

Stellungnahme

zum Hearing 2 der Unabhängigen Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt“

Berlin, den 12.02.2026

**game - Verband der
deutschen Games-Branche**

Friedrichstraße 165
10117 Berlin

www.game.de

Ansprechperson

Dr. Christian-Henner Hentsch
Leiter Recht &
Regulierung

T +49 30 2408779-22
henner.hentsch@game.de

Maren Raabe
Leiterin Politische
Kommunikation

T +49 30 2408779-15
maren.raabe@game.de

Stellungnahme zum Hearing 2: Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste

Das Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend hat am 03.09.2025 die Expertenkommission "Kinder- und Jugendschutz in der digitalen Welt" eingesetzt. Ziel der Kommission ist es, eine Strategie für den "Kinder- und Jugendschutz in der digitalen Welt" mit konkreten Handlungsempfehlungen für die zuständigen Akteure wie Bund, Länder und Zivilgesellschaft zu erarbeiten. Dazu hat die Kommission sechs Hearings geplant, wovon das zweite Hearing am 13.02.2026 den technischen Jugendmedienschutz, Plattformgestaltung und die Verantwortung digitaler Dienste in den Blick nimmt. Der game - Verband der deutschen Games-Branche ist als Sachverständiger geladen und bedankt sich für die Möglichkeit vorab schriftlich und im Hearing mündlich Stellung zu nehmen.

Der game - Verband der deutschen Games-Branche begrüßt die Einsetzung der Kommission und die umfassende Diskussion zum Schutz von Kindern und Jugendlichen in der digitalen Welt. Games-Unternehmen haben für ihre Angebote ein essenzielles Interesse am Schutz der jüngsten Nutzerinnen und Nutzer. Daher setzen wir uns schon immer für einen modernen, konvergenten und international anschlussfähigen gesetzlichen Jugendschutz ein. Viele der frühesten, innovativsten und vorbildlichsten inhaltlichen sowie technischen Jugendschutzlösungen stammen aus unserer Branche. Viele dieser Best-Practices werden von anderen digitalen Diensten übernommen und genutzt. Die Vielfalt der Lösungen spiegeln auch die Vielfalt der Angebote wider und macht deutlich, dass es für unterschiedliche Herausforderungen im Jugendschutz immer auch passgenaue Lösungen braucht - und bereits gibt.

Von größter Bedeutung ist im aktuellen Zusammenhang allerdings die klare Unterscheidung von Games auf der einen und Sozialen Medien auf der anderen Seite. Insbesondere der Jugendschutz bei Games ist in Deutschland weitgehend und differenziert im Jugendschutzgesetz reguliert. Vergleichbar zum Film arbeiten Wirtschaft sowie Bund und Länder eng im Rahmen der Freiwilligen Selbstkontrolle USK zusammen, unterstützt von unabhängigen Fachgremien. Die altersdifferenzierten Kennzeichen USK 0, 6, 12, 16 und 18 gehören zu den bekanntesten und erfolgreichsten Jugendschutzmaßnahmen. Auf Games-Plattformen werden diese konsequent genutzt und sind mit ebenso bekannten wie erfolgreichen Jugendschutzprogrammen im Zusammenwirken nutzbar. Seit der Novelle des Jugendschutzgesetzes werden auch Interaktionsrisiken wie Kaufmöglichkeiten, Standortweitergabe, Exzessive Nutzung, Glücksspiel oder Lootboxen effektiv und altersdifferenziert berücksichtigt. Diese führen seitdem sowohl zu Deskriptoren, die der Transparenz und Information dienen, als auch zu erhöhten Alterseinstufungen. Dieser über

Jahrzehnte gewachsene und immer weiterentwickelte Ansatz in Deutschland ist weltweit einzigartig und wird beispielsweise auf europäischer Ebene derzeit als Vorbild genommen. Für eine sachgerechte Diskussion ist daher die spezifische Situation im Games-Bereich trennscharf von anderen Bereichen wie Sozialen Medien zu differenzieren. Dies gilt umso mehr, als dass bei Games die maßgeblichen Inhalte immer direkt durch den Anbieter bereitgestellt werden und nicht durch Dritte. Angesichts von Vorhaben auf europäischer Ebene wie insbesondere dem Digital Fairness Act scheint zudem sinnvoll, Diskussionen zur Weiterentwicklung auf nationalstaatlicher Ebene in diesem Kontext zu denken. Hier empfehlen wir, die sehr guten Erfahrungen im Jugendschutz für Games in Deutschland in die Gespräche einzubringen, um für bereits erprobte und funktionierende Lösungen zu werben.

Wir sind der Verband der deutschen Games-Branche. Unsere Mitglieder sind Entwickler, Publisher und viele weitere Akteure der Games-Branche wie Esport-Veranstalter, Bildungseinrichtungen und Dienstleister. Als Mitveranstalter der gamescom verantworten wir das weltgrößte Event für Computer- und Videospiele. Wir sind zentraler Ansprechpartner für Medien, Politik und Gesellschaft und beantworten Fragen etwa zur Marktentwicklung, Spielekultur und Medienkompetenz und natürlich auch zum Kinder- und Jugendmedienschutz in Games. Unsere Mission ist es, Deutschland zum besten Games-Standort zu machen. Ein funktionierender und passgenauer Jugendschutz ist die Voraussetzung dafür, dass alle Spielerinnen und Spieler Games nutzen und Spaß daran haben können.

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?

I. Risiken, Schutzmaßnahmen und Gestaltung digitaler Dienste

In Deutschland werden Kinder und Jugendliche zum Schutz ihrer persönlichen Integrität bei der Mediennutzung im Vergleich zu anderen Ländern besonders geschützt. Seit Inkrafttreten der Reform des Jugendschutzgesetzes am 01.05.2021 werden alle Games vor dem Markteintritt von der ko-regulierten Selbstkontrollereinrichtung „Unterhaltungssoftware Selbstkontrolle“ (USK) auch auf so genannte Interaktionsrisiken wie Kommunikation mit anderen Spielern (Chats), unkontrollierte Käufe im Spiel, Glücksspielähnliche Mechanismen wie Lootboxen, Glücksspiel oder das Versenden von Standortdaten geprüft. Je nach Risiko führen diese Risiken dazu, dass Spiele ein höheres USK-Alterskennzeichen erhalten, wenn die technischen Jugendschutzeinstellungen, wie Kommunikations- oder Kauffunktionen, nicht durch geeignete Vorsorgemaßnahmen (§ 24a JuSchG) begegnet wird und beispielsweise In-Game-Käufe ausgeschaltet werden können. Zusätzlich sorgen Deskriptoren für Transparenz, indem sie alle möglichen Risiken zusammen mit dem Alterskennzeichen kenntlich machen (z.B. „Enthält: In-Game-Käufe“). Die USK informiert Familien auf ihrer Website und über viele andere Formate über diese Risiken und gibt Tipps für einen sicheren Umgang mit Games; beispielsweise mit dem Elternratgeber für digitale Spiele „Games? Na sicher!“.

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:

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

Games werden vor Veröffentlichung bei der Alterskontrolle auf jugendgefährdende und jugendbeeinträchtigende Inhalte geprüft. Sofern es ungeeignete, aber rechtlich zulässige Inhalte gibt, schützt das Alterskennzeichen Kinder und Jugendliche seit vielen Jahren sehr bewährt davor. Spiele mit rechtlich unzulässigen Inhalten erhalten kein Kennzeichen und werden in der Regel indiziert und sind damit sogar strafrechtlich verboten. Cybergrooming, Sextortion und Missbrauchsdarstellungen sind ein neuartigeres Phänomen, das laut Studiendaten vor allem in Social Media und Telekommunikationsdiensten eine Rolle spielt.

Für Chats im Games-Bereich sorgen unter anderem Filter-, Blockier- und Meldesysteme für Prävention.

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

Die Geschäftsmodelle in der Digitalwirtschaft und der Games-Branche haben sich in den vergangenen zwei Jahrzehnten stark verändert. Zu dem vorherrschenden Geschäftsmodell des Vertriebs von Games aus den Anfangszeiten, dem klassischen Verkauf einzelner Spiele, sind im Laufe der Jahre weitere hinzugekommen. Die hohe Verfügbarkeit schneller Internetverbindungen hat dazu geführt, dass Spiele oftmals online angebunden werden und so auch nach Veröffentlichung mit neuen Inhalten noch lange spielbar bleiben. Zur Finanzierung langer Verfügbarkeiten und stetiger Aktualisierungen bieten Publisher oft Zusatzinhalte an, für die Anbieter dann teilweise im Rahmen von In-Game- und In-App-Käufen Geld verlangen. Anbieter erzielen heutzutage einen maßgeblichen Teil ihres Umsatzes mit sogenannten In-Game- und In-App-Käufen, die ganz unterschiedlich ausgestaltet sind, oftmals jedoch nicht erforderlich sind für ein Vorankommen im Spiel. Diese unterschiedlichen Monetarisierungsmodelle und die damit verbundene Wahlmöglichkeit wird von den Spielerinnen und Spielern begrüßt: Solange es eine aktive Community zu einem Spiel gibt, werden aufgrund dieser zusätzlichen Monetarisierungsmöglichkeit in der Regel auch neue Inhalte zu diesem Spiel erstellt. Spielerinnen und Spieler können zudem entscheiden, welche Spieleinhalte ihnen einen gewissen Geldbetrag wert sind und auf andere verzichten, anstatt einen höheren Betrag für ein Gesamtpaket zu zahlen. Games, die eine aggressive Monetarisierungsstrategie verfolgen, ernten von den Spielerinnen und Spielern häufig deutliche Kritik, so dass die Spiele nicht angenommen werden und wirtschaftlich schlicht nicht erfolgreich sein können, solange nicht entsprechende Anpassungen vorgenommen werden.

Käufe von In-Game-Content und Lootboxen werden in der allgemeinen Debatte häufig vermengt. Lootboxen sind Überraschungspakete, die virtuelle Gegenstände oder Zusatzinhalte enthalten und in jedem Spiel, in dem diese Mechanik zum Einsatz kommt, individuell gestaltet sind. Inhalte aus Lootboxen sind für das Vorankommen in einem Spiel generell nicht erforderlich, sie sind also freiwillig und in vielen Fällen rein dekorativ. Den möglichen Inhalt kennen die Spieler vor dem Öffnen, die exakte Zusammensetzung ist ihnen hingegen vorab nicht bekannt. Die Ergebnisse einer aktuellen Umfrage verdeutlichen, dass Lootboxen trotz ihrer Nicht-Erforderlichkeit für den Verlauf eines Spieles eine bedeutende Rolle für viele Spieler haben und das Spielerlebnis bereichern können. 84% der Befragten geben an, dass ihnen die Möglichkeit zur Beschleunigung des Spielfortschritts durch Lootboxen wichtig ist. Darüber hinaus schätzen 82 Prozent der Befragten die Freude an der Überraschung beim Auspacken der Lootboxen. Lootboxen sind für die allermeisten

Spielerinnen und Spieler kein entscheidendes Motivationselement ein Spiel zu spielen. Nur ein Bruchteil der Umsätze entfällt auf Lootboxen. Nach einer Studie von Ipsos für Deutschland, Frankreich, Spanien, das Vereinigte Königreich und Italien haben nur 3,8 Prozent der Spieler zwischen 11 und 64 Jahren echtes Geld für Lootboxen verwendet, 96,2 Prozent haben dies nicht getan.

Seit 2019 haben sich die Konsolenhersteller Xbox, PlayStation und Nintendo verpflichtet, dass alle Spiele auf ihren Plattformen, die kostenpflichtige Zufallsgegenstände enthalten, die Wahrscheinlichkeiten für den Erhalt eines kostenpflichtigen Zufallsgegenstands angeben müssen (Drop rate disclosure). Im Google Play Store wurde diese Regelung ebenfalls 2019 eingeführt. Bei Apple bereits im Jahr 2017. Zudem muss die Wahrscheinlichkeiten für alle Spieler gleich sein, dass zufällige Gegenstände ohne nachteilige Manipulation aufgrund einer unfairen Verarbeitung personenbezogener Daten und in Übereinstimmung mit den geltenden Datenschutzgesetzen verteilt werden und dass die Bezahlung für zufällige Gegenstände niemals für den Spielfortschritt erforderlich ist (pay-to-win/pay-to-play).

Die USK hat diese Überlegungen auf Grundlage des novellierten Jugendschutzgesetzes in ihr Altersfreigabeverfahren integriert. Gemäß ihrer Bewertungspraxis können spielähnliche Mechanismen wie Lootboxen oder zufallsbasierte Belohnungssysteme die persönliche Integrität von Kindern und Jugendlichen beeinträchtigen. Eine transparente Darstellung der Wahrscheinlichkeiten für den Erhalt bestimmter Gegenstände wird daher im Rahmen der Altersbewertung positiv berücksichtigt. In die Bewertung durch die USK fließen zudem weitere Vorsichtsmaßnahmen ein: altersdifferenzierte Ausgabenobergrenzen, eine klare und nachvollziehbare Darstellung von Käufen und Gesamtausgaben, die Bereitstellung von Kostenvoranschlägen, wirksame Funktionen zur elterlichen Kontrolle sowie ein Spieldesign, das einen vollständigen Spielverlauf auch ohne Inanspruchnahme solcher Mechanismen ermöglicht. Diese Elemente werden bei der Festlegung der Altersfreigabe als relevant angesehen und entsprechend berücksichtigt.

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

Im Gegensatz zu Sozialen Netzwerken sind Kommunikationsmittel in und um Games Mittel zum Spielzweck, nicht Kern der Nutzung. Sie bleiben durch viele Nutzerinnen und Nutzer ungenutzt oder vollständig deaktiviert. Die Chat-Funktionen in Online-Spielen – ob gesprochen oder geschrieben – dienen den Spieler-Teams zur Absprache und damit der Individualkommunikation. Sie finden über Texteingabe oder auch via Headset und Sprach-Chat statt. Diese Chats sind im Vergleich zu anderen Kommunikationstools wie Messenger-Diensten oder Online-Foren aufgrund ihrer Funktionsweise ungeeignet für eine weite Verbreitung von Inhalten jeglicher Art oder einen Austausch, der über das parallele

Spielgeschehen hinausgeht. Die gesprochenen oder geschriebenen Inhalte sind nur über kurze Zeiträume überhaupt verfügbar. Außerdem ist die Anzahl derjenigen, denen sie überhaupt zur Kenntnis gelangen können, überschaubar gering. Kommunikation in Games eignet sich daher auch nicht für die Kommunikation über und Verbreitung von verschwörungsideologischen oder extremistischen Inhalten. Aus diesen Gründen sind Games klar zu unterscheiden von Sozialen Medien oder auch Diskussions-Foren, die selbst wenn bei ihnen im Einzelfall Games-Themen im Fokus stehen, jedoch gerade keine Games sind.

Sofern Chats oder Kommunikations- und Kontaktfunktionen in Games vorhanden sind, warnt die USK im Rahmen der Alterskennzeichnung mit Deskriptoren vor „Chats“ oder „Erhöhten Kommunikationsrisiken“ und schafft damit bei jedem Spiel Transparenz. Bei höherer Relevanz werden die vergebenen Alterskennzeichen erhöht. In der Regel werden vom Anbieter als Vorsorgemaßnahmen Wortfilter, Blockierfunktionen und/oder Meldemöglichkeiten für problematische Inhalte bereitgehalten. In manchen Fällen gibt es auch eine Moderation durch menschliche Community-Manager. Daneben kommen elterliche Begleittools zur Deaktivierung oder Beschränkung der Kommunikation auf bestimmte Kontakte zum Einsatz. Es können auch Einstellungen vorgenommen werden, um gegebenenfalls die Weitergabe von Klarnamen, Standortdaten und weiteren persönlichen Informationen auszuschließen. Bei der Kommunikation auf Plattformebene gibt es entsprechende Sicherheits- und Moderationseinstellungen. Spielmechanische Belohnungen oder wiederholte Aufforderungen zur Preisgabe hochsensibler persönlicher Daten, die eine Kontaktaufnahme oder missbräuchliche Nutzung ermöglichen, sind selbstverständlich ausgeschlossen.

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

Wie oben beschrieben, findet in den meisten Spielen nur eine eingeschränkte Kommunikation statt. Insofern sind Doxing, Stalking oder koordinierte Angriffe hier nicht verbreitet. Die Frage zielt wohl eher auf Social Media und Telekommunikationsdienste ab.

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

Wie oben beschrieben, findet in den meisten Spielen nur eine eingeschränkte Kommunikation statt. Insofern sind Selbstschädigung/Suizid, Essstörungen, gefährliche Challenges nicht verbreitet. Die Frage zielt auf Social Media und Telekommunikationsdienste ab. Im Umfeld von Games gibt es in der Regel Community-Manager, die in Foren und sozialen Medien auf den Umgangston achten und gegebenenfalls

einschreiten. Dies dient einerseits der Bindung der Spielerinnen und Spieler, verhindert aber vor allem eine toxische Spielumgebung, die ein Abwandern der Spielerinnen und Spieler nach sich ziehen könnte.

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

Geschäftspraktiken, die auf die Schwachstellen der Verbraucher abzielen, sind nach dem Gesetz gegen unlauteren Wettbewerb (UWG) und der zugrundeliegenden Richtlinie über unlautere Geschäftspraktiken ausdrücklich verboten. Darüber hinaus schreibt die DSGVO strenge Regeln für automatisierte individuelle Entscheidungen vor, einschließlich Profiling, die rechtliche oder ähnlich bedeutende Auswirkungen auf die betroffene Person haben. Darüber hinaus sind solche Praktiken im Rahmen des Gesetzes über digitale Dienste in Bezug auf die Transparenz von Werbung (Artikel 26 und 38) oder in Bezug auf den Schutz Minderjähriger (Artikel 28) bereits geregelt bzw. verboten. Darüber hinaus sind Unternehmen durch Gesetze und Regulierungsvorschriften verpflichtet, sicherzustellen, dass ihre Werbung nicht nur legal, anständig, ehrlich und wahrheitsgemäß ist (für ihr gesamtes Publikum), sondern auch nicht die Leichtgläubigkeit oder Unerfahrenheit von Kindern ausnutzt, die mit ihren Werbeinhalten interagieren. Insbesondere irreführende Werbung ist nach § 5 UWG verboten.

Games verarbeiten bei jeder Spiel-Session zwar viele Daten der – auch minderjährigen – Spielerinnen und Spieler. Dies erfolgt in der Regel auf der Grundlage des Nutzungsvertrages, der selbstverständlich alle Nutzungen aufführt. Die Daten werden zur Verbesserung des Spielerlebnisses und zur Weiterentwicklung des Spiels meist anonymisiert weiterverarbeitet. Profiling und Tracking findet in aller Regel nicht statt. Games sind ganz überwiegend nicht durch Werbung finanziert, sondern durch Käufe und In-Game-Käufe oder Abo-Modelle, so dass sich bei Games nicht die gleichen Fragen stellen wie bei webefinanzierten Diensten.

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

Die Gestaltungsentscheidungen von Games-Anbietern werden seit der letzten JuSchG-Novelle als Risiken für die persönliche Integrität im Rahmen der Alterskennzeichnung überprüft und spielen eine ganz erhebliche Rolle für deren Alterseinstufung. Ohne eine Alterskennzeichen können Spiele in der Regel im Handel oder auf den relevanten Plattformen nicht vertrieben werden.

Nach den Leitkriterien der USK können dauerhaft im Spiel angelegte Funktionalitäten insbesondere in den folgenden Fällen die geistig-seelische Integrität oder das psychische Wohlbefinden nachhaltig beeinträchtigen und daher zu einer erhöhten Alterskennzeichnung führen:

- Beeinträchtigungen der Identitätsfindung, inneren Autonomie oder individuellen Meinungsbildung durch übermäßige Anreize, Druckmechanismen oder manipulative Handlungsvorgaben.
- Einfluss auf Geltungsansprüche in Gemeinschaften, Identitäts- und Beziehungsmanagement, etwa durch Ranglisten, Wettbewerbsdruck oder soziale Ausschlussmechanismen.
- Einschränkung der Entscheidungsfreiheit oder kommerziellen Autonomie durch intransparente Kaufoptionen, Lootboxen, Pay-to-Progress-Mechanismen oder Glückspiel-Imitationen.
- Gefährdung der sexuellen Selbstbestimmung durch ungesicherte Kommunikations- oder Sharing-Funktionen.

Die Spruchpraxis der letzten Jahre hat gezeigt, dass ca. 30 Prozent der geprüften Games potenzielle Nutzungsrisiken enthalten. Bei rund einem Drittel der Fälle resultierte aus dem konkreten Risiko eine höhere Alterskennzeichnung. In den anderen Fällen waren die entlastenden Vorsorgemaßnahmen ausreichend. Die Einbeziehung der Interaktionsrisiken in den Prozess der Alterskennzeichnung trägt dazu bei, dass Anbieter systematisch Vorsorgemaßnahmen bereitstellen. Gleichzeitig sorgen die Deskriptoren für die nötige Transparenz und ermöglichen es Eltern, die Risiken zu erkennen und bei den Kindern und Jugendlichen zu adressieren. Im Ergebnis gibt diese präventive Risikobewertung flankierenden Schutz, ohne die digitale Teilhabe der Kinder und Jugendlichen über Gebühr einzuschränken.

Im Übrigen enthält Abschnitt 6.3.1 der Leitlinien zu Artikel 28 Absatz 4 DSA äußerst detaillierte und präskriptive Formulierungen dazu, was die EU-Kommission als obligatorische Standardeinstellungen (mandatory default settings) betrachtet. So wie er formuliert ist, liest sich die Liste eher wie eine Vorschrift für obligatorische Produktmerkmale als nur für Einstellungen in Bezug auf ansonsten bereits vorhandene Merkmale. Dies würde die Leitlinien weit über den Wortlaut des DSA hinaus ausdehnen und wirft Fragen hinsichtlich des Umfangs der Regelungsbefugnis auf, die Art. 28 Abs. 4 der EU-Kommission tatsächlich überträgt. Beispielsweise impliziert die Liste der erforderlichen Standardeinstellungen die Existenz von Screenshot-Blockern oder detaillierten Nachrichten- und Benachrichtigungseinstellungen, die nicht näher bezeichnete „Kernschlafzeiten“ von Minderjährigen berücksichtigen (ohne jedoch Angaben dazu zu machen, welche Schlafenszeiten die EU-Kommission für welches Alter als angemessen erachtet).

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

Nach der KI-Verordnung sind Systeme verboten, die Schwachstellen aufgrund des Alters ausnutzen.

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

Die Wirksamkeit der bestehenden Maßnahmen wird aktuell im Rahmen der Evaluation des novellierten Jugendschutzgesetzes umfassend überprüft. Ergebnisse sind noch in diesem Jahr zu erwarten. Auf Grundlage der bisherigen Erfahrungen der beteiligten Stakeholder ist jedoch bereits wahrzunehmen, dass die erfolgten Weiterentwicklungen sehr erfolgreich zu greifen scheinen und von Eltern gut angenommen werden.

Wie bereits geschildert, gibt es bereits zahlreiche Regulierungen und Verbote zum Schutz von Kindern und Jugendlichen. Die meisten Games halten diese Regeln ein und sind an einer spielerfreundlichen, nicht-toxischen Spielumgebung interessiert. Es gibt aber natürlich immer vereinzelte „schwarze Schafe“, insbesondere aus dem Ausland. Aber auch in der EU gibt es Anbieter, die aufgrund des Herkunftslandprinzips die deutschen Regelungen zum Jugendschutz nicht oder nur unzureichend beachten. Dies macht deutlich, dass es teilweise kein Regulierungs-, sondern ein Vollzugs- oder Durchsetzungsdefizit gibt und dass nationalstaatliche Regelungen in ihrer Wirkung limitiert sind. Weitere Regelungen werden den „Wettbewerbsvorteil durch Rechtsbruch“ noch weiter verstärken und könnten auch zur Abwanderung oder Abkehr weiterer Anbieter führen. Zudem arbeitet die EU derzeit an einem Digital Fairness Act (DFA), der neue Regelungen zum Minderjährigenverbraucherschutz und insbesondere auch zu Dark Patterns und Lootboxen vorsieht. Hier ist das BMBFSFJ gefragt, seine deutsche Perspektive im Jugendmedienschutz einzubringen und sicherzustellen, dass das geplante europäische Minderjährigenverbraucherschutzrecht das deutsche Jugendschutzrecht nicht überlagert. Die regulierte Selbstregulierung und auch die neuen Regelungen des JuSchG zu Interaktionsrisiken haben sich aus Sicht der Games-Branche bewährt und sollten unbedingt erhalten bleiben. Wir glauben, dass erfolgreiche deutsche Regelungen sogar Blaupause für den DFA und andere Mitgliedstaaten sein können.

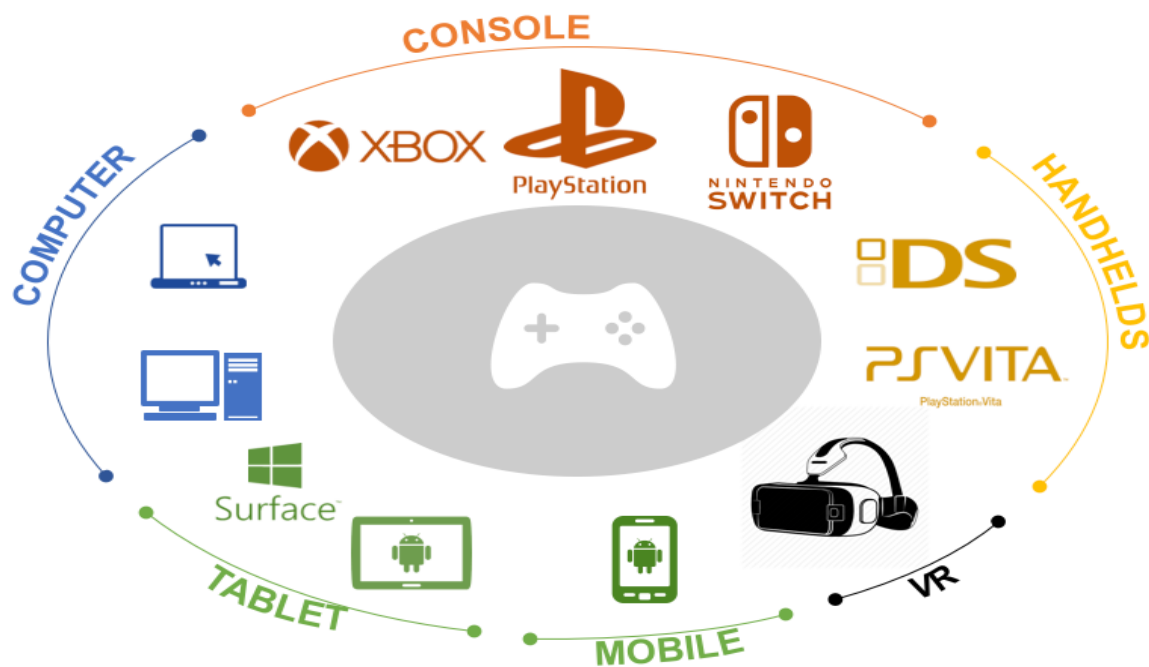
Die Top-3-Maßnahmen sollten in Hinblick auf Games also weniger zusätzliche Regelungen zu den vielen bestehenden sein, sondern vielmehr in der Abstimmung der bestehenden und kommenden Regelungen auf deutscher und EU-Ebene bestehen, um einen modernen,

konvergenten und international anschlussfähigen gesetzlichen Jugendschutz zu gewährleisten.

II. Plattformverantwortung, Regulierung und Durchsetzung

Aus Sicht der Games-Branche ist grundsätzlich zwischen dem Spiel und der Plattform, auf der es angeboten wird, zu unterscheiden. Als Plattform kann zwischen den Marktplätzen für PC-Spiele (z.B. Epic, Steam, GoG), Spielekonsolen (z.B. Nintendo Switch, Playstation, Xbox) und den mobilen Plattformen (z.B. Apple Store und Google Play Store) differenziert werden. In manchen Fällen (z.B. Roblox) kann auch ein Spiel zur Plattform werden, wenn Spielerinnen und Spieler Inhalte im Spiel hochladen können. Dies ist aber die Ausnahme, denn das Spielgeschehen wird in der Regel – gerade aus jugendschutzrechtlichen Gründen – von Publisher kuratiert und kontrolliert. Sofern ein Spiel einen Chat enthält, wird es dadurch noch nicht zur Plattform im Sinne des DSA (so genannter ancillary service). Jugendschutzrechtlich werden bei Chats jedoch Vorsorgemaßnahmen nach § 24a JuSchG implementiert.

Neben den originären Games-Plattformen gibt es auch Plattformen, die die um Games herum genutzt werden, wie Discord, Twitch, YouTube und Reddit. Dabei handelt es sich nicht um Games oder Games-Plattformen, da sie in erster Linie soziale Kontakte, Livestreaming, die Erstellung von Inhalten und das Engagement in der Community ermöglichen. Einige der folgenden Fragen zielen wohl vor allem auf diese Kommunikations-Plattformen und die damit verbundenen Gefahren bei Social Media ab, die aufgrund der soeben beschriebenen organisatorischen und technischen Besonderheiten bei Games nicht einschlägig sind.



- 1. Wie sollte die Verantwortung der Plattformbetreiber gegenüber Kindern und Jugendlichen rechtlich und praktisch konkretisiert werden (z.B. Sorgfaltspflichten, Risikoanalysen, Melde- und Abhilfewege, Transparenzpflichten)?**

Der DSA sieht in Art. 28 bereits verbindliche und europaweit harmonisierte Pflichten für Plattformen gegenüber Kindern und Jugendlichen vor. Derzeit konkretisiert die EU-Kommission mit Leitlinien die weiteren Pflichten und vor allem auch mit Positivbeispielen.

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

Auch hier gibt es nach dem DSA ausführliche Pflichten für Audits, Reporting und Aufsicht.

- 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?**

Bei der Umsetzung der bestehenden Vorschriften und der Leitlinien im deutschen Jugendschutzrecht kommt es vor allem auf die Prüfung der Games durch die Selbstkontrollereinrichtung – für Games also die USK – an. Hier hat der neue JMStV bereits einige Änderungen und auch Verbesserungen gebracht.

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

Zur Verbesserung des technischen Kinder- und Jugendmedienschutzes wären insbesondere folgende Maßnahmen denkbar:

- Eine Integration der freiwilligen Selbstkontrollen in den EU-Rechtsrahmen, um sie auch gegenüber dem DFA abzusichern.
- Eine gesetzessystematische Stärkung von qualitativ hochwertigen Alterskennzeichen, die im Rahmen pluralistischer Kennzeichnungsverfahren entstehen, gegenüber einfacher Anbieterkennzeichnungen.
- Eine Schaffung zusätzlicher gesetzlicher Anreize zur Kooperation mit Selbstkontrollereinrichtungen (insbesondere der den Anbieter privilegierende Ansatz des sog. Vorbefassungsschutzes für Mitglieder einer Selbstkontrollereinrichtung nach § 20 Abs. 5 JMStV im Rahmen einer Selbstverpflichtung).
- Eine ausdrückliche Berücksichtigung und Verortung von Alterskennzeichen sowie Deskriptoren wie sie für Spieleplattformen im Rahmen der Kennzeichnungspflicht nach § 14a JuSchG festgelegt sind, als Vorsorgemaßnahme auf Online-Plattformen sowie effektive Instrumente zur Durchsetzung in Verknüpfung mit Privilegierungen im Rahmen der regulierten Selbstregulierung.
- Eine gesetzlich normierte Einbindung von Selbstkontrollereinrichtungen bei „dialogischen Verfahren“ des Digital Services Coordinators in Bezug auf Mitglieder von Selbstkontrollereinrichtungen.
- Eine ausdrücklichere Berücksichtigung von Elternbegleittools als zentrale Schutzmaßnahmen. Diese stellen die Basis jeglicher Jugendschutzeinstellungen und Filterfunktionen dar. Auch Altersfeststellungen sind von solchen Einstellungsfunktionalitäten abhängig.
- Stärkung und Schaffung von Anreizen für präventive Ansätze, z.B. im Rahmen von Zertifizierungen und Anerkennungen technischer Maßnahmen, insbesondere bei Selbstkontrollereinrichtungen.
- Eine klare EU-weite Definition der „Altersverifikation“, um Rechtsunsicherheiten und national unterschiedliche Interpretationen auszuschließen.

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?

Ende-zu-Ende-Verschlüsselung (E2EE) schützt in der Regel Kommunikationsdaten (Chat, Voice) direkt zwischen Nutzern, sodass Dritte nicht mitlesen können. Chats in Spielen sind aber in aller Regel öffentlich, beispielsweise, um für eine Aufgabe andere Team-Mitglieder anzusprechen und anschließend die Quest gemeinsam zu lösen. Die Frage zielt wohl eher auf Social Media oder Telekommunikationsdienste ab.

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?

Der im Dezember 2025 in Kraft getretene JMStV beinhaltet auch neue Regelungen für Betriebssysteme und App-Stores. Diese Regelungen sind mit Blick auf die DSA-Verordnung wohl europarechtswidrig. Der DSA zielt auf eine Vollharmonisierung, so dass die in ihr enthaltenen Regelungen abschließend sind. Ergänzende nationale Regelungen zu denselben Regelungsgegenständen sind damit nicht zulässig. Auch eine lediglich wiederholende oder rekurrierende Definition ist nicht zulässig.

Außerdem haben die Länder nicht im erforderlichen Umfang die Bedeutung der Dienstleistungs- und Warenverkehrsfreiheiten als Grundpfeiler des europäischen Binnenmarkts berücksichtigt. Hierzu gehört unter anderem das Herkunftslandprinzip, wonach Mitgliedstaaten der Europäischen Union den freien Verkehr von Diensten der Informationsgesellschaft aus anderen Mitgliedstaaten nicht aus Gründen einschränken dürfen, die in den koordinierten Bereich der Richtlinie 2000/31/EG fallen. Die nun vorgeschlagene Novellierung verkennt weiterhin, dass es den Staatsvertragsgebern verwehrt ist, generell-abstrakte Maßnahmen zu erlassen, die auf in anderen Mitgliedsstaaten niedergelassene Dienste der Informationsgesellschaft Anwendung finden sollen. Es ist unionsrechtswidrig, Anbietern aus anderen EU-Mitgliedsstaaten unmittelbare Pflichten aufzuerlegen. Dies ergibt sich auch aus dem Urteil des EuGH vom 09.11.2023. Faktisch dürfte der JMStV daher auf Digitale Dienste mit EU-Sitz außerhalb Deutschlands keine Anwendung finden.

Grundsätzlich ist eine Inländerdiskriminierung, also eine Beschränkung des Anwendungsbereichs auf in Deutschland sowie in Drittstaaten niedergelassene Anbieter, möglich. Allerdings gibt es derzeit keine Betriebssysteme und App-Stores für Games mit Sitz in Deutschland. Im Übrigen ist zu berücksichtigen, dass gerade bei Games, die immer international vertrieben werden, eine solche Maßnahme zu einem unverhältnismäßigen Standortnachteil für in Deutschland niedergelassene Anbieter führt. Insofern werden Anbieter auch künftig bewusst den „europäischen Ausweg“ suchen, um sich dem deutschen Jugendschutzsystem zu entziehen.

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

Games-Anbieter haben ein großes Interesse an einem modernen, konvergenten und international anschlussfähigen gesetzlichen Jugendschutz. Auch wenn 80 Prozent der Spielenden in Deutschland Erwachsene sind, so sind Games doch ein Medium für die ganze Familie. Vor diesem Hintergrund werden mit dem Jugendschutz möglicherweise verbundene wirtschaftliche und betriebliche Implikationen in der Regel proaktiv angenommen und als Investment in eine sichere Spielumgebung betrachtet. Als belastend wird jedoch empfunden, dass im Spannungsverhältnis zwischen Bund und Ländern – und nun auch der EU – Kompetenzstreitigkeiten auf dem Rücken der Branche ausgetragen werden. Es wird von der Branche erwartet, dass die verantwortlichen Gesetzgeber einheitliche und umsetzbare Vorgaben machen, die sich nicht widersprechen oder zu übertrumpfen versuchen. Zusätzlich kommt eine Konkurrenz einer Vielzahl an zuständigen Behörden und Stellen hinzu, die im Kompetenzkampf Verunsicherung verursachen. Weil Games stets weltweit vertrieben werden, müssen die politischen Wünsche und Vorstellungen vieler Länder und Institutionen gleichzeitig umgesetzt werden. Nicht der Jugendschutz an sich oder die Vorsorgemaßnahmen sind die entscheidenden wirtschaftlichen Implikationen, sondern die hohen Kosten durch die sehr unterschiedlichen, ständig wechselnden und sich teils widersprechenden gesetzlichen Vorgaben.

III. Altersgrenzen, Altersverifikation und spezifische Schutzräume

Kinder haben nach Art. 17 der UN-Kinderrechtskonvention das Recht auf einen adäquaten Zugang zu Massenmedien. Die Vertragsstaaten erkennen in Art. 31 zudem das Recht des Kindes auf Freizeit, auf Spiel und altersgemäße aktive Erholung sowie auf freie Teilnahme am kulturellen und künstlerischen Leben an. Digitale Spiele nehmen hier als jugendkulturelles Massenphänomen eine besondere Rolle ein und bilden einen wichtigen Bestandteil der Freizeitbeschäftigung von Kindern, Jugendlichen sowie Erwachsenen. Games eröffnen Erlebnisräume, machen Medieninhalte selbst erfahrbar, knüpfen häufig an den Interessensgebieten von Kindern und Jugendlichen an und nehmen eine große Rolle in der Peergroup ein. Die Vielfalt der Spielkultur zeigt sich auf unterschiedliche Arten: So lädt

sie junge Menschen dazu ein, ihren eigenen Interessen nachzugehen, ihre Persönlichkeiten zu entwickeln, Kreativität auszuleben sowie Teil von Communitys zu werden. Da digitale Spiele in hohem Maße Teilhabe und Freizeitgestaltung ermöglichen, erfüllen sie insbesondere für Heranwachsende mit Behinderungen vielfältige Funktionen bei ihrer Persönlichkeitsentwicklung. Selbstverständlich müssen Kinder und Jugendliche auch vor den Gefahren geschützt werden. In der Abwägung der Maßnahmen muss jedoch stets zwischen dem Recht auf Teilhabe und der Schwere der Gefahr des jugendgefährdenden oder jugendbeeinträchtigenden Inhalts abgewogen werden, so wie dies im novellierten Jugendschutzgesetz ausdrücklich getan wird.

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

Eine pauschale Altersgrenze für bestimmte digitale Angebote ist weder rechtlich zulässig noch pädagogisch sinnvoll. Sowohl mit Blick auf die UN-Kinderrechtskonvention als auch wegen des Erziehungsrechts der Eltern in Art. 6 Abs. 2 GG ist ein solch pauschales Verbot mangels Abwägung unverhältnismäßig. Zudem sind Plattformen durch den DSA vollharmonisierend reguliert, so dass für nationale Alleingänge eigentlich kein Spielraum bleibt. Zudem wäre ein solches Verbot wegen des Herkunftslandprinzips bzw. dem Free Flow of Information gegenüber digitalen Diensten, die ihren Sitz in einem anderen EU-Mitgliedstaat haben gar nicht durchsetzbar.

Für die Games-Branche würde eine pauschale Altersgrenze das ausdifferenzierte Jugendschutzsystem der regulierten Selbstregulierung auf einen Schlag hinfällig machen. Je nach Altersgrenze würden alle darunter liegenden Altersgrenzen entfallen. Für Games-Anbieter gäbe es keine Anreize mehr, Jugendschutz im Game-Design mitzudenken oder Vorsorgemaßnahmen anzubieten. Auch die Akzeptanz des Jugendschutzrechts würde unter einem solchen Pauschalverbot leiden und viele Spielerinnen und Spieler würden – womöglich sogar mit Billigung oder gar Unterstützung ihrer Eltern – Umgehungen in andere Länder nutzen wie bspw. über eine VPN-Verbindung. Im Ergebnis gäbe es also weniger Jugendschutz statt mehr.

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

In der Praxis der Games-Branche geht es bei der Altersverifikation (Age Verification) um ein System, das sich auf harte (physische) Identifikatoren und/oder verifizierte Identifikationsquellen stützt, die ein hohes Maß an Sicherheit bei der Bestimmung des Alters eines Nutzers bieten. Damit kann die Identität eines Spielers oder einer Spielerin sicher

festgestellt werden. Die Feststellung, ob der Nutzer zu dem bestimmten Zeitpunkt auf genau diesen Dienst zugreifen darf, kann aber auch anonym über einen Dritten erfolgen, ohne personenbezogene Daten an den Anbieter weiterzugeben. Sofern eine echte Altersverifikation gewünscht ist, auch als „highly effective age assurance“ bezeichnet, müsste sie folgende Anforderungen erfüllen:

- Genauigkeit, d. h. die Fähigkeit, ein genaues Alter oder eine genaue Altersspanne zu bestimmen.
- Zuverlässigkeit, d.h. die Fähigkeit, unter realen Bedingungen zu funktionieren.
- Robustheit, d.h. Widerstandsfähigkeit gegen Umgehungsversuche.
- Nicht-Intrusivität, d.h. ein ausgewogenes Verhältnis zwischen Wirksamkeit und Schutz der Privatsphäre der Nutzer.
- Nichtdiskriminierung, d. h. Verfügbarkeit unabhängig von Faktoren wie ethnischer Zugehörigkeit oder Behinderung.

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?

Mit Blick auf alternative Altersabsicherungen (Age Assurance) gibt es weltweit verschiedene Ansätze, die jeweils konkurrierende Interessen von Kindern und Jugendlichen - Zuverlässigkeit und Schutz vor Umgehung einerseits und Schutz der Privatsphäre (Over-Collection) und Benutzererfahrung andererseits - in Ausgleich bringen wollen. Im Allgemeinen geht eine zuverlässigere Methode mit höheren Datenschutzbedenken und einer weniger reibungslosen Benutzererfahrung einher. Die meisten Leitfäden im europäischen Kontext verwenden „Alterssicherung“ als Oberbegriff für eine dreiteilige Taxonomie: In absteigender Reihenfolge ihrer Zuverlässigkeit lassen sich die einzelnen Methoden in Altersverifikation, Altersschätzung und Selbsterklärung einteilen, die auch als „age gating“ bezeichnet wird.

Die Altersschätzung erfolgt in der Regel mit einer Erkennungssoftware, die schätzt, ob ein Nutzer wahrscheinlich über oder unter einem bestimmten Alter oder innerhalb einer bestimmten Altersspanne liegt. Dazu gehören Schätzungen auf der Grundlage von Gesichtszügen, die automatisierte Analyse von Verhaltens- und Umgebungsdaten, der Vergleich der Art und Weise, wie ein Nutzer mit einem Gerät interagiert, mit anderen Nutzern desselben Alters sowie Messgrößen, die aus Bewegungsanalysen oder durch Tests ihrer Fähigkeiten oder Kenntnisse abgeleitet werden. Einige europäische Regulierungsbehörden erkennen an, dass diese Erkennungssoftware sogar die Anforderungen der Altersverifikation erfüllen kann, sofern die Schätzungstechnologie ausreichend fortgeschritten ist und/oder

das System mit einer Sicherheitsmarge konfiguriert ist. Mit Blick auf die rasanten Entwicklungen bei KI erscheint, dieser Weg immer zuverlässiger zu sein. Derzeit sind Altersschätzungen jedoch noch fehleranfällig und erfordern seitens der Anbieter aufwendige Verfahren, auf Beschwerden zu reagieren. Auch für Kinder und Jugendliche – und wohl auch die Eltern – ist diese Fehleranfälligkeit derzeit nicht zumutbar.

Bei einer Selbsterklärung (self-declaration) gibt ein Nutzer lediglich das Alter oder seine Altersgruppe an, ohne Nachweise vorzulegen. Beispiele für Selbsterklärungsmethoden sind die Angabe des Geburtsdatums oder die Erklärung, dass man über 18 Jahre alt ist. Diese Altersabsicherung ist nach Ansicht deutscher Gerichte jedenfalls bei den verpflichtenden Schutzmaßnahmen nach Art. 6a der AVMD-Richtlinie nicht ausreichend. In manchen Fällen kann aber auch die Selbsterklärung ein praktikables Instrument sein, beispielsweise wenn die Selbsterklärung den Nutzer unter eine Altersgrenze stellt und daher die strengsten Schutzmaßnahmen zur Anwendung kommen. Einige Leitlinien in anderen europäischen Ländern sehen auch Gestaltungsmöglichkeiten vor, die die Selbstauskunft etwas zuverlässiger machen – beispielsweise offene Fragen zum Alter zu stellen, ohne die geltende Altersgrenze zu nennen, und/oder zu verhindern, dass Nutzer ihre Antwort ändern können, wenn sie mit ihrer ursprünglichen Antwort unter die Altersgrenze für den Zugriff auf bestimmte Inhalte oder Funktionen fallen.

Je höher die Zuverlässigkeit sein soll, desto mehr Abstriche müssen beim Datenschutz und bei der Usability gemacht werden. Mit Blick auf die besondere Schutzwürdigkeit von Daten Minderjähriger empfiehlt sich zumindest eine anonymisierte Altersverifikation über zertifizierte Dritte, die aber natürlich auch Daten verarbeiten und vorhalten müssen und damit zum „Honey Pot“ werden. Die EU-Kommission konstatiert in ihren Leitlinien ausdrücklich, dass zu viele und zu hohe Altersabsicherungsmaßnahmen Kinder und Jugendliche von alltäglichen und meist jugendschutzrechtlich unproblematischen Angeboten im Internet ausschließen können und sie damit auch in ihrem Recht auf Teilhabe beschränken. Die Leitlinien empfehlen daher, dass Altersabsicherungsmaßnahmen nur dann vorgenommen werden sollen, wenn sie auch wirklich erforderlich sind. Nach Ansicht der EU-Kommission sind sie dies vor allem bei Glücksspiel, Pornographie und Alkoholverkäufen. Games fallen in der Regel in keine dieser Kategorien und deswegen könnten bei solchem „medium-risk content“ – zumindest bei steigender Zuverlässigkeit – datenschutzsensiblere Methoden wie die Altersschätzung ausreichend oder sogar zwingend sein.

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?

Speziell gestaltete digitale Räume für Kinder und Jugendliche sind wohl eher für Chats oder andere Social Media-Anwendungen gedacht, sind aber grundsätzlich auch bei Games möglich und können in Einzelfällen auch sinnvoll und förderlich sein. Sie sollten allerdings ein zusätzliches Angebot sein und nicht als zwingende Alternative zu den allgemeinen Foren gesehen werden. Die Leitlinien der EU Kommission zu Art. 28 DSA stellen ausdrücklich klar, dass „Instrumente zur Altersfeststellung (...) Anbietern auch dabei helfen [können], den Zugang von Erwachsenen zu bestimmten Plattformen, die für Minderjährige konzipiert sind, zu anderen als legitimen elterlichen, erzieherischen oder Aufsichtszwecken zu verhindern und so das Risiko zu verringern, dass sich Erwachsene als Minderjährige ausgeben und/oder versuchen, Minderjährigen Schaden zuzufügen.“

Allerdings müssen die Grenzen solcher Schutzräume klar benannt werden. Auch altersbasierte Zugangshürden können Minderjährige nicht vor allen Risiken schützen: Auch unter Gleichaltrigen bestehen Interaktions- und Kommunikationsrisiken wie Cybermobbing, Hassrede oder sexuelle Grenzverletzungen. Zudem können zulässige Inhalte kumulative Wirkungen entfalten, etwa durch Schönheitsideale oder Rollenklischees. Insofern brauchen solche Räume stets auch flankierende und begleitende Schutzmaßnahmen wie Moderation oder Melde- und Abhilfeverfahren. Zudem entstehen harte Altersgrenzen, die Ältere bzw. Jüngere zu einem bestimmten Zeitpunkt ausschließen.

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?

Ein technisch integrierter Kinder- und Jugendmedienschutz, der bereits „by design“ in digitale Dienste eingebettet ist, eröffnet erhebliche Chancen für Information, Bildung, Beteiligung, Entfaltung und Freizeit von Minderjährigen. Der Ansatz entspricht Art. 28 DSA, der nicht auf pauschale Zugangsbeschränkungen, sondern auf eine altersangemessene, risikobasierte Gestaltung digitaler Dienste abstellt, wie sie auch die Leitlinien der Europäischen Kommission oder die USK-Leitkriterien ausdrücklich hervorheben. Technischer Jugendschutz „by design“ ermöglicht niedrighwelligen Zugang zu Information und

Bildung, ohne Minderjährige generell auszuschließen. Durch „wertige“ Alterskennzeichen, Parental-Control-Systeme und einen elternseitig wahrnehmbaren altersdifferenzierten Zugang, können Minderjährige digitale Medien nutzen, die ihrem Entwicklungsstand entsprechen. Auch der Games-Bereich bietet vielfältige Lern-, Problemlösungs- und Kreativpotenziale, die durch eine intelligente technische Ausgestaltung erhalten bleiben, statt durch pauschale Verbote unterbunden zu werden.

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)?

Ein übermäßiger Medienkonsum von Kindern und Jugendlichen kann technisch nur bedingt wirksam begrenzt werden. Kinder und Jugendliche könnten sich bspw. mehrere Accounts mit unterschiedlichen Identitäten erstellen. Technische Vorkehrungen (Parental Control) zur Zeitbegrenzung und für Nutzungsstatistiken sind immer nur Tools, die aber auch angewendet bzw. durchgesetzt werden müssen. Sofern Eltern entscheiden, ihrem Kind ein Gerät und die Inhalte zur Verfügung zu stellen, liegt es auch an ihnen, dies zu steuern und ggfs. zu limitieren. Das ergibt sich auch aus dem Erziehungsrecht der Eltern in Art. 6 Abs. 2 GG und begrenzt damit mittelbar auch die Möglichkeiten der Anbieter.

3. Wie kann in Fällen von Sharenting und Family-/Kinder-Influencing einem Missbrauch von Bildern und personenbezogener Daten technisch, regulatorisch und durch Medienbildung vorgebeugt werden?

Diese Frage bezieht sich wohl vor allem auf Social Media. Bei Games findet Sharenting und Family-/Kinder-Influencing nicht statt.