GRUNDSATZPAPIER ZIVILGESELLSCHAFTLICHER ORGANISATIONEN ZUM THEMA ALTERSVERIFIKATION / ALTERSFESTSTELLUNG (*AGE ASSURANCE*)

HINTERGRUND

Altersverifikationssysteme (AVS) werden in der Fachwelt derzeit breit diskutiert und vielfach als die Lösung vieler Problemlagen im Jugendmedienschutz angesehen. Die Altersverifikationsindustrie hat sich zu einem Milliardengeschäft entwickelt und es bleibt kritisch zu evaluieren, inwiefern Altersfeststellung die Sicherheit im Internet verbessert. Hätten Kinder keinen Zugang zu digitalen Angeboten oder Inhalten, die nicht alters- oder entwicklungsangemessen sind, oder hätten Erwachsene keinen Zugang zu Online-Räumen für Kinder, wären viele der Anliegen des Jugendmedienschutzes gelöst, so die Annahme.

Wir, die zeichnenden zivilgesellschaftlichen Organisationen aus den Bereichen Kinderschutz/Kinderrechte und Netzpolitik/Datenschutz, fordern eine differenzierte und grund- und kinderrechtebasierte Auseinandersetzung mit dem Thema Altersfeststellung.

In einem mehrstufigen Prozess bestehend aus einem Fachgespräch, einem Workshop und einem fachlichen Austausch, haben wir uns detailliert mit den Möglichkeiten und Problemstellungen von Altersfeststellung auseinandergesetzt. Ziel dieser Auseinandersetzung war, eine gemeinsame Haltung zu erarbeiten, die sowohl die kinderrechtlichen Implikationen als auch die technischen, datenschutzrechtlichen Bedenken berücksichtigt.

Zentral für diese Haltung ist eine differenzierte Auseinandersetzung mit den unterschiedlichen Altersfeststellungsverfahren. Dieses Papier unterscheidet zwischen Altersauskunft (*age declaration*), die auf Selbstauskunft beruht und keine Verifikation des angegebenen Alters beinhaltet, Altersschätzung (*age estimation*), die mittels künstlicher Intelligenz (KI) das Alter von Nutzenden schätzt, sowie die dokumentenbasierte Altersverifikation (*age verification*), die anhand von Ausweisdokumenten oder -daten entweder direkt oder über Drittanbieter bzw. verifizierende Stellen das Alter der Nutzenden überprüft.

Ausgehend von der Annahme, dass aktuell verwendete *Age Declaration*-Verfahren, bei denen Nutzende selbst ihr Alter angeben oder die Volljährigkeit mit einem Klick bestätigen, keine effektive Zugangsschwelle darstellen und damit keinen nennenswerten Schutz bieten, haben wir Überlegungen angestellt, welche Vor- und Nachteile verschiedene Verfahren haben und welchen Grundprinzipien Altersfeststellung folgen muss, um grund- und kinderrechtekompatibel zu sein bzw. um die Risiken einer Beeinträchtigung der Grund-, Menschen- und Kinderrechte zu minimieren. Dabei haben wir uns auf drei Altersfeststellungssysteme fokussiert: Altersverifikation mittels staatlicher IDs, Altersschätzung anhand biometrischer Marker und zertifikatsbasierte Altersverifikation.

KONTEXTE

Nach aktueller Rechtslage sind AVS nur in wenigen eng gesteckten Rahmen verpflichtend. Das betrifft aktuell nach Jugendmedienschutz-Staatsvertrag sogenannte ‚relativ unzulässige Erwachseneninhalte' (Pornographie), nach Glücksspielstaatsvertrag Glücksspiel und (Sport-)Wetten sowie laut Jugendschutzgesetz die Abgabe bzw. den Verkauf von Alkohol und Tabak an Kinder und Jugendliche.

Sollte der umstrittene CSAM-Verordnungsentwurf[1] der Europäischen Kommission in der aktuellen Fassung (7080/25, 04.04.2025) in Kraft treten, würden Altersverifikationsverfahren für interpersonelle Kommunikationsdienste, durch die Kinder für sexuelle Zwecke angeworben werden könnten, zur Pflicht.

In den meisten Gesetzen werden Altersfeststellungsverfahren lediglich als eine mögliche Kinder- und Jugendschutzmaßnahme aufgezeigt – so im Digitale-Dienste-Gesetz (*Digital Services Act*) (gilt für Anbietende von Online-Plattformen, die für Minderjährige zugänglich sind), im Jugendschutzgesetz (das allerdings nur die Berücksichtigung des Alters nennt und offen lässt, ob es verifiziert wurde), in der Audiovisuelle-Mediendienste-Richtlinie, im Jugendmedienschutz-Staatsvertrag im Kontext entwicklungsbeeinträchtigender Inhalte und auch in der geplanten CSAM-Verordnung im Kontext von App-Marktplätzen.

Gemäß der Datenschutz-Grundverordnung (DSGVO) ergibt sich für Anbietende eine implizite Pflicht zur Altersüberprüfung, da sie bei der Nutzung ihres Dienstes durch unter 16-Jährige verpflichtet sind, die Einwilligung der Erziehungsberechtigten einzuholen. Diese Regelung kommt in der Praxis jedoch vielfach nicht zum Tragen, da Anbietende die Daten der Nutzenden auf Grundlage des berechtigten Interesses verarbeiten. Ebenso haben sich die Anbietenden mittels ihrer Allgemeinen Geschäftsbedingungen in der Regel selbst auf ein jeweiliges Mindestalter festgelegt (oft 13 Jahre), welches in den meisten Fällen durch diese nicht überprüft wird.

Wir nehmen diese Kontexte und dazugehörige, teils kontroverse Diskurse wahr und fordern, dass die folgenden grund- und kinderrechtebasierten Prinzipien von Anbietenden eingehalten werden, sofern sie entweder aufgrund von rechtlicher Verpflichtung, Nutzung des rechtlichen Spielraums oder freiwilliger Entscheidung Altersfeststellungssysteme einsetzen.

GRUNDPRINZIPIEN

Die im Folgenden genannten Prinzipien sollen einen grund- und kinderrechtebasierten Rahmen liefern, um Altersfeststellungssysteme wirksam, verhältnismäßig und nichtdiskriminierend zu gestalten sowie eine angemessene Berücksichtigung der DSGVO zu gewährleisten.

Privacy by design, *Safety by design, Transparency by design* sowie *Access(ibility) by design* – all diese Prinzipien sind wichtige Voraussetzungen für *Child Rights by Design*. In diesen Prinzipien finden sich folgende Anforderungen wieder, die nicht verhandelbar sein dürfen: Datenschutzkonformität, Anonymität, Unbeobachtbarkeit – keine Daten an Dritte, Datenminimierung, Unverknüpfbarkeit der Nutzendendaten, also keine Deanonymisierung, um Profilbildung zu verhindern, Intervenierbarkeit, Vertraulichkeit, Zuverlässigkeit, Nachvollziehbarkeit, Verständlichkeit, Verfügbarkeit und Integrität. Die Prämisse von *Zero Knowledge* muss sichergestellt werden. Diskriminierungs- und Ausschlussmechanismen müssen berücksichtigt und verhindert werden.

DATENMINIMIERUNG, PRIVACY BY DESIGN UND SAFETY BY DESIGN

Altersfeststellungssysteme müssen ein hohes Maß an Zuverlässigkeit bieten, d.h. das Alter der*des Nutzenden entweder korrekt auslesen oder verlässlich mittels technischen, inklusive KI-basierten Verfahren bestimmen. Datensicherheit und Datenminimierung müssen oberste Prämissen sein. Dies bedeutet sowohl, dass durch den Dienst erhobene Daten – wie z.B. angefertigte Fotoaufnahmen („Selfies“) – unmittelbar nach Nutzung der Daten unwiderruflich gelöscht werden, als auch, dass das Verfahren mit einem Minimum an Daten auskommt, um eine präzise Altersfeststellung zu

[1] Gemeint ist die Verordnung zur Vorbeugung und Bekämpfung sexuellen Kindesmissbrauchs (englisch: *Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse)*.

gewährleisten. Hierbei sollten datenschutzfreundliche Technologien wie der *Zero-Knowledge-Proof* zum Einsatz kommen, die eine Altersfeststellung ermöglichen, ohne dass sensible personenbezogene Informationen offengelegt werden müssen. Auf technischer Ebene sollte ein *Privacy by design*-Ansatz verfolgt werden, der den Prinzipien der Unbeobachtbarkeit (englisch: *unobservability)* und Unverknüpfbarkeit (englisch: *unlinkability)* folgt.

ZUGANG FÜR ALLE - ACCESS(IBILITY) BY DESIGN

Es muss sichergestellt werden, dass *alle* Nutzenden ihr Alter über mindestens ein Verfahren feststellen lassen können. Der Einsatz von Altersfeststellung darf nicht zur Ausgrenzung von Kindern und Erwachsenen führen, die bereits von struktureller Ausgrenzung und Diskriminierung betroffen sind. Es gilt zu berücksichtigen, dass leistungsstarke Endgeräte in der Bevölkerung zwar einen hohen Verbreitungsgrad haben, aber eine vollständig flächendeckende Verbreitung nicht angenommen werden kann. Daher muss sichergestellt werden, dass die Altersfeststellungssysteme stets auch mit älteren Geräten sicher nutzbar sind.

Sofern zertifikatsbasierte Verfahren eingesetzt werden, ist sicherzustellen, dass diese niedrigschwellig und ohne Ausschluss einzelner Personen(gruppen) zugänglich sind. Auch sollte bei derlei Verfahren möglichst auf bereits bestehende Infrastruktur zurückgegriffen werden, die ob der zusätzlichen Belastung durch öffentliche Gelder finanziell und personell ausgestattet sein muss.

EFFEKTIVITÄT, MONITORING UND PROZESSOPTIMIERUNG

Unabhängig vom gewählten Verfahren sollten die Möglichkeiten der Umgehung – z.B. mittels der Ausweisdokumente oder den Zugangsdaten einer anderen Person – in den Wirkungsgrad des Systems einkalkuliert und möglichst minimiert werden. Ein leicht umgehbares System, das gleichzeitig große datenschutzrechtliche Probleme und infrastrukturelle Kosten mit sich bringt, ist in seiner Effektivität und Verhältnismäßigkeit fragwürdig. Zudem sollte ein unabhängiges Monitoring-Verfahren etabliert werden, das die Verfahren und dessen Sicherheit evaluiert und einen Beitrag zur iterativen Verbesserung des Systems leistet. Kinder daran gemäß Art. 12 der UN-Kinderrechtskonvention zu beteiligen, begrüßen wir. Zudem sollte das Monitoring eingesetzt werden, um zu überprüfen, ob das System der Altersfeststellung (noch) adäquat in Bezug auf die anzunehmenden Risiken ist.

TRANSPARENZ – TRANSPARENCY BY DESIGN

Anbietende von Altersfeststellungssystemen sollten transparent über den Datenschutz, die Rechte der Beteiligten und das Verfahren kommunizieren (z.B. verwendete Trainingsdaten, Funktionsweisen und Fehlerquoten sowie Quelloffenheit/Open Source). Auch sollte die jeweilige Maßnahme transparent und adressat*innenadäquat erklärt werden, z.B. in kind- und jugendgerechter Sprache, damit sie befähigt werden, auf dieser Basis eine informierte Entscheidung über das gewählte Verfahren treffen zu können. Gleichzeitig entbindet eine transparente Kommunikation nicht von der Einhaltung der grund- und kinderrechtebasierten Prinzipien.

ALTERNATIVE ALTERSFESTSTELLUNGSMETHODEN UND WIDERSPRUCHSRECHT

Alle Nutzer*innen sollten in der Lage sein, ihr Alter über mindestens eines der Verfahren feststellen zu lassen oder verifizieren zu können, indem mindestens zwei unterschiedliche Verfahrensarten zur Auswahl gestellt werden. Neben dem Recht auf alternative Altersfeststellungsmethoden muss gewährleistet sein, dass es eine Möglichkeit zum Widerspruch sowie das Angebot einer alternativen Überprüfungsmethode im Fall einer falschen Altersschätzung oder anderweitiger Fehler gibt. Wer sein Alter nicht überprüfen oder feststellen lassen möchte, sollte das Angebot dann – sofern es sich um ein Angebot mit altersabgestuften Inhalten und/oder Funktionen handelt – in der sichersten Einstellung nutzen können.

Finanzierung

Es muss gewährleistet sein, dass sämtliche digitale Angebote, d.h. auch non-profit-Angebote, das System nutzen und finanzieren können. Staatliche Förderungen zu diesem Zweck begrüßen wir, ebenso wie eine staatlich geförderte Open Source-Lösung. Dabei dürfen jedoch Investitionen in AVS zu keiner Zeit gegen etwaige Förderungen in Bildung, wie z.B. in die Medien- und Digitalkompetenz, abgewogen werden.

Rolle von Drittanbietenden

Drittanbieter*innen nehmen in den Verfahren eine zentrale Rolle ein, um eine Trennung von Datenerhebung und Datennutzung sicherzustellen. Sie geben die Information über das Alter bzw. das Alterssegment der*des Nutzenden an den Anbieter weiter, ohne den genauen Zweck dessen zu kennen. Gleichzeitig erfährt der Anbieter die Identität des*der Nutzenden nicht (*Double-Blindness*-Verfahren). Wir weisen darauf hin, dass seitens dieser Drittanbieter*innen Datenschutzkonformität, Privatsphäre und Vertraulichkeit sichergestellt sein müssen.

Analyse einzelner Verfahren

Altersverifikation mittels staatlicher IDs

Das Verfahren der Altersverifikation mittels staatlicher IDs basiert darauf, dass das genaue Alter einer Person aus einem anerkannten Ausweisdokument ausgelesen und entweder als solches oder als Zugehörigkeit zu einer Alterskohorte (z.B. zwischen 13 und 16 Jahren oder </> 18 Jahre) übermittelt wird.

Dieses Verfahren hat den Vorteil, eine genaue Altersüberprüfung mit sicherem Ergebnis zu liefern. Der hohe Verbreitungsgrad von Ausweispapieren birgt zudem den Vorteil einer potenziell breiten Anwendung in der Gesellschaft. Bei der Nutzung staatlicher IDs ist es zentral, die Sicherheit der erhobenen Daten zu gewährleisten – mittels Pentests, Datenschutzaudits und Trust-Siegeln nach DIN/ISO-Vorgaben oder anderen bewährten Verfahren. Belegbare technische Maßnahmen wie Kryptografie und Anonymisierung sollten die Privatsphäre der Nutzenden zwingend sicherstellen. Zudem braucht es eine langfristige Sicherheitsstrategie, die den gesamten Entwicklungsprozess begleitet. Das Risiko des Datenmissbrauchs durch Unbefugte bleibt dennoch bestehen.

Die *alleinige* Nutzung staatlicher IDs zum Zwecke der Altersverifikation bewerten wir als kritisch, da dies zahlreiche Personengruppen von dem Verfahren ausschließen würde, z.B. Kinder unter 16 Jahren, für die aktuell keine Ausweispflicht besteht, Geflüchtete oder Personen ohne gültigen Aufenthaltsstatus und Staatenlose. Dies bewerten wir als Herausforderung und sind besorgt um den massiven Ausschluss von Teilhabemöglichkeiten einer großen Bevölkerungsgruppe, wenn für diese keine adäquaten Lösungen – wie beispielsweise das *Vouching*-System in Großbritannien, bei dem vertrauenswürdige Personen, wie z.B. Sozialarbeitende, die für das Alter der entsprechenden Personen bürgen können – gefunden werden. Weiterhin ist die Zugänglichkeit aktuell durch die unzureichende Verbreitung von eIDs erschwert. Da alle EU-Mitgliedsstaaten aufgrund der eIDAS-Verordnung verpflichtet sind, ihren Bürger*innen ab November 2026 eIDs anzubieten, hat die EUDI-Wallet das Potenzial, zukünftig eine EU-weite Standardisierung des Verfahrens zu ermöglichen.

Bei der Verwendung staatlicher IDs halten wir es für wichtig zu betonen, dass die Anonymität als zentrales Prinzip des Internets durch *Zero Knowledge Proof* zu wahren ist. Das verwendete Verfahren sollte daher in der Lage sein, nur die Information über das Alter bzw. die Alterskohorte zu übermitteln, nicht jedoch die Identität der*des Nutzenden. Dass aktuell bekannte Verfahren (noch) nicht in der Lage sind, nur das Alter auszulesen, bereitet uns große Sorge.

Zudem sehen wir das Risiko einer „Ausweispflicht im Netz“, wenn Nutzende unabhängig von ihrem Alter für den Zugang zu verschiedenen Online-Angeboten ihre Ausweisdaten preisgeben müssten, wobei zusätzlich die Gefahr besteht, dass die Systeme mehr Daten auslesen, als für die Erfüllung des Zwecks notwendig ist (Stichwort: Überidentifizierung).

Weiterhin gilt es zu bedenken, dass eingesetzte Verfahren teilweise relativ einfach zu umgehen sind, indem der Ausweis einer Person mit entsprechendem Alter genutzt wird. Daher sind Verfahren sinnvoller, die neben der Identifizierung auch die Authentifizierung der Nutzenden beinhalten, beispielsweise über einen Abgleich des Ausweises mit einem live-Selfie.

BIOMETRISCHE ALTERSSCHÄTZUNG

Verfahren der biometrischen Altersschätzung geben anhand biometrischer Marker eine Schätzung über das Alter einer Person, beispielsweise über das Gesicht oder die Hand(bewegung). Daneben existieren noch weitere Verfahren der Altersschätzung ohne biometrische Daten wie beispielsweise über die E-Mail-Adresse, die hier nicht betrachtet werden.

Diese Verfahren sollen einen niedrigschwelligen Zugang mit schneller Durchführbarkeit ohne die Nutzung von Ausweisdaten bieten, bei dem kein Medienbruch in der Nutzung entsteht.[2] Eine gute *User Experience* steht hier klar im Fokus. Dass dabei keine Ausweisdaten ausgelesen werden, macht die Verfahren allerdings nicht unproblematisch. Kritisch sehen wir insbesondere das Ausmaß an Daten, die in die (KI-basierten) Programme einfließen, um eine möglichst genaue Altersschätzung zu gewährleisten sowie die hohe Sensibilität der erhobenen Daten. Dies widerspricht dem Grundsatz der Datensparsamkeit. Auch die potenziell intransparente Datenverarbeitung und das Risiko einer widerrechtlichen Datensammlung durch die Anbietenden halten wir für problematisch. Weiterhin bleibt das Risiko des Datenmissbrauchs durch Dritte bestehen.

Zudem sind die derzeit existierenden Altersschätzungsverfahren mit Ungenauigkeiten verbunden und stets nur so gut wie das zugrundeliegende Material, mit dem die KI trainiert wird. Dies kann wiederum zum Ausschluss von Personen führen, die eigentlich zur Nutzung der Angebote berechtigt wären, z.B. Personen mit Behinderung oder trans*-Personen, deren Alter mit höherer Wahrscheinlichkeit ungenauer geschätzt wird. Daher unterstützen wir, dass KI-basierte Systeme eine hohe Diversität in den Trainingsdaten aufweisen und eine hohe Genauigkeit (*True Positive Rate*) in der Altersschätzung nachweisen müssen, bevor diese eingeführt werden.

Wir weisen darauf hin, dass sich solche Verfahren potenziell umgehen lassen, indem das Gesicht einer anderen (älteren) Person oder potenziell auch KI (z.B. Deepfakes) genutzt wird. Auch ist denkbar, dass Erwachsene sich durch die Altersschätzung eines Kindes unbefugten Zugang zu Kinderangeboten verschaffen.

ALTERSVERIFIKATION MITTELS ZERTIFIKATSINFRASTRUKTUR

Das System einer zertifikatsbasierten Infrastruktur wäre analog zum Verfahren, das in Deutschland im Rahmen der COVID 19-Impfungen angewandt wurde. Dabei stellt eine verifizierende Stelle, der das Alter der*des Nutzenden bekannt ist (z.B. die Schule oder die Bank) ein Zertifikat aus, das von einer zu definierenden Instanz (z.B. einer Browser-Extension) ausgelesen werden kann, sodass die Information an den*die Web-Anbieter*in weitergeleitet und entsprechende Inhalte freigeschaltet oder gesperrt werden.

Das Verfahren bietet eine Reihe von Vorteilen, die sich insbesondere im Kontext der Datensparsamkeit, der Anonymität und der hohen Genauigkeit verorten lassen. Dieses dezentrale System ist als Gesamtsystem nur schwer angreifbar und daher relativ ausfallsicher, allerdings bleibt es in seiner Verlässlichkeit stark abhängig von der technischen Infrastruktur der verifizierenden Stellen.

[2] Die genannten Vorteile gelten gleichermaßen für *Age Declaration*-Verfahren.

Dennoch ergibt sich daraus nicht zwangsläufig eine Fälschungssicherheit, da Zertifikate potenziell an andere Personen weitergegeben werden oder getauscht werden könnten. Zudem besteht das Risiko einer Be- oder Überlastung bestehender Infrastruktur. Daraus resultiert z.B. die Frage, wer die Kosten für die Zertifikatsinfrastruktur und den Personalaufwand in den verifizierenden Stellen trägt. Die Implementierung eines derartigen Systems dürfte sich auf vielen Ebenen als komplex erweisen.

Für ein funktionierendes, zertifikatsbasiertes System ist es notwendig, dass die verifizierenden Stellen niedrigschwellig für alle Nutzenden erreichbar und vertrauenswürdig sind. Ausgestellte Zertifikate müssen widerrufen werden können, wenn der Verdacht auf fälschliche Ausstellung des Zertifikats besteht oder ein Zertifikat fehlerhafte Informationen enthält. Auch durch eine limitierte zeitliche Gültigkeit des Zertifikats könnte dieser Herausforderung begegnet werden. Kinder sollten unabhängig von ihren Erziehungsberechtigten in der Lage sein, Zertifikate erhalten zu können, indem verifizierende Stellen etabliert werden, die für Kinder niedrigschwellig erreichbar sind. Das Verfahren muss kindgerecht und einfach zugänglich sein.

FAZIT

Vor dem Hintergrund der vorangegangenen Ausführungen weisen wir ausdrücklich darauf hin, dass es keine technische *One-Size-Fits-All*-Lösung für sämtliche Online-Risiken gibt und stets gilt, die Kinderrechte auf Schutz, Förderung/Befähigung und Teilhabe bestmöglich miteinander in Einklang zu bringen, zumal der Einsatz von Altersfeststellungssystemen Implikationen für die Grundrechte aller Nutzenden hat. Daher plädieren wir für einen ganzheitlichen Ansatz, der eine Verzahnung von medienerzieherischen Maßnahmen, elterlicher Verantwortung - wozu auch Parental Control Maßnahmen und andere technische Jugendschutzmaßnahmen zählen - Anbieter-Verantwortung, gesetzlicher Regulation und technischen Lösungen forciert. Dabei muss der Grundsatz für jegliche technische Lösung, die Kinder und Jugendliche im Netz schützen und gleichzeitig auch befähigen und teilhaben lassen soll, *child-appropriate by design* lauten. Unabhängig vom Verfahren sollten aus unserer Sicht zudem stets die oben genannten Grundprinzipien befolgt werden: *Privacy by design*, *Safety by design, Transparency by design* sowie *Access(ibility) by design* – all diese sind wichtige Voraussetzungen für *Child Rights by Design*.

Unter den aktuell existierenden technischen Systemen für Altersfeststellung im Netz können wir derzeit keine klare Empfehlung aussprechen. Wir plädieren für eine Kombination verschiedener Vorsorgemaßnahmen und eine stete Überprüfung der Verhältnismäßigkeit der Maßnahmen. Dazu gehören eine Untersuchung und Abwägung der Auswirkungen auf betroffene Grundrechte. Eine solche Prüfung sollte den legitimen Zweck, die Eignung, Erforderlichkeit und Angemessenheit einer Maßnahme betrachten. Sollten Altersfeststellungssysteme eingeführt werden, dann nur unter Anwendung der oben genannten Prinzipien. Denn nur so kann Altersfeststellung zu einem kindgerechten Netz und effektiven Kinderschutz im Netz beitragen.

AUSBLICK

Dieses Grundsatzpapier zeigt einen Rahmen auf, der eine Orientierung zur Bewertung grund- und kinderrechtskonformer Lösungen bietet. Es gilt jedoch zu beachten, dass Altersfeststellungssysteme die zugrundeliegenden Probleme eines nicht kindgerechten Internets nicht lösen können. Vielmehr müssen digitale Angebote, allen voran soziale Medien, insgesamt kindgerecht(er) gestaltet sein, wozu auch eine altersabgestufte Inhalte- und Funktionenbereitstellung zählen kann. Es bedarf eines *child-appropriate designs (siehe Child Rights by Design)* und einer konsequenten Umsetzung rechtlicher Vorgaben wie dem *Digital Services Act* (DSA), der wichtige Leitplanken für Anbieter von Online-

Plattformen[3] liefert. Dazu zählen u.a. Art. 28 (Schutz Minderjähriger) und die dazugehörenden Richtlinien, die grundlegende Sorgfaltspflichten im Kinder- und Jugendmedienschutzbereich für Anbietende von Online-Plattformen aufstellen sowie Art. 35 zur Risikominimierung. Darüber hinaus definiert der DSA negative Auswirkungen von digitalen Diensten auf die Rechte des Kindes sowie den Schutz von Minderjährigen als systemische Risiken, zu dessen Minderungen sehr große Online-Plattformen und Suchmaschinen Altersüberprüfungen nutzen können, dazu aber nicht verpflichtet sind. Einen Ansatz, der allein auf Altersfeststellung beruht, um Zugang zu dem sozialen Netzwerk zu erhalten bzw. zu versperren, halten wir für nicht geeignet.

Das Grundsatzpapier ist das Ergebnis eines vom Kinderschutzbund Bundesverband e.V. und SUPERRR Lab initiierten Prozesses, mit dem Ziel, eine gemeinsame Haltung verschiedener zivilgesellschaftlicher Organisationen zum Thema Altersfeststellung zu erarbeiten. An der Erarbeitung des Papiers waren weitere Organisationen aus den Bereichen Kinderrechte / Kinderschutz und Digitalpolitik / Datenschutz sowie Einzelpersonen beteiligt, darunter Dr. Stephan Dreyer (Leibniz-Institut für Medienforschung \| Hans-Bredow-Institut) und Dr. Ingrid Stapf (Eberhard Karls Universität Tübingen).

Der Kinderschutzbund Bundesverband

SUPERRR

Deutsches Kinderhilfswerk

unicef für jedes Kind

DEUTSCHER BUNDESJUGENDRING

BAJ Bundesarbeitsgemeinschaft Kinder- und Jugendschutz

netzforma*e.V. Verein für feministische Netzpolitik

D4CR

SEITEN STARK

[3] Neben soziale Medien sind im DSA Vorgaben für App-Stores, Videosharing-Plattformen, Suchmaschinen und vielen weiteren Anwendungsbereichen geregelt.