder Essstörungen ermutigen – einschließlich fiktiver Inhalte wie Memes oder Illustrationen – sowie jegliche explizite und grafische Selbstverletzungsinhalte, unabhängig vom Kontext. Wir entfernen Inhalte, die Anleitungen für extremen Gewichtsverlust enthalten. Ebenso entfernen wir Inhalte, die Opfer oder Überlebende von Suizid, Selbstverletzung oder Essstörungen verspotten, sowie Echtzeit-Darstellungen von Suizid oder Selbstverletzung. Inhalte über die Genesung von Suizid, Selbstverletzung oder Essstörungen, die erlaubt sind, aber möglicherweise verstörende Bilder enthalten (wie eine verheilte Narbe), werden hinter einem Sensitivitätsbildschirm platziert und die Sichtbarkeit wird auf Erwachsene ab 18 Jahren beschränkt.

Wenn Menschen Inhalte zu Suizid, Selbstverletzung oder Essstörungen posten oder danach suchen, leiten wir sie zu lokalen Organisationen weiter, die Unterstützung bieten können. Wenn unser Community Operations Team eine unmittelbare Gefahr erkennt, kontaktieren

wir lokale Notdienste – auch in Deutschland – um Hilfe zu leisten. Weitere Informationen finden Sie im [Meta Safety Center](#).

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

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

Bitte lesen Sie hierzu unsere Antwort auf die übergeordnete Leitfrage sowie die erste Fragensammlung unter I. und insbesondere unsere Darstellung der [Teen Account](#)- und [Parental Oversight](#)-Funktionen.

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

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

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)?

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

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?

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

Wie bereits oben in unserer ausführlichen Antwort zur Leitfrage dargelegt, sind wir der Ansicht, dass bestehendes EU-Recht durch zusätzliche Regelungen zur Altersverifikation ergänzt werden sollte. Das Verständnis des Alters ist grundlegend, um altersgerechte Erlebnisse und Schutz zu bieten. Der DSA und seine DSA Guidelines nach Art. 28 zum Jugendschutz harmonisieren zu Recht die Gesetze der Mitgliedstaaten und definieren ein einheitliches EU-weites Regelwerk, konzentrieren sich jedoch hauptsächlich darauf, dass regulierte Dienste Risiken auf ihren Plattformen mindern. Es besteht Bedarf an neuen, zusätzlichen Regelungen, die einen verbindlichen europäischen Rahmen für Altersverifikation schaffen – idealerweise kombiniert mit elterlicher Zustimmung. Dies würde Klarheit und verbesserte Praktiken in der gesamten Branche bringen.

Während der DSA für alle Online-Vermittler und Plattformen gilt, haben sehr große Online-Plattformen und Suchmaschinen (VLOPs und VLOSEs) zusätzliche Verpflichtungen. Das bedeutet, dass viele Apps, die von jungen Menschen häufig genutzt werden (z. B.

iMessage, Roblox), nicht in gleicher Weise von den Regeln erfasst werden – und neue Apps werden in wichtigen Bereichen wie Altersverifikation und elterlicher Kontrolle nicht denselben Anforderungen unterliegen. Das ist problematisch, denn alle Apps müssen in der Lage sein, altersgerechte Erlebnisse zu bieten.

Um die Online-Umgebung für junge Menschen sicherer und vertrauenswürdiger zu machen, sind aus unserer Sicht neue, harmonisierte EU-Regeln erforderlich, die Altersverifikation und elterliche Zustimmung auf Betriebssystem- oder App-Store-Ebene einschließen. Wir ermutigen Deutschland, sich für solche neuen gesetzlichen Regeln auf EU-Ebene einzusetzen und das bestehende nationale Rahmenwerk bis zum Handeln der Europäischen Kommission entsprechend zu ergänzen. Dies wird dazu beitragen, den Jugendschutz im Internet zu verbessern und Eltern klare Möglichkeiten zu geben, die vielen Apps zu überwachen, die ihre Kinder nutzen.

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

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?

Bitte lesen Sie zu dieser Frage unsere ausführliche Antwort zur Leitfrage sowie unsere Antwort zum Fragenkomplex III. Aus unserer Sicht eignet sich die Ebene der Betriebssysteme und App-Stores sehr gut sowohl für die Anknüpfung der Altersverifikation als auch für Verankerung der elterlichen Zustimmung zum Download von Apps durch Teenager.

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

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?

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

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?

Wie oben bereits an verschiedenen Stellen unserer Antworten zum Fragebogen erwähnt, bietet der DSA in den wichtigsten Bereichen bereits einen umfassenden Rahmen. Neue politische Vorschläge sollten darauf abzielen, Lücken im Bereich Jugendschutz zu schließen. Dies betrifft den Bereich der Altersverifikation und die Rolle der Eltern. Eine Ergänzung der aktuellen Gesetzgebung in diesen konkreten Bereichen würde zu einem stärkeren Jugendschutz führen, ohne neue Überschneidungen oder Widersprüche mit bereits regulierten Bereichen zu schaffen.

Wir möchten unsere Antwort auf die oben genannten Fragen bündeln und noch einmal auf unsere ausführliche Antwort, insbesondere zur Leitfrage, verweisen. Aus diesem Grund geben wir hier nur eine kurze Zusammenfassung der wichtigsten Überlegungen.

Wichtige Überlegungen

Für Regierungen, die eine Regulierung von Altersbeschränkungen erwägen, ist die wichtigste Überlegung, auf welche Dienste das Gesetz Anwendung findet (Geltungsbereich). Weitere zentrale Aspekte sind, wie das Alter verifiziert wird und welche Rolle die Eltern spielen. Die Berücksichtigung aller drei Punkte stellt sicher, dass die Gesetzgebung den Bedürfnissen von Familien gerecht wird und effektiv umgesetzt werden kann.

I. Geltungsbereich

Die Online-Aktivitäten junger Menschen umfassen ein komplexes Ökosystem aus Apps und Diensten. Jede Intervention muss ein umfassendes Verständnis dafür widerspiegeln, wie Jugendliche das Internet nutzen, und sollte ähnliche Dienste konsistent behandeln. Jugendliche nutzen durchschnittlich 40 Apps pro Woche mit unterschiedlichen Funktionen und damit verbundenen unterschiedlichen Risiken. Der Anwendungsbereich sollte

entsprechend weit gestaltet sein, damit Jugendliche nicht auf unsichere unregulierte Dienste ausweichen.

II. Wie das Alter verifiziert wird

Damit Altersbeschränkungen funktionieren, muss die Verifikation effektiv sein. Derzeit unterscheiden sich die Methoden je nach App – ein Jugendlicher kann auf einem Dienst angeben, 18 zu sein, während er auf einem anderen als 14 verifiziert ist. Ein zentralisiertes, standardisiertes System würde dieses Problem lösen. Ein vielversprechender Ansatz ist, App-Stores oder mobile Betriebssysteme dazu zu verpflichten, bei der Installation einer App durch einen Jugendlichen eine elterliche Zustimmung einzuholen und das Alter zu verifizieren. Dies ist datenschutzfreundlich, genießt elterliche Unterstützung und nutzt bestehende Freigabesysteme, über die Eltern entscheiden können, welche Apps ihre Kinder nutzen dürfen.

Mit der Verifikation auf OS-/App-Store-Ebene als erster Verteidigungslinie kann das Alters-Signal datenschutzfreundlich an Dienste wie die von Meta angebotenen weitergegeben werden, sodass Jugendliche Zugang zu altersgerechten Angeboten wie Teen Konten erhalten während der Zugang zu ungeeigneten Diensten eingeschränkt wird. Dienste wie die von Meta spielen weiterhin eine Rolle – wenn sie Hinweise auf eine fehlerhafte Altersangabe finden, geben sie diese Information an den OS/App-Store zurück, um das Alters-Signal zu verbessern und einen positiven Feedback-Kreislauf zu schaffen.

Dieser Ansatz reduziert auch das Risiko von Umgehungen. Die Verifikation auf dieser Ebene verhindert, dass Jugendliche einfach VPNs oder den Tor-Browser herunterladen, um plattformspezifische Sperren zu umgehen – ein Hauptproblem aktueller Systeme.

Eine branchenweite Lösung, bei der alle Apps denselben, konsistenten Standard erfüllen müssen, würde die notwendige Einheitlichkeit schaffen, um junge Menschen am effektivsten zu schützen.

Es gibt für die Altersfeststellung verschiedene denkbare Systeme. Meta ist im Dezember als Gründungspartner der Open Age Initiative beigetreten. Open Age, eine Non-Profit-Organisation mit Fokus auf Altersverifikation, unterstützt von k-ID, hat ein neues Altersverifikations-Tool namens „AgeKey“ eingeführt. Für teilnehmende Plattformen können Nutzer*innen einen verifizierten AgeKey auf ihrem Gerät einrichten und damit verifizierte Altersdaten mit mehreren Diensten teilen.

III. Elterliche Zustimmung

Gesetzgebung sollte Eltern befähigen, zu steuern, wie ihre Familie digitale Dienste nutzt, und Eltern in ganz Europa wünschen sich das letzte Wort darüber, welche Apps ihre Jugendlichen nutzen dürfen. Eine [Morning Consult-Umfrage](#) unter europäischen Eltern, darunter aus Deutschland, ergab, dass fast 75 % in allen acht befragten Ländern ein europaweites Gesetz

befürworten würden, das eine elterliche Zustimmung für das Herunterladen von Apps durch unter 16-Jährige verlangt.

Fazit

Meta möchte ein konstruktiver Partner im Gesetzgebungsprozess sein und mit politischen Entscheidungsträgern zusammenarbeiten. Die Sicherheit von Jugendlichen zu gewährleisten ist eine unserer wichtigsten Produkt-Prioritäten, und wir werden weiterhin kontinuierlich Verbesserungen an unseren eigenen Diensten vornehmen. Gemeinsame politische Veränderungen können dies ergänzen. Gemeinsam können wir eine bessere Online-Umgebung schaffen, der Eltern und Jugendliche vertrauen können. Wir stehen bereit, unsere Expertise in den Gesetzgebungsprozess einzubringen.

4. Braucht es aus Ihrer Sicht speziell gestaltete digitale Räume für Kinder und Jugendliche mit begrenztem oder ausgeschlossenen Zugang für Erwachsene, und wie ließen sich solche Räume technisch, rechtlich und organisatorisch realisieren?

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?

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)?

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?