

Stellungnahme anlässlich des zweiten Hearings der Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt“ am 13. Februar 2026 zum Thema „Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste“

Berlin/Köln, 6. Februar 2026

Im Herbst 2025 hat die Bundesregierung die Expertenkommission "Kinder- und Jugendschutz in der digitalen Welt" einberufen.

Die Kommission soll eine Strategie für den "Kinder- und Jugendschutz in der digitalen Welt" mit konkreten Handlungsempfehlungen für die zuständigen Akteure wie Bund, Länder und Zivilgesellschaft erarbeiten. Dabei liegt der Themenfokus auf den notwendigen Voraussetzungen für ein sicheres, digitales Umfeld für Kinder und Jugendliche sowie auf den gesundheitlichen Folgen von Medienkonsum und auf der Stärkung von Medienkompetenz bei Kindern, Jugendlichen, Eltern und Fachkräften.

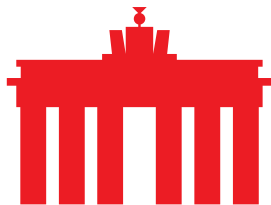
Am 13. Februar 2026 findet das zweite Hearing der Expertenkommission statt. Hierbei soll das Thema „Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste“ erörtert werden. In diesem Zusammenhang hat die Expertenkommission Gelegenheit zur Stellungnahme zu folgender Leitfrage gegeben:

„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?“

eco – Verband der Internetwirtschaft e.V. (eco) bedankt sich für die Möglichkeit zur Stellungnahme und Hearing-Teilnahme.

Die Bekämpfung rechtswidriger, insbesondere jugendschutzrelevanter Internetinhalte sowie ein effektiver und zugleich praktikabler Jugendmedienschutz sind eco und seinen Mitgliedsunternehmen wichtige Anliegen. So betreibt eco als Teil der Selbstregulierung seit 30 Jahren eine Beschwerdestelle für rechtswidrige und jugendschutzrelevante Internetinhalte (eco Beschwerdestelle) und setzt sich für die schnelle Löschung rechtswidriger Internetinhalte ein. Die eco Beschwerdestelle steht zudem mit den eco Mitgliedsunternehmen im regelmäßigen Austausch zu Fragen eines modernen, praktikablen und zugleich effektiven Jugendmedienschutzes, und nimmt zudem durch regelmäßige Fachvorträge vor Eltern und pädagogischen Fachkräften eine wichtige Rolle bei der Sensibilisierung und Vermittlung von Maßnahmen im Bereich des Jugendmedienschutzes ein.

Nachfolgende Ausführungen basieren auf unseren Erfahrungen und Einschätzungen als Internet-Branchenverband und Betreiber einer Internet-Beschwerdestelle.



▪ Allgemeine Erwägungen

Digitale Medien und digitale Kommunikation sind aus der Lebensrealität von Kindern und Jugendlichen nicht mehr wegzudenken. Sie gehören schlicht weg zu ihrem Alltag und bieten schier unendliche Möglichkeiten. Egal ob beim Lernen, zu Informations- oder Unterhaltungszwecken, um mit Freunden und Familie in Kontakt zu bleiben oder um die eigene Persönlichkeit zu entdecken - um nur einige Beispiele zu nennen.

Neben allen Vorteilen, die digitale Dienste bieten, gibt es wie im analogen Leben auch „online“ Risiken, die es zu adressieren gilt. Zugleich entwickeln sich digitale Medien und digitale Kommunikation stetig weiter. Damit stellt sich kontinuierlich die Frage, wie der Schutz junger Menschen im digitalen Raum zeitgemäß gelingen kann, ohne ihre gesellschaftliche Teilhabe zu beschneiden.

Der Jugendmedienschutz fußt auf drei Säulen: Teilhabe, Schutz und Befähigung, die letztlich einen Dreiklang bilden. Dabei sind Teilhabe, Schutz und Befähigung gleichermaßen wichtig und im stetigen Spannungsfeld zueinander. Der richtige Ansatz und ein eventueller Vorrang eines dieser Elemente muss in jeder neuen Konstellation neu austariert werden.

Zugleich besteht der Wunsch (und die Notwendigkeit) der Eltern und Erziehungsverantwortlichen, ihr Mitspracherecht zu behalten.

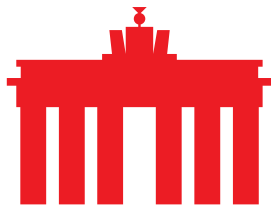
Vor diesem Hintergrund unterstützt eco den Ansatz des Hearings, technische, regulatorische und pädagogische Maßnahmen gemeinsam zu denken und zu erörtern.

▪ Risiken, Schutzmaßnahmen und Gestaltung digitaler Dienste

Wichtig und am wirksamsten sind mehrschichtige, risikobasierte Ansätze, um Kinder und Jugendliche vor Inhalts- und Interaktionsrisiken zu schützen bzw. deren Folgen zu begrenzen. Dabei gibt es keine „One size fits all“-Lösung, da jeder digitaler Dienst letztlich ein einzigartiges Angebot zur Verfügung stellt und unterschiedliche Dienstarten darüber hinaus über unterschiedliche Handlungs- und Reaktionsmöglichkeiten verfügen. Für die Frage nach den wirksamsten Maßnahmen ist daher stets eine differenzierte (Einzelfall-)Betrachtung notwendig.

Ganz allgemein lässt sich dennoch sagen, dass von den Unternehmen in Abhängigkeit vom jeweiligen Angebot bzw. Dienst insbesondere folgende Maßnahmen als Elemente eines wirksamen, mehrschichtigen Schutzansatzes bei der Begrenzung von Risiken für Kinder und Jugendliche in Betracht gezogen werden können:

- Altersgerechte Voreinstellungen bzw. Account-Einstellungen
- Gut sichtbare Möglichkeiten zum Melden und Blockieren von Inhalten sowie klare Abläufe, wie das auf gemeldete Probleme reagiert wird
- Freiwillige technische Maßnahmen zur Erkennung von unzulässigen Inhalten



- Klare allgemeine Geschäftsbedingungen, Community Guidelines etc.
- Präventive Maßnahmen wie Sensibilisierung, Aufklärung und Vermittlung von Medienkompetenz
- Enge Zusammenarbeit zwischen Unternehmen, spezialisierten Beschwerdestellen und Strafverfolgungsbehörden

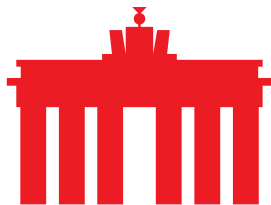
Altersgerechte Voreinstellungen bzw. Account-Einstellungen, wie sie bereits heute von vielen Unternehmen vorgesehen sind bzw. angeboten werden, bieten eine Vielzahl von unterschiedlichen Möglichkeiten, um vor Risiken zu schützen bzw. diese zu begrenzen. Dabei kommen entsprechende Einstellungsmöglichkeiten in Bezug auf diverse Risiken in Betracht. Sie können beispielsweise Kontakt- und Kommunikationsfunktionen betreffen und hierdurch vor digitaler sexualisierter Gewalt in Form von Grooming oder Sextortion sowie anderen Interaktionsrisiken schützen. Pausenempfehlungen für die Nutzenden oder von den Eltern wählbare Zeitlimits können Risiken einer übermäßigen Nutzung von Diensten reduzieren. Schließlich könne Accounteinstellungen einen wesentlichen Beitrag zum Schutz von Daten und Privatsphäre leisten.

Gut sichtbare Meldeoptionen und klare Abläufe zum Umgang mit Meldungen leisten einen wesentlichen Beitrag, wenn es um die Reduzierung der Verfügbarkeit von illegalen und jugendschutzrelevanten Online-Inhalten wie z.B. Missbrauchsdarstellungen, Volksverhetzung und andere verfassungsfeindliche Inhalte oder Selbstgefährdungsrisiken geht. Hierbei betrifft der mögliche Schutz nicht nur eine einzelne Person, sondern alle Nutzenden eines Dienstes.

Freiwillige technische Maßnahmen können dazu beitragen, bestimmte illegale Inhalte zu erkennen/identifizieren und so Inhaltsrisiken zu reduzieren. Die Möglichkeit zum Einsatz und die konkrete Ausgestaltung entsprechender Maßnahmen hängt dabei wesentlich vom jeweiligen Dienst und den zu identifizierenden Inhalten ab. Häufig sind sie kombiniert mit menschlicher Moderation, insbesondere bei Äußerungsdelikten. Insgesamt gilt, dass der Einsatz technischer Maßnahmen zur Identifizierung von Inhalten stets verhältnismäßig ausgestaltet und Datenschutz sowie Grundrechte wahren muss. Zudem ist eine Schwächung von Verschlüsselungstechnologien zu vermeiden. Auch ist der Einsatz entsprechender Maßnahmen stark abhängig von der jeweils angebotenen Dienstart.

Allgemeine Geschäftsbedingungen, Community Guidelines und dergleichen helfen bei der Durchsetzung von Maßnahmen im Rahmen der Content Moderation und geben zudem Orientierung für die Nutzenden der entsprechenden Dienst. Hierdurch leisten sie auch einen Beitrag zu Sensibilisierung, Aufklärung und Vermittlung von Medienkompetenz.

Im Hinblick darauf, dass Befähigung und Teilhabe wesentliche Elemente des Jugendmedienschutzes sind, kommt der Vermittlung von Medienkompetenz bzw. der Sensibilisierung und Aufklärung rund um Risiken, Gefährdungslagen und Schutzmaßnahmen bzw. Reaktionsmöglichkeiten eine zentrale Rolle. Hierdurch können sämtliche Risiken reduziert bzw. deren Wirkungen begrenzt werden.



Schließlich ist eine enge Zusammenarbeit zwischen Unternehmen, spezialisierten Beschwerdestellen und Strafverfolgungsbehörden zentral, wenn es um die Löschung von rechtswidrigen Internetinhalten geht. Beschwerdestellen leisten durch ihre Expertise und Zusammenarbeit sowohl mit den Unternehmen wie den Strafverfolgungsbehörden einen wesentlichen Beitrag. Sie übermitteln validierte Informationen zu verbotenen Internetinhalten an die Unternehmen, die aufgrund der Vorprüfung schnell agieren und die die Inhalte entfernen können. Zudem bewirkt die Kooperation mit Strafverfolgungsbehörden, dass Täter verfolgt werden können, wodurch ein Beitrag zur Generalprävention geleistet wird.

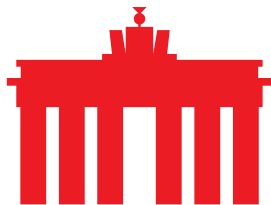
Altersgerechte Default-Einstellungen sorgen dafür, dass Schutzmechanismen automatisch aktiv sind, ohne dass Nutzer:innen sie selbst einstellen müssen. Viele Anbieter bieten bereits altersgerechte Kontomodelle an, die speziell für Kinder oder Jugendliche angepasst sind und automatisch Schutzmechanismen enthalten. Empfehlungs- und Rankingsysteme sollten problematische Inhalte weniger sichtbar machen und transparent gestaltet sein, während Sharing- und Kontaktfunktionen den direkten Austausch zwischen Erwachsenen und Minderjährigen einschränken können. Auch das Interface-Design spielt eine Rolle: Schutzfunktionen müssen leicht auffindbar sein und manipulative Gestaltungen vermieden werden. Ergänzend ermöglichen Parental-Control-Funktionen Zeit-, Inhalts- oder Budgetbegrenzungen, um Kinder beim sicheren Umgang mit digitalen Angeboten zu unterstützen. Für international tätige Anbieter ist dabei entscheidend, dass Schutzmechanismen global umsetzbar bleiben und nationale Sonderregelungen nicht zu Fragmentierung führen.

Der Umstand, dass die in ihrer Ausrichtung divers aufgestellten Unternehmen bereits heute viele für ihr Angebot passende und effektive Schutzmaßnahmen implementiert haben, sollte im weiteren Diskurs stets bedacht werden, gerade auch mit Blick auf etwaige konkrete inhaltlich-regulatorische Handlungs- bzw. Weiterentwicklungsnotwendigkeiten.

▪ **Plattformverantwortung, Regulierung und Durchsetzung**

Der Jugendmedienschutz ist gemeinschaftliche und gesamtgesellschaftliche Aufgabe. Auch Plattformbetreiber tragen daher einen Teil der „Verantwortung“ für den Schutz von Kindern und Jugendlichen, die sich an bestehenden rechtlichen Vorgaben wie Art. 28 DSA, JMStV und JuSchG orientiert.

Insgesamt ist essenziell, dass die Verantwortung von Plattformen rechtlich klar definiert und praktisch umsetzbar ist. Dabei ist zu berücksichtigen, dass Vorgaben kohärent und international anschlussfähig sein müssen, um nationale Insellösungen zu vermeiden und der globalen Nutzung der Plattformen gerecht zu werden. EU-weit einheitliche Ansätze und (regulatorische) Weiterentwicklungen spielen dabei eine wichtige Rolle, um Schutzmaßnahmen europaweit konsistent umzusetzen und administrative Aufwände zu reduzieren. Im Hinblick auf Weiterentwicklungen ist dabei wichtig, Vorgaben technologieoffen zu formulieren, um unterschiedlichen Diensten und Geschäftsmodellen gerecht zu werden.



Zudem sind stets auch das austarierte Haftungsgefüge und die Verantwortlichkeitsregelungen des DSA zu beachten.

Die Umsetzung bestehender Vorschriften zum Schutz Minderjähriger kann durch klare Leitlinien und standardisierte Verfahren weiter unterstützt werden. Auch der dialogische Austausch mit den Unternehmen sollte fortgesetzt werden. Die bestehenden verpflichtenden Audits und Transparenzberichte können insoweit helfen, Themen zu identifizieren, für die es weitere Orientierung bedarf.

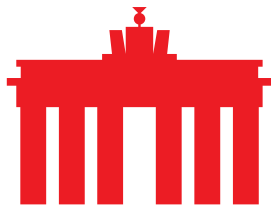
Im Hinblick auf den technischen Jugendmedienschutz werden zunehmend auch Betriebssysteme und App-Stores in den Blick genommen.

Betriebssysteme und App-Stores können den technischen Jugendmedienschutz unterstützen, indem sie Jugendschutzeinstellungen bereitstellen, die entweder geräteweit oder innerhalb einzelner Apps wirken, und durch einheitliche Alterskennzeichnungen oder Label-Standards, die Orientierung für Kinder, Eltern und Anbieter schaffen. Auch Default-Beschränkungen für Käufe oder bestimmte Funktionen können automatisch Schutz bieten.

eco möchte erneut darauf hinweisen, dass es unterschiedliche technische Wege gibt, diese Maßnahmen umzusetzen, und entsprechende Vorgaben sollten flexibel gestaltet sein, sodass globale Anbieter die Schutzmaßnahmen je nach technischer Umsetzung und nationalem Rechtsrahmen konsistent einhalten können. Betriebssystemansätze sollten dabei auch Account- bzw. Profil-basierte Ansätze in der Umsetzung als ausreichend und geeignet zulassen. Regulatorisch könnten standardisierte Anforderungen und Leitlinien dazu beitragen, Schutzmaßnahmen transparent und wirksam zu implementieren, ohne die Innovationsfähigkeit der Anbieter unnötig einzuschränken.

Im Hinblick auf die Frage nach wirtschaftlichen und betrieblichen Implikationen im Zusammenhang mit einem umfassenden Jugendmedienschutz möchte eco hervorheben, dass sich umfassender Jugendmedienschutz auf betriebliche Aufwände, technische Implementierungen und Produktentwicklungen auswirkt. Dazu gehören Anpassungen von Algorithmen, Interfaces und Meldesystemen, laufende Risikoanalysen und Compliance-Checks sowie mögliche Einschränkungen bei Monetarisierung oder Funktionsumfang. Außerdem sind Mitarbeiterschulungen und externe Beratungen erforderlich, um die Schutzmaßnahmen wirksam umzusetzen. Wichtig ist, dass diese Maßnahmen effizient, skalierbar und international umsetzbar gestaltet werden, damit sie Innovation und Wettbewerbsfähigkeit der Anbieter nicht übermäßig beeinträchtigen. Zudem gilt es zu berücksichtigen, dass nicht alle Optionen des technischen Jugendmedienschutzes mit dem im Einzelfall gewählten technischen Set-Up kompatibel sein können. Auswirkungen auf die technische Sicherheit des jeweiligen Dienstes sind zu vermeiden.

Zu den technischen Sicherheitsfunktionen gehört auch der Einsatz von Verschlüsselungstechnologien. Ende-zu-Ende-Verschlüsselung schützt die Privatsphäre der Nutzenden, auch die von Kindern und Jugendlichen, weil Nachrichten nur vom Absender und Empfänger gelesen werden können. Aufgrund



der gravierenden Auswirkungen auf die Sicherheit aller Nutzenden lehnt eco eine Schwächung von gewählten Verschlüsselungstechnologien ab.

Mitunter wird dem Einsatz von Verschlüsselungstechnologien entgegengehalten, dass dies die Identifizierung von illegalen Inhalten erschwere, da keine proaktive Suche durch die Unternehmen möglich sei. Plattformen federn dieses vermeintliche Manko ab, indem sie sichere Meldesysteme bereitstellen, über die Nutzer:innen riskante Inhalte melden können, und Risikoberichte erstellen, die anonymisierte Informationen über problematische Nutzungsmuster auswerten. Zudem arbeiten die Unternehmen mit spezialisierten Beschwerdestellen zusammen, die ebenfalls als Anlaufstelle für die Nutzenden zur Verfügung stehen und Inhalte an die Plattformen melden, bei denen ein Rechtsverstoß festgestellt bzw. validiert wurde.

Wichtig ist, dass der Schutz der Privatsphäre und der technischen Sicherheitsfunktionen nicht leichtfertig eingeschränkt wird und Präventionsmaßnahmen so umgesetzt werden, dass Kinder und Jugendliche geschützt sind, ohne die Ende-zu-Ende-Verschlüsselung aufzuheben.

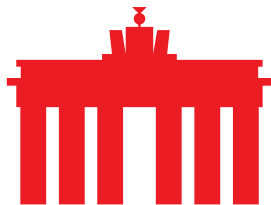
▪ Altersgrenzen, Altersverifikation und spezifische Schutzräume

Die aktuelle Diskussion um Altersgrenzen, Altersverifikation und altersgerechte Schutzräume ist in Europa und international vielfältig: Einige (Mitglieds-)Staaten haben nationale Mindestaltersgrenzen festgelegt oder diskutieren diese, das Europäische Parlament empfiehlt im Rahmen eines sog. INI Reports ein Mindestalter von 16 Jahren für Social Media sowie vergleichbare Lösungen für Video-Sharing-Plattformen und risikobehaftete AI Dienste, mit Möglichkeiten für jüngere Kinder bei Zustimmung der Eltern (REPORT on the protection of minors online, https://www.europarl.europa.eu/doceo/document/A-10-2025-0213_EN.html). Auf EU-Rats-Ebene haben sich die Mitgliedsstaaten mehrheitlich in der sog. „Jütland-Erklärung“ im Oktober 2025 für Altersbegrenzungen ausgesprochen und zudem eine datensparsame und interoperable Altersverifikation gefordert, etwa über EU-Digital-Wallets. Gleichzeitig existieren unterschiedliche Ansätze in anderen Ländern wie Australien oder Großbritannien. Für international tätige Plattformen bedeutet dies einen komplexen rechtlichen Flickenteppich und potenzielle Compliance-Herausforderungen.

Zugleich haben viele Anbieter bereits auf freiwilliger Basis seit Jahren praktikable Lösungen implementiert, wie altersgerechte Accounts, Jugendschutzeinstellungen und standardisierte Schutzmechanismen, um Kindern und Jugendlichen einen sicheren Zugang zu digitalen Diensten zu ermöglichen.

Die Festlegung eines Mindestalters für die Nutzung bestimmter digitaler Dienste ist also nicht gänzlich neu. Viele Anbieter haben den Jugendschutz seit Jahren im Blick und legen ein für ihr Angebot/Produkt passendes Mindestalter fest bzw. haben spezielle Schutzeinstellungen für Minderjährige implementiert.

Im Hinblick auf die aktuelle Diskussion zu verbindlichen, gesetzlich verankerten Altersgrenzen gilt es aus Sicht von eco zudem folgende, mitunter gegensätzliche Punkte zu bedenken:



Altersbegrenzungen für bestimmte digitale Angebote sind insbesondere dort sinnvoll, wo erhöhte Risiken für Kinder und Jugendliche bestehen, und können helfen derartige Risiken zum Beispiel durch spezielle Schutzeinstellungen für bestimmte Altersgruppen zu mitigieren. Die Festlegung von Altersbegrenzungen sollte risikobasiert erfolgen und sich an Art, Funktion und Nutzungskontext des jeweiligen Dienstes orientieren, etwa an Interaktionsmöglichkeiten, kommerziellen Anreizen oder sensiblen Inhalten. Wichtig ist, dass Altersgrenzen verhältnismäßig, verständlich und technisch umsetzbar sind und ausreichend Flexibilität bieten, um der Vielfalt digitaler Dienste und Geschäftsmodelle gerecht zu werden.

Altersbegrenzungen gehen einher mit Altersprüfungen. Eine altersangemessene Altersverifikation sollte sowohl den Schutz von Kindern und Jugendlichen als auch Datenschutz und Nutzerfreundlichkeit berücksichtigen. Zugleich sind Teilhabeaspekte zu berücksichtigen. Rechtlich und praktisch sinnvoll sind abgestufte Lösungen, die sich am jeweiligen Risikoniveau des Angebots orientieren. Dabei trägt ein grundsätzlich differenzierter Ansatz der Vielfalt digitaler Dienste und Nutzungskontexte Rechnung. Unterschiedliche Formen der Altersabsicherung – wie Altersschätzungen, Verifikationsverfahren oder token- bzw. walletbasierte Nachweise – können je nach Risiko und Nutzungskontext geeignet sein.

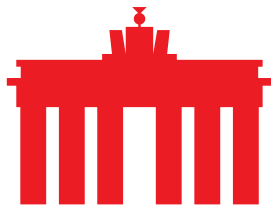
Dabei sollte der Grundsatz der Datenminimierung gelten, sodass nur so viele Altersinformationen erhoben werden, wie für den jeweiligen Zweck erforderlich sind. Entscheidend ist, dass Over-Collection personenbezogener Daten vermieden wird, Diskriminierungsrisiken berücksichtigt werden und Verfahren möglichst robust gegen einfache Umgehung sind.

Bei der Frage nach konkreten Vorgaben für spezielle Verfahren zur Altersprüfung besteht ein Spannungsfeld. Einerseits gibt es bestehende, bereits etablierte Verfahren und Infrastrukturen, auf die aufgebaut werden kann und die aufgrund ihrer Verbreitung und Bekanntheit nicht konterkariert werden sollten. Technologieneutrale Vorgaben sind dabei wichtig, da sie Schutzanforderungen definieren, ohne bestimmte technische Lösungen festzuschreiben, und es Anbietern ermöglichen, je nach Dienst und bestehender Infrastruktur unterschiedliche Verfahren einzusetzen. Klare Leitlinien können dazu beitragen, Innovation zu ermöglichen und gleichzeitig ein angemessenes Schutzniveau sicherzustellen. Andererseits können einheitliche Lösungsansätze zu einer besseren Akzeptanz und Nutzerfreundlichkeit der Verfahren führen.

Wichtig ist insgesamt, dass Altersverifikationslösungen für alle Beteiligten (Anbieter wie Nutzer:innen) praktikabel, barrierearm und für international tätige Anbieter konsistent umsetzbar sind.

Rund um das Thema Altersbegrenzungen bzw. Mindestalter gilt es zudem zu berücksichtigen, dass dem Wunsch der Eltern und Erziehungsverantwortlichen nach Mitbestimmung Rechnung getragen wird. Sie kennen ihre Kinder am Besten und sollten ein weitgehendes Mitspracherecht haben.

Schließlich darf auch nicht verkannt werden, dass digitale Dienste heutzutage auch bei der Informationsverschaffung und beim Lernen eine wichtige Rolle spielen. Dies gilt es bei der Frage eines Mindestalters ebenfalls zu berücksichtigen.



Neben der Frage nach einem Mindestalter für bestimmte digitale Dienste steht die Frage nach speziell gestalteten digitalen Räumen für Kinder und Jugendliche mit begrenztem oder ausgeschlossenen Zugang für Erwachsene.

Speziell gestaltete digitale Räume für Kinder und Jugendliche können ein sinnvoller Baustein des Jugendmedienschutzes sein, insbesondere bei interaktiven oder kommunikativen Angeboten. Einige Anbieter setzen solche Konzepte für altersgerechte Schutzräume bereits erfolgreich um. Solche Räume lassen sich technisch durch altersbezogene Konten, eingeschränkte Kontaktfunktionen, angepasste Inhalte und Default-Einstellungen umsetzen. Rechtlich und organisatorisch ist dabei wichtig, klare Verantwortlichkeiten, transparente Regeln und praktikable Zugangsmodelle zu schaffen, die die grundlegenden Schutzprinzipien wie Altersangemessenheit, Datenschutz und Einbeziehung von Eltern wahren und von international tätigen Anbietern konsistent umgesetzt werden können. Gleichzeitig sollte berücksichtigt werden, dass nicht alle Dienste oder Geschäftsmodelle gleichermaßen für getrennte Schutzräume geeignet sind und flexible Lösungen erforderlich bleiben.

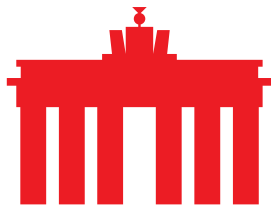
▪ Chancen, Teilhabe und spezielle Problemfelder

Digitale Dienste spielen eine wichtige Rolle für Bildung, Informationszwecke und Freizeitgestaltung von Kindern und Jugendlichen. Ein integrativer Schutz „by design“ kann hierbei altersgerechte Inhalte, sichere Interaktionsräume und transparente Hinweise auf problematische Inhalte ermöglichen. Er unterstützt Eltern, Lehrkräfte und pädagogische Fachkräfte dabei, Kinder die Nutzung digitaler Dienste heranzuführen und in der digitalen Welt zu begleiten. Technischer Jugendmedienschutz sollte aber nie der alleinige Ansatz sein, sondern sollte stets als ein Element des Jugendmedienschutzes verstanden werden. Zusätzlich bedarf es weiterer Maßnahmen oder Ansätze. Ein besonders wichtiges, weiteres Element des Jugendmedienschutzes ist die Vermittlung von Medienkompetenz.

Medienkompetenzförderung hilft Kindern, Risiken einzuschätzen, digitale Chancen zu nutzen und verantwortungsbewusst zu agieren. Gleichzeitig bleiben kreative Nutzung und Teilhabe an digitalen Angeboten möglich.

Medienkompetenz bzw. die Sensibilisierung vor und für bestimmte Gefährdungslagen ist ein wichtiger Baustein auch im Hinblick auf das Thema „übermäßiger Medienkonsum“. Aufklärung und Medienkompetenzförderung bei Kindern, Eltern und Lehrkräften unterstützen, gesunde Nutzungsgewohnheiten zu entwickeln. Unterstützend helfen Einstellungsmöglichkeiten oder Standardsettings bei Accounts für Kinder und Jugendliche (wie z.B. zeitliche Limits, optische Hinweise auf Nutzungsdauer und adaptive Empfehlungen) vor einem übermäßigem Nutzungsverhalten. Auch weitere Designentscheidungen der Anbieter können dazu beitragen, dass Interaktionsmechanismen nicht unbeabsichtigt zu übermäßigem Engagement führen.

Im Hinblick auf Sharenting oder Family/ Kinder-Influencing und einem damit einhergehenden Missbrauch von Bildern und personenbezogenen Daten kommt der Aufklärung und Sensibilisierung der Eltern, die Inhalte von Kindern ins Netz



stellen, eine zentrale Rolle zu. Sie müssen die damit verbundenen Risiken kennen bzw. besser erkennen und bewusst über das Teilen entscheiden.
Medienpädagogische Angebote für Kinder, Eltern und Lehrkräfte fördern zusätzlich die Kompetenz, Chancen und Risiken digitaler Medien einzuschätzen.

Über eco: Mit rund 1.000 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco das Internet maßgeblich mit, fördert neue Technologien, gestaltet Rahmenbedingungen und vertritt die Interessen der Mitglieder in Politik und internationalen Gremien. Die Schwerpunkte des Verbandes sind die Verlässlichkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit, Vertrauen und eine ethisch orientierte Digitalisierung. Deshalb setzt sich eco für ein freies, technologieneutrales und leistungsfähiges Internet ein.