

Maßnahmen zur Altersverifikation in Metaversen: Ethische, rechtliche und sicherheitstechnische Aspekte

*Jessica Heesen, Thomas Kunz, Matthias Meitzler, Maria Pawelec,
Marina Steenbergen und Ulrich Waldmann*

Zusammenfassung

Metaversen ermöglichen immersive, digitale Interaktionen, bergen jedoch vor allem für Kinder und Jugendliche besondere Risiken, da sie u. a. einen unkontrollierten Zugang zu nicht altersgerechten Inhalten und Interaktionen begünstigen. Der Beitrag beleuchtet Altersverifikationen in Metaversen aus ethischer sowie rechtlicher Perspektive und diskutiert die Anforderungen des Jugend- und Datenschutzrechts sowie grundlegende Prinzipien wie informationelle Selbstbestimmung, digitale Souveränität und Nichtdiskriminierung. Vorgestellt wird ein sicherheitstechnischer Ansatz auf Basis selbstbestimmter digitaler Identitäten, der pseudonyme Nachweise von Altersgruppen ermöglicht, ohne in Metaversen reale Identitäten offenzulegen. Er schafft damit einen angemessenen Rahmen für den Schutz Minderjähriger in transnationalen Metaversen.

1. Einleitung

Metaversen sind persistente, virtuelle Welten, die – häufig mit Hilfe von Virtual-Reality (VR)-Zubehör – eine neue Form der digitalen Vernetzung und Interaktion ermöglichen. In ihnen agieren Nutzende als *Avatare*, d. h. als verkörperte virtuelle Repräsentationen ihrer selbst, die sie in Echtzeit steuern. Typische Anwendungen umfassen u. a. Gaming, virtuelle Events, Bildungsangebote, simulationsgestützte Produktentwicklung und interaktiven Austausch im Allgemeinen. Charakteristisch für Metaversen ist das hohe Maß an *Immersion*, wodurch Nutzende in die virtuelle Welt eintauchen.

Aufgrund ihrer innovativen Form virtueller Präsenz, Immersion und Interaktion sowie fehlender Moderationsstrukturen bergen Metaversen neuartige, den Datenschutz sowie die (informationelle) Selbstbestimmung, die Identität und die Sicherheit der Nutzenden in besonderem Maße betreffen-

de Risiken (Al-kfairy u. a. 2025), welche über bereits bekannte Problemlagen des Internets und sozialer Medien hinausgehen (Croll/Krause 2024). Hierzu gehört beispielsweise die illegitime Aneignung von Avataren oder der Einsatz von rein KI-gesteuerten Avataren, die sich als menschliche Akteure ausgeben und Nutzende gezielt manipulieren können.

Verifikationsmaßnahmen können einen wichtigen Beitrag leisten, um diesen Risiken zu begegnen. Sie eignen sich etwa zur Einschätzung anderer Nutzenden, u. a. ob es sich um den Avatar einer realen Person oder einen KI-gesteuerten Avatar (Kunz/Waldmann 2025a) handelt, oder besonders des Alters eines Nutzenden durch eine entsprechende Altersverifikation.

Schätzungsweise zwei Drittel aller Nutzenden von Metaversen sind derzeit jünger als 16 Jahre (Standards Australia 2024). Als „Early Adopters“ agieren Kinder und Jugendliche mit Blick auf Medien häufig offener und risikobereiter und sind dabei mitunter weniger stark für mögliche Gefahren sensibilisiert als Erwachsene. In der Folge können sie von den negativen Auswirkungen der Mediennutzung stärker betroffen sein (vgl. Livingstone u. a. 2019, S. 4; Stapf/Heesen 2026). Die Vulnerabilität und die besondere Schutzbedürftigkeit von Kindern und Jugendlichen rücken vor diesem Hintergrund die Frage nach strukturellen Vorkehrungen im Sinne altersangemessener Zugangs- und Interaktionskontrollen in den Fokus.

Auf der Grundlage spezieller Risiken von Metaversen für Kinder und Jugendliche sowie qualitativer Interviews mit Expertinnen und Experten wird in diesem Beitrag zunächst die Legitimität entsprechender (Alters-)Verifikationsmaßnahmen aus ethischer Perspektive diskutiert. Im Anschluss folgen eine Darstellung der rechtlichen Anforderungen an (Alters-)Verifikationsmaßnahmen und die Beschreibung eines technischen Lösungsansatzes, mit dem das Alter der Nutzenden sicher und datensparsam verifiziert, der Zugang zu bestimmten Angeboten wirksam eingeschränkt und der Schutz von Privatheit verbessert werden kann. Den Abschluss bilden eine Berücksichtigung möglicher Grenzen von Altersverifikationen, die Ermittlung von Verantwortlichkeiten zur Umsetzung der Maßnahmen sowie ein Fazit.

2. Empirische und methodische Grundlagen

Der vorliegende Beitrag basiert sowohl auf umfassenden ethischen, rechtlichen und technischen Literaturstudien als auch semi-strukturierten, qualitativen Interviews mit Expertinnen und Experten, die im Rahmen des For-

schungsprojekts „Privatheit, Ethik und IT-Sicherheit in Metaversen“ (Pri-Meta; 2024-2027) durchgeführt wurden.* Leitfaden-gestützte Interviews ermöglichen eine Erfassung des „Bezugsrahmen[s] des Befragten“ und erlauben Einsichten in deren „Relevanzstrukturen und die Erfahrungshintergründe“ solcher (Schnell u. a. 2008, S. 387).

Die insgesamt 20 Interviews wurden unter einer explorativen, qualitativen Herangehensweise zwischen Oktober 2024 und November 2025 geführt, u. a. mit Expertinnen und Experten für Kinder- und Jugendmedienschutz, Medienkompetenzbildung sowie mit Personen, die sich auf die Nutzung von virtuellen Realitäten durch vulnerable Gruppen wie alte Menschen oder Menschen mit Behinderung spezialisiert haben. Die Befragten sollten ein möglichst breites Feld an Stakeholdern abdecken, die gesellschaftlich relevante Anwendungen in Metaversen (weiter-)entwickeln oder selbst nutzen. Kernthemen der Interviews waren Erfahrungen der Befragten mit Metaversen, ihre Einschätzung aktueller und künftiger technischer Entwicklungen, Chancen und Gefahren der Anwendungen, u. a. für den Datenschutz und gesellschaftliche Teilhabe. Die Interviewleitfäden wurden dabei teilweise an die jeweiligen Schwerpunkte der Befragten angepasst. Tab. 1 gibt einen Überblick über die geführten Interviews.

Tab. 1: Qualitative Interviews mit Expertinnen und Experten

Interview	Befragte Person	Hauptthema	Datum
I1	Vertreterin aus dem Bereich Tod und Digitalisierung	Entwicklung virtueller Trauerräume	08.10.2024
I2	Vertreter einer gemeinnützigen Stiftung	Entwicklung von Angeboten für ältere Menschen in VR	15.10.2024
I3	Experte für digitale Barrierefreiheit	Inklusion in und Zugänglichkeit von Metaversen	22.10.2024
I4	Unternehmensberaterin	Rolle von VR in Unternehmensentwicklung	05.12.2024
I5	Ev. Pfarrer	Digitalisierung und VR im Bereich Kirche und Trauer	06.12.2024
I6	Online-Rollenspielerin	Identität und Körperlichkeit im Kontext von Avataren	14.01.2025

* Die betreffenden Forschungsarbeiten wurden vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) sowie vom BMFTR und dem Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Interview	Befragte Person	Hauptthema	Datum
I7	VR-Designerin	Entwicklung von VR-Anwendungen	31.01.2025
I8	Ev. Pfarrer für Kirche im digitalen Raum	Kirche und Spiritualität in Minecraft	13.02.2025
I9	Experte für Lernbehinderungen	VR in der (Aus-)Bildung und Chancen für Inklusion	25.02.2025
I10	Kommunalvertreter	Kommunen in Metaversen	28.04.2025
I11	VR-Entwickler	Kommunen in Metaversen	23.05.2025
I12	Experte für Bürgerbeteiligung	Bürgerbeteiligung und Partizipation in Metaversen	22.07.2025
I13	Experte für Kinder- und Jugendmedienschutz	Kinder- und Jugendmedienschutz in Metaversen	07.08.2025
I14	Labengineer im Bereich Augmented and Virtual Reality Design	Chancen und Risiken von AR und VR	07.08.2025
I15	VR-Künstlerin	Kunst und Medienbildung zu VR und Metaversen	04.09.2025
I16	Vertreter eines Branchenverbands	Industrie und Metaversen	17.10.2025
I17	Digitalpolitiker	Politische Implikationen und Aufmerksamkeit für Metaversen	21.10.2025
I18	Zwei Expert:innen für Kinder- und Jugendmedienschutz	Kinder- und Jugendmedienschutz in Metaversen	19.11.2025
I19	Experte für Datenschutz	Privatheit und Datenschutz in Metaversen	21.11.2025
I20	Digital- und Politikberater	Politik und demokratische Prozesse in Metaversen	24.11.2025

Die Interviews wurden mit Zustimmung der Befragten aufgezeichnet, transkribiert und mit Hilfe der qualitativen Analysesoftware *MAXQDA* codiert. Die Entwicklung der insgesamt 155 Kategorien (Codes) erfolgte sowohl deduktiv auf Grundlage der Interviewleitfäden als auch induktiv durch die Auswertung des Materials. Die Codes beziehen sich insbesondere auf technische Grundlagen und Herausforderungen von Metaversen, ebenso wie auf aktuelle Trends, die Akzeptanz, das Immersionserleben, gesellschaftliche, wirtschaftliche und politische Chancen und Gefahren (vor allem im Hinblick auf Gerechtigkeit und Inklusion), die Sicherheit, psychische Integrität, Privatheit und Datenschutz, Identität, Körperlichkeit und Avatargestaltung, Zukunftsvisionen sowie Handlungsempfehlungen. Insgesamt

wurden über 1.400 Textstellen codiert. Der vorliegende Beitrag bezieht sich hauptsächlich auf die Aussagen der Befragten zur Altersverifikation und zur Vulnerabilität von Kindern und Jugendlichen in Metaversen, aber auch auf die Chancen, die solche immersiven Umgebungen jungen Menschen bieten.

3. Nutzungsrisiken von Metaversen für Kinder und Jugendliche

Die Nutzung von Metaversen birgt verschiedene Gefahren für Kinder und Jugendliche, die teils auch aus den sozialen Medien oder Online-Games bekannt sind. So sind Kinder und Jugendliche aufgrund ihrer noch nicht vollständig ausgeprägten Fähigkeit zur Selbstregulation besonders anfällig für exzessive und suchtähnliche Nutzungsweisen (Kim 2023). In Metaversen und Online-Gaming-Umgebungen ist hier bedeutsam, dass sich die Auswahl und Gestaltung von Avataren auch auf die Identitätsgestaltung junger Nutzenden auswirken (Fu u. a. 2025). Dies macht den potenziell unkontrollierten Erwerb virtueller Güter wie Kleidung oder Accessoires in Metaversen attraktiv.

Weitere mögliche Risiken sind Mobbing, Cyberbullying, Grooming und sexuelle Übergriffe, die sich aus den Interaktionen in Metaversen ergeben (Fiani u. a. 2024). Zwar sind diese Risiken auch aus sozialen Netzwerken bekannt (vgl. Europäische Kommission 2025, S.1), doch werden sie in Metaversen durch affektiv wirkende Avatar-Interaktionen, die Immersion und das Embodiment (also die Verschmelzung des menschlichen Bewusstseins mit dem virtuellen Körper in der VR; vgl. Wienrich 2023, S. 59) als besonders eindringlich erlebt.

In Metaversen ist zudem weder das tatsächliche Alter der Nutzenden von Avataren erkennbar, noch ist klar ersichtlich, ob sich dahinter überhaupt eine reale Person verbirgt. Insbesondere für Kinder und Jugendliche besteht dadurch die Gefahr, intensive parasoziale Beziehungen zu KI-basierten Avataren aufzubauen. Dies kann emotionale Abhängigkeiten fördern und manipulative Einflussnahmen, beispielsweise in Bezug auf Konsum oder politische bzw. weltanschauliche Einstellungen, begünstigen.

Kinder und Jugendliche weisen darüber hinaus häufig nur ein geringes Bewusstsein für Datenschutzrisiken auf. Dies ist in Bezug auf Metaversen besonders problematisch, da bei Nutzung von VR-Zubehör neben Verhaltensdaten auch biometrische Daten (z. B. Eye-Tracking, Stimm- und Be-

wegungsprofile, Herzfrequenz) sowie Informationen über die physische Umgebung erfasst werden (vgl. UNICEF 2023, S. 20).

4. Ethische Aspekte der Altersverifikation

Aus ethischer Sicht dienen Systeme zur Altersverifikation nicht nur dem Schutz von Kindern und Jugendlichen, sondern auch ihrer Teilhabe und Befähigung. Kinder sollten dazu befähigt werden, eine Kommunikationssituation bewerten zu können, um selbstbestimmt und kreativ in Metaversen aktiv zu sein. Altersverifikation kann, neben anderen Maßnahmen, dazu einen Beitrag leisten. Sie muss jedoch bestimmte ethisch begründete Kriterien erfüllen, um individuelle Rechte und gesellschaftliche Zielvorstellungen für ein sicheres und selbstbestimmtes Aufwachsen in digitalen Umgebungen zu wahren.

4.1 Schutz, Befähigung und Teilhabe

Vor dem Hintergrund der oben genannten Nutzungsrisiken gilt es, Kinder und Jugendliche in Metaversen bestmöglich zu schützen. Laut UN-Kinderrechtskonvention haben Kinder jedoch nicht nur ein Recht auf Schutz und Privatheit, sondern auch auf Befähigung und Teilhabe (Stapf u. a. 2023).

Medienmündigkeit ist ein wesentlicher Kern von Selbstbestimmung in digitalen Kontexten und umfasst die selbstbestimmte Nutzung, Produktion und kritische Reflexion medialer Angebote, Plattformen und Inhalte durch Heranwachsende. Daraus folgt, dass Kinder und Jugendliche zu einem selbstbestimmten Umgang mit neuen Technologien und der Partizipation an Angeboten wie Metaversen befähigt werden sollten.

In diesem Sinne werden aktuell verschiedene Lösungen diskutiert, u. a. Nachweise über die Herkunft von Avataren (Council of Europe and IEEE 2024; Witzleb 2025), altersgerechte Räume mit beschränktem Erwachsenenzugang oder die Einführung von Altersgrenzen für spezifische Angebote (Niestadt 2024). Die letztgenannten Ansätze sollen den unterschiedlichen Entwicklungsständen von Kindern und Jugendlichen ebenso gerecht wer-

den wie dem durchaus berechtigten Interesse, mit Erwachsenen in Kontakt zu treten (Brailovskaia u. a. 2025).¹

Einige Metaversen verfügen bereits über Bereiche, die nur von Personen einer gewissen Altersgruppe genutzt werden sollen, beispielsweise „ab 18 Jahren“-markierte Räume in *Metas Horizon Worlds*, in denen u. a. „intensive Gewalt, sexuelle Inhalte, vulgäre Sprache und/oder reglementierte Güter wie Tabak oder Alkohol“ präsent sein können (Meta 2025). In *VRChat* finden sich wiederum Clubs zum Feiern und Tanzen, die ebenfalls nur ab 18 Jahren zugänglich sind (Krell/Wettmann 2023). Dabei stellt die Plattform sogenannte Badges aus, die für andere Nutzende gemeinsam mit dem Namen des Avatars sichtbar sind und ihnen ermöglichen, nur mit Volljährigen zu interagieren. Dennoch mangelt es solchen Räumen bislang an geeigneten technischen Verifikationsmaßnahmen, um das Alter der Nutzenden sicher festzustellen, bzw. um altersgerechte Zugänge zu schaffen. Entsprechende Maßnahmen wären dann „nicht nur zu begreifen als Durchsetzungsinstrument für harte Alters- und Zugangssperren, sondern [...] eher als Schlüssel, um Voreinstellungen zu steuern, die [...] altersangemessene [sowie anonyme] Nutzungserfahrungen ermöglichen“ (I13).

In sogenannten „Walled Garden“-Formaten sind Austausch, Experimentieren und Befähigung von Kindern und Jugendlichen unter geschützten Bedingungen möglich. Zugänge können dann altersdifferenziert geöffnet werden – bei jüngeren Kindern unter elterlicher Begleitung, während ältere Jugendliche zunehmend eigenverantwortlich handeln können. Ein solcher gestufter Ansatz führt „schrittweise an eine gesunde, eigenverantwortliche und gemeinschaftsfördernde Mediennutzung“ heran (I13), womit Teilhaberechte und informationelle Selbstbestimmung gewahrt bleiben.

Pauschale Zugangsverbote für Personen unter einer bestimmten Altersgrenze zu sämtlichen Metaversen – analog zu dem kürzlich in Australien in Kraft getretenen (und in Deutschland aktuell diskutierten) Social-Media-Verbot für unter 16-Jährige (Stapf/Hecktor 2026) – werden der oben definierten Zielsetzung von Schutz, Befähigung und Teilhabe indes nicht gerecht. Kindern und Jugendlichen blieben hierdurch möglicherweise positive und für ihre Entwicklung wichtige Erfahrungen verwehrt. Zudem besteht die Gefahr eines hemmenden Einflusses auf die kindliche Befähigung zum kritischen Umgang mit der Technologie, die sonst nur noch aus theoretischer Distanz erworben werden könnte (I13). Weiterhin werden durch

1 Als weiterer Ansatz wird die virtuelle Begleitung von Kindern und Jugendlichen durch Erwachsene in Form eines Avatars vorgeschlagen (I14).

solche pauschalen Ausschlüsse die „Erziehungsrechte und -möglichkeiten von Eltern und Erziehungsberechtigten“ potenziell unterlaufen (Dreyer 2025).

Aus ethischer Sicht dienen Systeme zur Altersverifikation somit nicht nur dem Schutz von Kindern und Jugendlichen, sondern ermöglichen auch ihre Teilhabe an altersgerechten Angeboten und ihre Befähigung zu einem kritischen Umgang mit Metaversen.

4.2 Normative Kriterien für die Ausgestaltung der Altersverifikation

In der digitalen Kommunikation ist die Ausgestaltung von Infrastrukturen und Diensten ein zentraler Faktor für individuelle und gesellschaftliche Handlungsoptionen. Designlösungen bestimmen, welche Entscheidungen Nutzende von Metaversen überhaupt treffen können. Systeme zur Altersverifikation müssen daher ausreichend begründete Kriterien erfüllen, um individuelle Rechte und ethisch akzeptable Wertvorstellungen zu wahren.

Zentral ist zunächst, dass ihre Einführung nicht zur Etablierung einer *Überwachungsinfrastruktur* führen darf. Ein flächendeckender, verpflichtender Einsatz von Altersverifikationssystemen wäre unverhältnismäßig, da er „Eingriffe in die Informations- und Kommunikationsfreiheiten aller Nutzenden“ bedeuten würde (Dreyer 2025). Denn je intensiver Plattformen die Identität oder das Alter ihrer Nutzenden überprüfen müssen, desto stärker werden anonyme oder pseudonyme Teilhabeformen eingeschränkt – Formen, die für demokratische Partizipation, freie Meinungsäußerung und insbesondere für vulnerable Gruppen von erheblicher Bedeutung sind. Damit ergeben sich drei wesentliche Voraussetzungen für die Etablierung von (Alters-)Verifikationssystemen:

Erstens braucht es einen *risikobasierten Ansatz*, sodass Altersverifikationen nur dann eingesetzt werden dürfen, wenn entsprechende Risiken für die Entwicklung von Kindern und Jugendlichen bestehen. Sie fungieren dann weniger als Schranken, die Nutzende von bestimmten Inhalten und Funktionen aussperren, sondern vielmehr als Weichen, die sie in passende, altersadäquate und sichere Umgebungen führen (Meineck 2025) – und auf diese Weise auch Befähigung und Teilhabe ermöglichen.

Zweitens müssen Verifikationssysteme als solche mit *informationeller Selbstbestimmung, digitaler Souveränität und Privatheit* vereinbar sein. Die Befragten heben in diesem Zusammenhang den Wert und die Bedeutung von Anonymität und Pseudonymität hervor. Ein Vertreter eines deutschen

Digitalverbands betont die „Chance [...], sich einfach als der auszugeben, der man gerne sein möchte“ (I16). Ähnlich äußern sich auch ein Digitalpolitiker (I17) sowie ein Experte für Kinder- und Jugendmedienschutz (I13). Zentral ist diese Möglichkeit sowohl für die persönliche Entfaltung in der öffentlichen Kommunikation als auch für die freie Meinungsäußerung; andernfalls könnte das Gefühl des Überwachtwerdens zur *Selbstzensur* der Nutzenden führen (I19).

Verifikationssysteme sollten darum nur solche personenbezogenen Daten erheben, die für die gegenständliche Verifikation – hier die Überprüfung des Alters – zwingend notwendig sind. Wenn Plattform-Betreiber lediglich die Altersgruppe der Nutzenden feststellen können und sonst keine weiteren Informationen erhalten, dann sei dies im Hinblick auf Privatheit und informationelle Selbstbestimmung „sogar besser [...] als] im Laden, wo ich meinen Ausweis der Verkäuferin oder dem Verkäufer unter die Nase halte und die im Prinzip alle meine Daten auf dem Ausweis lesen können“ (I18). Neben Art und Umfang der erhobenen Daten ist auch relevant, wo und wie sie verarbeitet werden und wer darauf Zugriff hat. Maßgeblich ist hierbei die Gewährleistung einer sicheren, verschlüsselten Datenübermittlung (vgl. auch Europäische Kommission 2025, S. 15; zu den Sicherheitsrisiken durch Altersverifikationsfirmen s. Booth 2025). Ferner sollte die Datenerhebung zur Altersverifikation nicht mit anderen Datenerhebungen auf Online-Plattformen verknüpft und darum auch nicht durch den Betreiber des jeweiligen Metaversums selbst durchgeführt werden, sondern durch einen unabhängigen Dritten (vgl. Europäische Kommission 2025, S. 11). Erforderlich ist zudem eine wirksame Kontrolle der datenerhebenden Institutionen, um möglichem Missbrauch entgegenzuwirken.

Drittens sind aus ethischer Perspektive auch *Nicht-Diskriminierung* und *Zugangsgerechtigkeit* relevant, wozu besonders eine *Nutzungsfreundlichkeit* von Altersverifikationssystemen beitragen kann, die auch für deren Akzeptanz und praktische Umsetzung von Bedeutung ist (Schellenberg/Mikát 2022). Entsprechende Systeme sollten unabhängig von „Behinderung, Sprache, ethnischer Zugehörigkeit, Geschlecht, Religion und Zugehörigkeit zu einer Minderheit“ nutzbar sein (Europäische Kommission 2025, S. 15), um eine gleichberechtigte Partizipation an digitalen Anwendungen wie Metaversen zu ermöglichen. Faktische Ausschlüsse – etwa durch die Beschränkung auf bestimmte nationale Identitätsnachweise, die vorausgesetzte Mitwirkung Erwachsener oder komplexe technische bzw. sprachliche Anforderungen – sind daher zu vermeiden (Meineck 2025). Der Nicht-Diskriminierung dienen niedrigschwellige, altersgerechte und transparente *Korrektur- und Unterstüt-*

zungsoptionen bei technischen Fehlern oder Bedienungsproblemen (I18). Um unberechtigten Ausschlüssen entgegenzuwirken, müsste es Nutzenden demnach möglich sein, die Ergebnisse einer Verifikation überprüfen und revidieren zu lassen oder eine alternative Form der Verifikation zu beantragen, wenn das Verifikationssystem den Zugang zu einem bestimmten Dienstangebot etwa irrtümlich verweigern sollte. In diesem Zusammenhang sind kindgerechte Hilfsfunktionen (z. B. durch Erklärungen in einfacher Sprache), technische Assistenz (z. B. via Chat) sowie eine klar verständliche Offenlegung der Gründe für etwaige Zutrittsverweigerungen integrale Bestandteile einer verantwortungsvollen Systemgestaltung. Dies würde nicht nur die Selbstwirksamkeit junger Nutzenden fördern, sondern zugleich ihr Vertrauen in digitale Schutzmechanismen stärken.

5. Rechtliche Verpflichtungen und Anforderungen an Altersverifikationen

Ob geltendes Recht den Einsatz von Verifikationsmaßnahmen in Metaver- sen bereits reguliert und dabei auch die drei zuvor aufgeworfenen, zen- tralen Anforderungen berücksichtigt, ergibt sich unionsweit primär aus dem Gesetz über digitale Dienste (Digital Services Act, DSA) als Teil des Plattformrechts sowie der Datenschutz-Grundverordnung (DSGVO) als Fundament des Datenschutzrechts.

5.1 Risikobasierte Jugendschutzmaßnahmen nach dem DSA

Der DSA soll als unmittelbar geltende Verordnung EU-weit einheitlich die allgemeine Sicherheit digitaler Dienste bzw. Dienste der Informations- gesellschaft² erhöhen, indem die Anbieter digitaler Dienste zu verschiede- nen Sicherheitsmaßnahmen verpflichtet werden, darunter auch zu Jugend- schutz-Maßnahmen. So haben „Anbieter sehr großer Online-Plattformen“ mit bestimmten jährlichen Nutzendenzahlen und Umsätzen nach Art. 35 DSA Risikominderungsmaßnahmen zu ergreifen, z. B. „Werkzeuge zur Al- tersüberprüfung“ (Art. 35 Abs. 1 S. 2 lit. j DSA). Nach dem Wortlaut der Norm gehören „Werkzeuge zur Altersüberprüfung“ aber nur „unter Um-

2 Art. 3 lit. a DSA verweist als Definition für digitale Dienste auf Art. 1 Abs. 1 lit. b Richtlinie (EU) 2015/153, wonach es sich um „Dienstleistung(en) der Informations- gesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“ handelt.

ständen“ zu solchen Risikominderungsmaßnahmen dazu, sodass es sich bei Art. 35 Abs. 1 S. 2 DSA um eine nicht-abschließende Liste an Maßnahmen handelt, deren konkrete Auswahl sich an den spezifischen Risiken eines digitalen Dienstes orientiert. Diese Risiken sind wiederum im Rahmen einer von Art. 34 DSA vorgesehenen Risikobewertung festzustellen.

Demgegenüber fordert Art. 28 DSA sämtliche (und nicht nur sehr große) Anbieter von Online-Plattformen auf, „geeignete und verhältnismäßige Maßnahmen“ zu ergreifen, um den Zugriff auf entwicklungsschädigende Inhalte durch Minderjährige einzuschränken und „für ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen“ zu sorgen. Nach ErwG 71 DSA trifft die Pflicht alle Online-Plattformen, die Risiken für Minderjährige bergen und für solche zugänglich sind, etwa wenn die Allgemeinen Geschäftsbedingungen (AGB) die Nutzung erlauben oder Daten der Nutzenden verarbeitet werden, aus denen ihr Alter hervorgeht.

Zusätzlich geltende Leitlinien zu Art. 28, die als Bewertungsrahmen für die Angemessenheit der Maßnahmen nach Art. 28 DSA dienen (Europäische Kommission 2025, Rn. 3), und besonders die Ausgestaltung von Altersverifikationen (nach den Leitlinien sog. „Altersfeststellungen“) in den Fokus nehmen, beziehen sich dabei auf die Risiken der 5C-Typologie³ (Europäische Kommission 2025, Anhang) nach der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD 2021). Darunter fallen u. a. Inhalts- und Kontaktrisiken, die – wie eingangs beleuchtet – bei vielen Metaversen in hohem Maße vorhanden sein können (Steenbergen 2026).

Der ersten zentralen Anforderung, Altersverifikationssysteme nach einem *risikobasierten Ansatz* einzurichten, um u. a. die *Teilhabe* von Kindern und Jugendlichen nicht einzuschränken, wird durch den DSA somit bereits Rechnung getragen: Die Erforderlichkeit und die Ausgestaltung von Altersverifikationsmaßnahmen als mögliche Maßnahme nach Art. 28 Abs. 1 u. Art. 35 DSA ist davon abhängig, ob eine Online-Plattform wie ein Metaversum Risiken für Minderjährige birgt und wie hoch diese Risiken jeweils sind.

5.2 Wahrung von Nicht-Diskriminierung und Zugangsgerechtigkeit

Ferner greifen die Art. 28 DSA-Leitlinien auch die aufgeworfene Anforderung an *Nicht-Diskriminierung* und *Zugangsgerechtigkeit* auf, indem sie

3 Die 5C umfassen Inhaltsrisiken (content), Verhaltensrisiken (conduct), Kontaktrisiken (contact), Verbraucherrisiken (consumer) und Querschnittsrisiken (cross cutting risks).

fünf Merkmale vorschreiben, die Altersverifikationsmaßnahmen aufzuweisen haben: Genauigkeit, Zuverlässigkeit, Robustheit, Nicht-Intrusivität und die Nichtdiskriminierung selbst (Europäische Kommission 2025, Rn. 49). Dabei hat die Notwendigkeit der Genauigkeit zur Folge, dass bisher oftmals eingesetzte Eigenerklärungen wie die selbstständige Eingabe des Geburtsdatums fortan als ungeeignet gelten (Europäische Kommission 2025, Rn. 52, Steenbergen 2026, S. 154) – was im Hinblick auf die zuvor aufgeworfenen Risiken für Minderjährige zu befürworten ist. Stattdessen müssen Anbieter digitaler Dienste als präzisere Methode sog. „Altersüberprüfungen“ durchführen, wenn ihre Plattform hohe Risiken für Minderjährige aufweist. Eine solche Altersüberprüfung setzt eine verifizierte Identifizierung der Nutzenden voraus (Europäische Kommission 2025, Rn. 29).

Der *Nicht-Diskriminierung*, *Zugangsgerechtigkeit* und auch *Nutzungsfreundlichkeit* entgegenstehen könnte jedoch, dass nach den Leitlinien zumindest bei digitalen Diensten mit mittleren Risiken auch Altersschätzungen mittels Gesichts- oder Verhaltensprofil-Analysen ausreichend sind – dies, obwohl Altersschätzungen von der Europäischen Kommission selbst als weniger genaue Methode der Altersfeststellung eingestuft werden (Europäische Kommission 2025, Rn. 30 u. 33). Prinzipiell sollen Anbieter von Online-Plattformen durch die Zulässigkeit der Altersschätzung bei ihrer Pflicht unterstützt werden, mehr als eine Methode der Altersfeststellung anzubieten, damit Nutzende zwischen mehreren Methoden wählen können und nicht vereinzelt ausgeschlossen werden (Europäische Kommission 2025, Rn. 48). Vor dem Hintergrund, dass Altersschätzungen aber anfälliger für technische Fehler oder Bedienungsprobleme sein können (Jandt 2025, S. 72), ist fraglich, wie *nutzungsfreundlich* ihre alleinige Bereitstellung in der Praxis tatsächlich ist, und ob sie nicht auch negative Auswirkungen auf die *Teilhabe* von Kindern und Jugendlichen haben können, wenn fehlerhafte Altersschätzungen sie „[...] am Zugang zu Online-Plattformen hindern, auf die sie andernfalls zugreifen könnten“ (Europäische Kommission 2025, Rn. 33).

5.3 Datenschutzrechtliche Anforderungen zur Wahrung der Informationellen Selbstbestimmung und Privatheit

Altersschätzungen mittels Gesichts- oder Verhaltensprofil-Analysen werfen abschließend Fragen zur Wahrung der *informationellen Selbstbestimmung*, *digitalen Souveränität und Privatheit* als weitere Anforderung auf. Insbesondere stellt sich die Frage, ob geltendes Recht diese Anforderung bei

der Umsetzung von Altersfeststellungsmethoden bereits angemessen berücksichtigt.

Das Recht auf informationelle Selbstbestimmung als Ausprägung des Grundrechts auf Datenschutz (Art. 8 GRCh) wird maßgeblich durch die DSGVO geschützt, sodass entscheidend ist, ob die DSGVO beim Einsatz von Altersfeststellungen überhaupt Anwendung findet, und ob Anwender von Altersfeststellungen überhaupt entsprechende Maßnahmen nach der DSGVO umsetzen müssen. Immerhin wird dem Anschein nach nur eine abstrakte Information wie das Alter eines Nutzenden erfasst.

Als EU-weit unmittelbar anzuwendende Verordnung reguliert die DSGVO jede Verarbeitung personenbezogener Daten. Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO alle Informationen, „die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“, z. B. der Realname eines Nutzenden. Durch das sehr weite Begriffsverständnis fallen aber auch Informationen darunter, die erst gemeinsam mit anderen Informationen die Identität des Nutzenden preisgeben (z. B. Identifikationsnummern, IP-Adressen oder physiologische Merkmale wie das Alter). Nach aktueller Rechtsprechung und einem relativen Verständnis ist der Personenbezug jedoch dynamisch zu bestimmen; entscheidend ist, ob eine Stelle, der Informationen vorliegen, über (zusätzliche) Informationen verfügt, die eine Zuordnung zur betroffenen Person ermöglichen.⁴

Im ersten Schritt einer (Alters-)Verifikation muss das gegenständliche Datum (z. B. das Alter) einer Person (z. B. eines Metaverse-Nutzenden) von einer Stelle (z. B. einer Behörde) mittels einer vertrauenswürdigen Quelle (z. B. einem Ausweisdokument) festgestellt werden. Im zweiten Schritt muss das Ergebnis von der Stelle, die das Ergebnis benötigt (z. B. dem Metaverse-Betreiber), abgerufen oder eingesehen werden. Zudem ist eine überprüfbare Zuordenbarkeit zwischen dem Datum und dem den Nachweis präsentierenden Nutzenden erforderlich, damit festgestellt werden kann, ob das Ergebnis bzw. abgefragte Datum dem Nutzenden auch tatsächlich zugehörig ist, und nicht etwa ein Kind den Ausweis der Sorgeberechtigten nutzt. Während es für die Frage des Personenbezugs beim zweiten Schritt darauf ankommt, inwiefern die prüfende Stelle wie der Metaverse-Betreiber durch den Nachweis und die Zuordnung den Nutzen-

4 EuGH, Urteil vom 4.9.2025, Rechtssache C-413/23P, Europäischer Datenschutzbeauftragter (EDSB) ggf. einheitlicher Abwicklungsausschuss (SRB), NJW 2025, S. 3415–3423, Rn. 76 f.

den identifizieren kann, müssen Nutzende im ersten Schritt allenfalls ihre Identität preisgeben.

Aufgrund der weitreichenden Definition der Verarbeitung nach DSGVO genügt bereits eine Abfrage personenbezogener Daten, um eine Verarbeitung zu bejahen. Eine (dauerhafte) Speicherung des Ergebnisses ist keine Voraussetzung. Demnach werden Verifikationsmaßnahmen insgesamt ungeachtet ihrer Ausgestaltung als Altersprüfung, Altersschätzung oder zu sonstigen Verifikationszwecken der DSGVO unterliegen.

Da Betreiber eines Metaversums eine oder mehrere Methoden der Altersverifikation in den Nutzungsprozess ihrer Plattform einbinden müssen, entscheiden sie zugleich über die Zwecke und Mittel der mit der Verifikation verbundenen Verarbeitung und gelten damit als Verantwortliche nach Art. 4 Nr. 7 DSGVO (Geissler/Schindwein 2025).

Damit haben sie wiederum die Datenschutz-Grundsätze nach Art. 5 DSGVO einzuhalten, wozu insbesondere der *Datenminimierungsgrundsatz* (Art. 5 Abs. 1 lit. c DSGVO) gehört, der voraussetzt, dass sämtliche an den Verifikationsmaßnahmen Beteiligte nur solche personenbezogenen Daten erheben und erhalten, die sie für den Zweck der Verifikation auch tatsächlich brauchen, ebenso wie den *Zweckbindungsgrundsatz* (Art. 5 Abs. 1 lit. b DSGVO), nach dem Verifikationsmaßnahmen u. a. – wie zuvor gefordert – so betrieben und implementiert werden müssen, dass keine Verknüpfung zwischen den zur Altersverifikation erhobenen Daten und den bei der Nutzung einer Plattform erhobenen Daten erfolgt.

Zur Einhaltung der Grundsätze haben Verantwortliche technische und organisatorische Maßnahmen nach Art. 25, 32 DSGVO zu ergreifen, die von der DSGVO – ähnlich wie Art. 28 und Art. 35 DSA – aufgrund des risikobasierten Ansatzes und der Technologieneutralität grundsätzlich offengehalten werden. Es besteht somit zwar keine zwingend einzuhaltende Liste mit Anforderungen, bestimmte Maßnahmen wie eine eingangs geforderte verschlüsselte Übermittlung der Daten werden in der DSGVO aber explizit als Maßnahme genannt und zählen mittlerweile oftmals zur gängigen Praxis. Zusätzlich ergeben sich erforderliche Maßnahmen teilweise bereits aus den Art. 28-DSA-Leitlinien: Dazu gehört z. B. die Einbindung eines Dritten⁵ zur Durchführung der Identitätsabfrage statt durch den Be-

5 Für solche Datenverarbeitungen sieht die DSGVO verschiedene Konstellationsmöglichkeiten vor, z. B. die Ausgestaltung als gemeinsame Verantwortlichkeit nach Art. 26 DSGVO oder als Auftragsverarbeitung nach Art. 28 DSGVO, wobei die Ausgestaltung vom konkreten Sachverhalt abhängt.

treiber eines Metaversums selbst (Europäische Kommission 2025, Rn. 41 u. 53). Indem Nutzende dadurch gegenüber dem Betreiber eines Metaverse weiterhin pseudonym auftreten können, trägt eine solche Einbindung und Trennung der Prozesse wiederum zur Datenminimierung bei. Als weitere Maßnahme könnten eingebundene Dritte das Ergebnis der Verifikation (z. B. die Zuordnung zu einer bestimmten Altersgruppe) dem Nutzenden oder dem Betreiber des Metaversums – wenn immer möglich – als einfache Ja- oder Nein-Antwort statt als genaues Geburtsdatum oder genaues Alter bereitstellen. Die Art. 28-DSA-Leitlinien empfehlen für diesen Prozess die Verwendung der geplanten europäischen Brieftasche für die Digitale Identität (European Digital Identity-Wallet, EUDI-Wallet)⁶ nach der eIDAS-2-Verordnung, die europäischen Bürgerinnen und Bürgern als europaweit einheitliche Lösung für verifizierbare Identitätsnachweise (Europäische Kommission 2025, Rn. 1 ff.) voraussichtlich ab 2027 zur freiwilligen Nutzung zur Verfügung stehen wird.

Allerdings ist zu berücksichtigen, dass technische und organisatorische Maßnahmen nicht erst beim Betrieb von Verifikationsmechanismen ansetzen, sondern bereits bei der Implementierung von datenverarbeitenden Technologien. Vor dem Hintergrund, dass von der Europäischen Kommission gestattete Altersschätzungen regelmäßig die Verarbeitung großer Mengen (verhaltensbezogener) personenbezogener Daten oder Daten besonderer Kategorien nach Art. 9 DSGVO wie biometrische Daten für Gesichtsanalysen erfordern (Kunz/Waldmann 2025b), ist daher fraglich, ob Altersschätzungen überhaupt die Grundsätze an Datensparsamkeit und -minimierung einhalten können.

Neben den Datenschutzgrundsätzen haben Betreiber von Metaversen als Verantwortliche zudem die Umsetzung der datenschutzrechtlichen Betroffenenrechte nach Art. 12 ff. DSGVO zu gewährleisten. Im Zuge dessen müssen Nutzende nicht nur über den Vorgang der Altersverifikation transparent informiert werden, im Rahmen des Rechts auf Löschung sowie Berichtigung muss es ihnen auch möglich sein, ihre personenbezogenen Daten – wozu auch der Altersnachweis gehört – beim Metaverse-Betreiber und eingebundenen Dritten löschen bzw. berichtigen zu lassen. Dies setzt insbesondere eingangs hervorgehobene *Korrektur- und Unterstützungsoptionen* während der Altersverifikation voraus, aber auch im Anschluss. Um die Richtigkeit der Daten im Sinne des Richtigkeitsgrundsatzes nach Art. 5

6 Siehe dazu auch eine entsprechende App zur Altersverifikation, das sogenannte Mini-Wallet, welches von der EU-Kommission im April 2026 vorgestellt wurde.

Abs.1 lit. d DSGVO von vornherein zu gewährleisten, sollten Nutzende rechtzeitig oder regelmäßig gebeten werden, den Nachweis zu erneuern, damit Betreiber von Metaversen die entsprechende Altersgruppe aktualisieren können, wenn ihnen das genaue Geburtsdatum nicht bekannt ist und eine selbstständige Aktualisierung somit ausscheidet.

Insgesamt besteht durch ein Zusammenspiel zwischen DSA, den zugehörigen Leitlinien sowie den Grundsätzen der DSGVO und dem dazugehörigen Aufsichtsregime durch Aufsichtsbehörden somit bereits ein rechtliches Fundament, um eine ethische Ausgestaltung von Altersverifikationssystemen anzustreben und sowohl die Privatheit als auch informationelle Selbstbestimmung als eine der drei wesentlichen Anforderungen wirksam durchzusetzen. Allein die von der Europäischen Kommission eingeräumte Möglichkeit zum Einsatz von Altersschätzungen bei Plattformen mit mittleren Risiken wahrt die Rechte der betroffenen Nutzenden nicht vollständig. Gerade aus Sicht der Datensparsamkeit bleiben Altersüberprüfungen die bevorzugte und rechtssichere Methode, wenn je nach Anlass nur die Altersgruppe der Nutzenden mitgeteilt wird.

6. Technische Umsetzung einer datenschutzfreundlichen Altersverifikation

Aktuelle Praktiken der Altersverifikation nutzen unzuverlässige und für Metaversen ungeeignete Verfahren. Wirksame und datenschutzfreundliche Verfahren sind dagegen auf Basis von Self-Sovereign Identity (SSI) möglich und auch für die Nutzung in Metaversen geeignet, da sie die flexible, kryptografisch gesicherte Ausstellung von Identitätsnachweisen ermöglichen und deren Nutzung unter der Kontrolle der betroffenen Nutzenden stellen.

6.1 Aktuelle Praxis der Altersverifikation

Altersverifikationsverfahren werden in der Praxis derzeit meist nur unzureichend umgesetzt. Entweder findet keine zuverlässige Altersverifikation, sondern lediglich eine Eigenerklärung statt, oder die Verfahren sind nicht datenschutzfreundlich, da mehr personenbezogene Daten als notwendig preisgegeben werden müssen (Kunz/Waldmann 2025b). Zu den Verfahren, die beispielsweise bei Social-Media-Diensten zum Einsatz kommen, zählen neben der Eingabe des Alters das Hochladen von Ausweiskopien (teilweise in Kombination mit Video-Selfies zum Abgleich), Video-Selfies mit KI-ge-

stützter Altersschätzung, Altersschätzung anhand der Online-Aktivitäten der Nutzenden sowie Social-Vouching, bei dem den Nutzenden bekannte Personen aufgefordert werden, das angegebene Alter zu bestätigen.

Unter aktuellen Metaversen nutzt *VRChat* einen Drittanbieter für die Altersverifikation, der Nutzende auffordert, über ihre Kamera ein offizielles Ausweisdokument zu präsentieren, anhand dessen das Alter festgestellt wird. Darüber hinaus haben Nutzende über 18 Jahre bei *VRChat* die Möglichkeit, nach erfolgreicher Altersverifikation ihrem Profil ein „18+“-Badge hinzuzufügen, das sie für andere Nutzende sichtbar machen können (VRChat 2025; s. Abschn. 4.1). Auch hier müssen Nutzende folglich mehr personenbezogene Daten offenlegen als zwingend erforderlich, wenn auch nicht gegenüber dem Betreiber von *VRChat* selbst.

Eine datenschutzfreundlichere Möglichkeit der Altersverifikation bietet die Online-AusweisFunction (eID) des Personalausweises und des elektronischen Aufenthaltstitels. Diese stehen jedoch nur Personen zur Verfügung, die 16 Jahre und älter sind.

Aus unserer Sicht stellt eine Altersverifikation auf Basis von Self-Sovereign Identity (SSI) eine zuverlässige, flexible, datenschutzfreundliche und diskriminierungsarme Alternative zu den genannten Verfahren dar, indem sie datenminimierte Identitätsnachweise beliebiger (auch jüngerer) Nutzer ermöglicht. SSI wird bisher für die Altersverifikation noch nicht eingesetzt, bietet aber entscheidende Vorteile. Denn die Ausstellung und Überprüfung SSI-basierter Nachweise kann auf verschiedene Beteiligte verteilt werden, sodass der Bedarf an zentralen Behörden abnimmt. Zugleich werden proprietäre Unternehmenslösungen und Monopolstellungen im Identitätsmanagement vermieden.

6.2 Lösungsentwurf SSI-basierter Identitätsnachweise für Metaversen

Die mit SSI-basierten Identitätsnachweisen verbundenen Prozesse lassen sich nutzerzentriert und anwendungsnah gestalten. Im Zuge der *Teilhabe* und *informationellen Selbstbestimmung* können Nutzende und damit auch Kinder und Jugendliche durch SSI ihre digitalen Identitäten selbst verwalten und über die Weitergabe von Informationen selbst entscheiden. In der Regel wird eine öffentliche, gegenüber den verschiedenen Dienstleistern weitgehend neutrale Blockchain als zentrale Registrierungskomponente eingesetzt. Dadurch wird sichergestellt, dass die betroffenen Nutzenden zur Kontrolle ihrer Informationen nicht auf private Architekturen der datenverarbeitenden

Dienstleister angewiesen sind. Zugleich kann auch das Tracking von Nutzen- den und die Verkettung von Aktivitäten im Sinne der datenschutzrechtlichen *Zweckbindung* erschwert werden (Kunz/Waldmann 2025a; Schumm u. a. 2025). Die Identitätsdaten befinden sich im Besitz des betroffenen Nutzen- den, um nicht nur die einzelnen Identitätsattribute, sondern auch die damit verbundenen Aktionen zu kontrollieren. Damit entzieht sich SSI weitgehend der Kontrolle einer einzelnen Organisation, eines einzelnen Softwareanbieters oder einzelnen Dienstes (Schumm u. a. 2025).

Um unseren SSI-basierten Lösungsansatz verständlich zu machen, werden zunächst die Grundlagen von SSI kurz erläutert. SSI basiert auf zwei Grundbausteinen, den sogenannten dezentralen IDs (*Decentralized Identifier*, DID) und den verifizierbaren Identitätsdaten (*Verifiable Credentials*, VC). Beide werden durch das World Wide Web Consortium (W3C) spezifi- ziert (Sporny u. a. 2022; 2025). Ein Aussteller (*Issuer*) stellt einer Person (*Holder*) digitale Identitätsnachweise (VC) aus, die eine Behauptung über eine Person (*Subject*) enthalten und vom *Holder* in ihrer digitalen Brieffta- sche (Wallet) gespeichert werden. Der Aussteller hat die Identitätsdaten zu- vor geprüft, etwa durch Abgleich mit dem Personalausweis der betroffenen Person (*Subject*), und bestätigt durch eine digitale Signatur die Korrektheit der Daten. In der Regel werden beide Rollen, *Holder* und *Subject*, von der- selben Person eingenommen. Abb. 1 zeigt die grundlegenden Beziehungen der SSI-Rollen am Beispiel der Ausstellung eines Altersnachweises durch eine Meldebehörde an Nutzende als *Subject* und *Holder*.

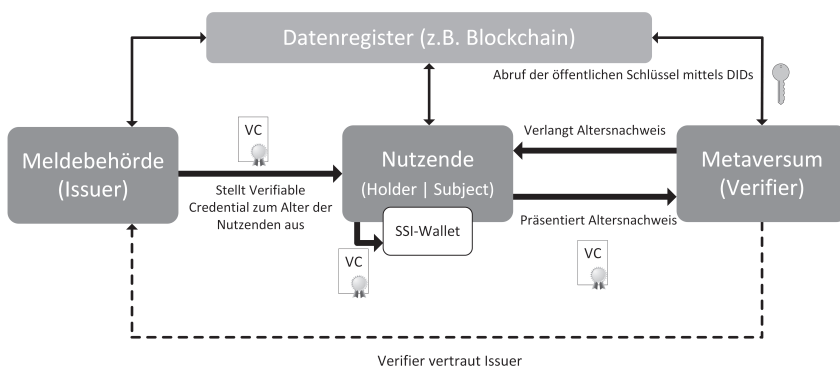


Abbildung 1: Die Beziehungen zwischen Issuer, Holder, Subject und Verifier am Beispiel einer Altersverifikation

Der Betreiber eines Metaversums kann nun als Dienstleister in der Rolle des *Verifier* von der nutzenden Person (*Holder* und *Subject* des VC) den Altersnachweis verlangen. Die nutzende Person als *Holder* des VCs kann entscheiden, ob sie der Anfrage nachkommen und das entsprechende VC präsentieren möchte. In diesem Fall signiert sie das ausgewählte VC und sendet es an den *Verifier*. Dieser kann nun die Gültigkeit und Korrektheit des Nachweises verifizieren.

Dazu sind die an einem VC beteiligten Parteien über ihre Kennungen (DIDs) eindeutig referenziert. Diese DIDs sind in öffentlich-zugänglichen, meist blockchainbasierten Datenregistern hinterlegt und dort mit weitergehenden Informationen (z. B. Links auf Einträge in der europäischen „Trusted List“ mit den zugelassenen VC-Ausstellern) verknüpft. Jede DID ist mit einem öffentlichen Schlüssel verbunden, wodurch die Identifizierung eines *Subjects* mit der Authentifizierung eines *Holder*s auch kryptografisch gesichert ist. Ein *Verifier* kann die öffentlichen Schlüssel über das Datenregister abrufen und damit das vom *Holder* präsentierte VC verifizieren.

Auf Basis von SSI können beliebige Beziehungen zwischen beliebigen *Holdern*, *Subjects*, *Issuern* und *Verifiern* abgebildet werden. So können sich die vom *Holder* in seinem Wallet verwalteten Identitätsnachweise auch auf ein anderes *Subject* beziehen, beispielsweise eine andere Person, eine Organisation, ein physisches oder digitales Objekt (z. B. einen Avatar). Ein *Holder* kann beliebig viele DIDs besitzen. Im Gegensatz zu herkömmlichen Registrierungsstellen werden die eigentlichen Identitätsdaten aber nicht in einem Datenregister verwaltet, sondern unterliegen der Kontrolle des jeweiligen *Holder*s in dessen Wallet. Voraussetzung ist, dass der *Verifier* dem betreffenden *Issuer* vertraut, die Identitätsdaten des *Subjects* ausreichend geprüft zu haben. Umgekehrt müssen die *Issuer* die *Verifier* gar nicht kennen und nicht mit ihnen kommunizieren. Die *Issuer* erfahren somit nicht, wann und für welche Dienste die VCs zum Einsatz kommen, sodass die DIDs dem Schutz der Kommunikation und der Privatheit dienen.

6.3 Nutzung SSI-basierter Identitätsnachweise in Metaversen

In Metaversen lässt sich SSI auf vielfältige Weise nutzen. Ein Anwendungsfall betrifft das erstmalige Betreten eines Metaversums und die in den meisten Fällen damit verbundene Registrierung durch dessen Betreiber (Kunz/Waldmann 2025a). Der Betreiber kann einen Altersnachweis auf Basis eines VC von den Nutzenden verlangen, um so etwa rechtlichen

Verpflichtungen des Jugendschutz- bzw. Plattformrechts nach Art. 28 DSA nachzukommen. Gleichzeitig können damit aus ethischer Sicht altersangemessene Nutzungserfahrungen (s. Abschn. 4.1) ermöglicht werden. Die Altersnachweise sollten von einer offiziellen Meldebehörde (*Issuer*) nach einer Identifizierung (z. B. Vorlage einer Geburtsurkunde) ausgestellt werden. So wird eine vom DSA vorgesehene und zur Wahrung der Privatheit erforderliche *Verifikation durch unabhängige Dritte* gewährleistet; zugleich kann sich der Betreiber (*Verifier*) auf die Korrektheit der enthaltenen Daten verlassen. Betreiber von Metaversen übernehmen hingegen ausschließlich die Altersangabe aus dem Zertifikat und verknüpfen sie mit dem Konto des Nutzenden, ohne das Alter erneut zu bestimmen. Eine *Datenverknüpfung* von Aktivitäten der Nutzenden in der realen Welt mit Aktivitäten im Metaversum wird durch die getrennte Nutzung von Zertifikaten in der realen Welt und Zertifikaten der virtuellen Identitäten erschwert. Durch ihre insgesamt *datensparsame* Ausgestaltung dient der Lösungsansatz somit dem Schutz der Kommunikation und der Privatheit und beugt einer *Überwachungsinfrastruktur* vor.

Ein zweiter Anwendungsfall betrifft die Kommunikation zwischen zwei beliebigen Avataren in öffentlichen Räumen eines Metaversums. Da Avatare frei gestaltet werden können, ist es kaum möglich, vom Aussehen eines Avatars auf das Alter des dazugehörenden Nutzenden zu schließen. Auch hier sollen VCs als Identitätsnachweise eingesetzt werden, sodass Nutzende untereinander ihr Alter nachweisen können. Dies dient insbesondere dem Schutz von Kindern und Jugendlichen. Dabei ist nicht erforderlich, dass die Altersnachweise das exakte Lebensalter enthalten. Stattdessen ist es ausreichend, wenn sich der Nachweis lediglich auf eine Altersgruppe bezieht (z. B. „zwischen 13 und 16 Jahren“ oder „über 18 Jahre“) und diese nur dann für andere Nutzende sichtbar wird, wenn beide Seiten dem zugestimmt haben (s. Abb. 2). Die Nachweise sollen vom Betreiber des Metaversums ausgestellt werden, nachdem dieser im Rahmen der Registrierung das Alter der Nutzenden geprüft hat (vgl. erster Anwendungsfall in Abb. 1). Dies hat u. a. den Vorteil, dass keine Angaben über eine Meldebehörde in den Nachweisen enthalten sind und Nutzende beim Prüfen somit keine weiteren Rückschlüsse (z. B. auf den Wohnort ihres Gegenübers) ziehen können.

Abb. 2 zeigt schematisch den Ablauf des Austauschs von Identitätsnachweisen zwischen zwei Nutzenden im Metaversum. Dies wird durch die explizite Anfrage eines der beiden Nutzenden initiiert. Nutzer N1 möchte in Gestalt des Avatars A1 mit Nutzer N2 kommunizieren. Bevor N2 dem zustimmt, möchte er zunächst das Alter seines Gegenübers wissen (Schritt

1). N1 hat den entsprechenden Nachweis in seinem Wallet gespeichert und kann ihn N2 präsentieren (Schritt 2). Nachdem N2 die Nachweise gesehen und erfolgreich verifiziert hat (Schritt 3), kann N2 informiert entscheiden, ob er mit N1 in Kontakt treten möchte. Auf die gleiche Weise kann N1 auch entsprechende Nachweise von N2 verlangen.

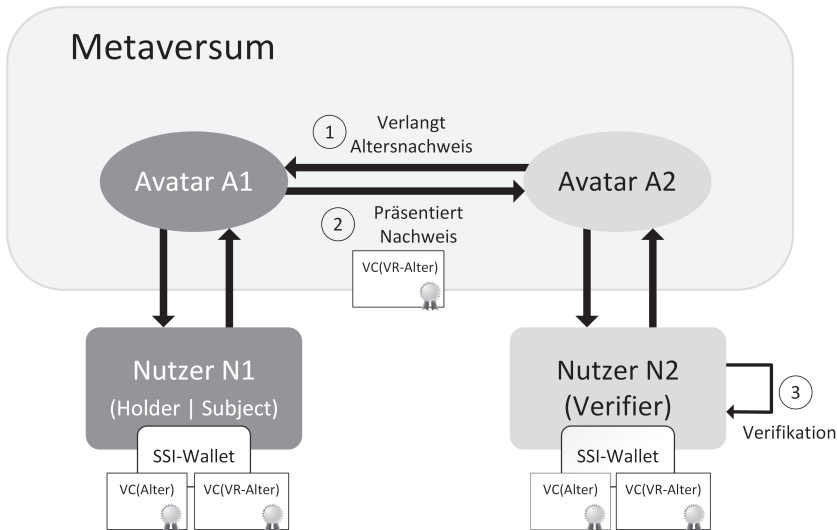


Abbildung 2: Nutzung von SSI in Metaversen

Aufgrund der Flexibilität von SSI sind weitere Nutzungsmöglichkeiten in Metaversen denkbar. So können beispielsweise VCs verwendet werden, um das Besitzverhältnis zwischen Nutzenden und ihren Avataren digital abzubilden. Solche VCs können Nutzenden im Metaversum helfen, zu erkennen, ob sie mit einem Avatar kommunizieren, der von einem anderen Nutzenden gesteuert wird, oder mit einem autonom agierenden, KI-gesteuerten Avatar (Kunz/Waldmann 2025a). Dies wirkt u. a. dem Risiko entgegen, dass insbesondere Kinder und Jugendliche intensive parasoziale Beziehungen zu KI-Agenten aufbauen und dann von diesen etwa in Bezug auf Konsum oder Weltanschauungen manipuliert werden könnten (s. Abschn. 3).

SSI-basierte Nachweise der Altersgruppe lassen sich zudem mit der Anwendung von Abstandsregelungen in Metaversen kombinieren, um Nutzende vor *virtuellen Belästigungen* durch andere Nutzende zu schützen.

Beispielsweise werden in *Horizon Worlds* und *VRChat* bereits „Safe Zones“ oder „Personal Space Options“ eingesetzt, die einen unsichtbaren Schutzkreis um den Avatar des Nutzenden herum bilden und dafür sorgen, dass sich andere Avatare nicht ohne gegenseitige Zustimmung nähern können (vgl. Krell/Wettmann 2023, S. 41). Denkbar wäre, dass solche Abstandsregelungen bzw. „Safe Zones“ für die Kommunikation und evtl. weitere Interaktionsmöglichkeiten für junge Nutzende erst geöffnet werden, nachdem sie gegenseitig einen Kontaktwunsch signalisiert und freiwillig ihre Altersgruppe ausgetauscht haben. Jeder Nutzende kann jederzeit die Kommunikation beenden und seine eigene „Safe Zone“ wieder gegenüber anderen verschließen. Ein solcher Ansatz ist besonders geeignet, um Kindern und Jugendlichen zu ermöglichen, mit Erwachsenen in Metaversen zu interagieren, sie aber auch vor entsprechenden unerwünschten Interaktionen zu schützen (Befähigung und Schutz; s. Abschn. 4.1). Wir schlagen folgende drei Aktionen vor, die zusammen ausgeführt werden müssen, um anderen Nutzenden einen Kontaktwunsch mitzuteilen:

- Unterschreitung eines bestimmten Abstands zum anderen Avatar für wenige Sekunden;
- Blickkontakt zum anderen Avatar;
- Ausführen einer bestimmten Geste (z. B. Winken) in Richtung des anderen Avatars.

Erwidert der andere Nutzer mit seinem Avatar den Blickkontakt und die Geste, wird im Hintergrund eine Bitte um Mitteilung der Altersgruppe (und ggf. weiterer freiwillig gegebener Informationen) an ihn gesendet. Ergänzend empfiehlt sich die Kennzeichnung von Avataren, die einem Nutzenden bereits aus einer früheren Begegnung bekannt sind. Sinnvoll ist die Angabe des Avatar-Namens (Benutzername), der Altersgruppe und der letzten Begegnung (ob diese zustande kam oder abgelehnt wurde).

Um zu vermeiden, dass Nutzende über verschiedene Angebote hinweg wiedererkannt, ihre dortigen Aktivitäten miteinander verknüpft und somit in ihrem Recht auf *Privatheit* und *informationelle Selbstbestimmung* eingeschränkt werden, ist aber unabdingbar, dass Nutzende verschiedene, voneinander getrennte Identitäten schaffen und nutzen können. Dafür ist nicht nur erforderlich, dass Nutzende verschiedene Nachweise (mit unterschiedlichen Schlüsseln und von unterschiedlichen Ausstellern) in staatlichen als auch privatwirtschaftlichen Wallets verwalten können, die SSI-Infrastruktur muss auch offen gestaltet werden und für viele unterschiedliche Aussteller von Nachweisen und Diensteanbietern nutzbar sein. Damit kann eine die

Privatheit gefährdende Verknüpfung und Profilbildung personenbezogener Daten zumindest erschwert werden.

Dennoch werden Dienstanbieter in der Rolle der *Verifier* den betroffenen Nutzenden zunächst überlegen bleiben, solange Dienstanbieter bestimmen können, welche persönlichen Attribute die Nutzenden präsentieren müssen. Denn Dienstanbieter könnten mehr Daten anfordern, als sie für den angegebenen Verarbeitungszweck benötigen, und Nutzende würden vom Dienstangebot ausgeschlossen werden, wenn sie der Präsentation aller angeforderten Daten nicht nachkämen (Schumm u. a. 2025). Um ausufernde Identifizierungspflichten zu verhindern, müssen daher SSI-Anwendungsprofile definiert werden, die den Betreibern von Metaversen vorschreiben, welche Daten sie von Nutzenden für welche Zwecke erheben dürfen. Das ursprüngliche SSI-Paradigma, welches ausgestellte Zertifikate ausschließlich in den Wallets des betroffenen Nutzenden speichert und die darin vom Nutzenden auch einfach gelöscht werden können, sollte dabei nicht aufgegeben werden.

7. Grenzen der Altersverifikation

Eine flächendeckende Einführung von Altersverifikationsmaßnahmen wird grundsätzlich kontrovers diskutiert. Insbesondere wird sie abgelehnt, wenn sie durch proprietäre, intransparente Verfahren großer Internetkonzerne realisiert wird (Open Letter 2026). Eine pseudonyme Altersverifikation, wie sie in diesem Beitrag beschrieben wurde, kann dagegen als transparent und datenschutzfreundlich gelten, bei einem Einsatz auf Basis des EUDI-Wallets interoperabel eingesetzt werden, und damit einen wichtigen Beitrag zum Schutz von Kindern und Jugendlichen in digitalen Räumen wie Metaversen leisten.

Dennoch kann eine SSI-basierte Altersverifikation nicht alle Probleme lösen – die spezifischen Herausforderungen von Metaversen sowie allgemeine Einschränkungen von (Alters-)Verifikationssystemen müssen auch für die vorgeschlagenen SSI-Prozesse Beachtung finden:

Erstens verbleibt trotz der im Vergleich zu Eigenerklärungen geringen Umgehungsmöglichkeiten ein Restrisiko, dass Kinder und Jugendliche dennoch Wege finden, Zugangssperren erfolgreich zu umgehen (Meineck 2025). Unverantwortliches Handeln kann damit nicht unterbunden werden. So müssten SSI-Wallets und die Präsentation der Zertifikate allein unter der *Kontrolle der Nutzenden* stehen, wozu eine herstellerunabhängige

Unterstützung von Wallets sowie eine Auswahl geeigneter, barrierefreier Authentifizierungsverfahren notwendig ist. Trotz Erfüllung dieser Voraussetzungen bleibt dennoch die Möglichkeit bestehen, dass eine volljährige Person ihr Smartphone mit Wallet und Altersnachweis mitsamt der zugehörigen PIN einer jüngeren Person überlässt oder nach erfolgreich erbrachtem Altersnachweis das Headset weiterreicht. Umgekehrt können auch Erwachsene die Verifikation von Minderjährigen nutzen, um sich als Kind auszugeben und sich auf diese Weise Kindern in missbräuchlicher Weise zu nähern (*Cybergrooming*). Kontinuierliche biometrische Authentifizierungsverfahren sind in dieser Hinsicht schwieriger zu umgehen, da sie einer Person sicherer zugeordnet werden können als eine einmalige PIN-Eingabe. Gerade im Hinblick auf Diskussionen und Kritik an Verifikationsmaßnahmen (Open Letter 2026) sowie auf die Sorge vor einer Überwachungsinfrastruktur bleibt die geringere Datenschutzfreundlichkeit solcher Verfahren aber hervorzuheben.

Zweitens gilt bezüglich der *Nutzungsfreundlichkeit und Unterstützung der digitalen Souveränität* zu beachten, dass in der Regel ein VR-Headset getragen wird, um ein Metaversum für immersive Erlebnisse zu nutzen, obwohl jede Form der Verifikation regelmäßig ein weiteres Medium erfordern wird – nach dem SSI-basierten Vorschlag ein entsprechendes Wallet, das meistens auf den Smartphones der Nutzenden gespeichert wird. Bei gleichzeitigem Tragen eines VR-Headsets wird die Nutzung des Smartphones eventuell eingeschränkt sein und die immersiven Erfahrungen gestört werden. Zudem müssen sich Nutzende (*Holder*) für gewöhnlich gegenüber ihrem Wallet authentifizieren (z. B. durch die Eingabe einer PIN), um die gespeicherten VCs anwenden und ihre privaten kryptografischen Schlüssel nutzen zu können. Aus diesem Grund erscheint eine Kopplung von Smartphone und VR-Headset etwa über Bluetooth sinnvoll, sodass Nutzende über das Sichtfeld ihres VR-Headsets mit dem Smartphone und dem darauf installierten Wallet interagieren können. Alternativ ist auch ein im VR-Headset installiertes Wallet oder die Nutzung eines cloudbasierten Wallets denkbar. Letzteres kann nutzungsfreundlich sein, stellt aber die alleinige Kontrolle des Wallets durch den Nutzenden infrage. Damit Kinder und Jugendliche ihre Altersnachweise zudem effektiv kontrollieren können, sind hier kindgerechte *Unterstützungs- und Hilfefunktionen* wie Erklärungen in einfacher Sprache oder direkte technische Assistenz entscheidend.

Drittens lässt sich selbst bei wirksamer Altersverifikation das Risiko schädlicher Online-Erfahrungen nicht vollständig eliminieren. Inhalts- und Interaktionsrisiken wie Mobbing, Stalking, sexuelle Belästigung, Desinfor-

mation, Hassrede oder die negative Beeinflussung von Selbstbildern können hinter der Altersschranke ungehindert stattfinden (Dreyer 2025).

8. Geteilte Verantwortung für sichere Metaversen

Altersverifikationen können den Zugang zu digitalen Räumen demnach zwar steuern, der Schutz von Kindern und Jugendlichen im digitalen Raum bleibt aber eine geteilte Verantwortung.

Kinder und Jugendliche benötigen zunächst die entsprechenden Kompetenzen, um Online-Risiken zu erkennen und verantwortungsvoll mit digitalen Angeboten umzugehen. Nur dann können sie sich selbstbestimmt und gefahrenbewusst in digitalen Räumen bewegen. Von *Bildungseinrichtungen und Sorgeberechtigten* braucht es daher Sensibilisierung, medienpädagogische Konzepte, kontinuierliche Begleitung und einen dialogischen Austausch mit Kindern und Jugendlichen.

Aufseiten der *Betreiber von Metaversen* muss die gesetzlich festgelegte und von der Europäischen Kommission vorgesehene Einbindung von Altersverifikationssystemen umgesetzt und das Ergebnis der Altersverifikation durchgesetzt werden. Dies ist Teil eines Bündels von Anforderungen an die Betreiber für eine altersgerechte, inklusive und sichere Ausgestaltung von Metaversen, zu der neben der Umsetzung der (datenschutz-)rechtlichen Anforderungen auch die Gewährleistung einer effektiven Inhaltsmoderation gehört.

Somit stehen *Politik und Gesetzgeber* nicht nur in der Verantwortung, Medienkompetenzerziehung finanziell zu fördern, ausreichende Weiterbildungsangebote für Erwachsene zu schaffen bzw. zu unterstützen und Beratungsangebote für Kinder und Jugendliche bei negativen Nutzungserfahrungen bereitzustellen, sondern vor allem bereits bestehende regulatorische Maßnahmen gegenüber den Betreibern von Metaversen wirksam durchzusetzen – dies über die EU hinweg und grenzüberschreitend. Hierzu sollten Betreiber von Metaversen möglichst verpflichtet werden, verbindliche, unabhängige und wahrnehmbare Klassifizierungen ihrer Angebote vorzunehmen, damit sich solche ihrer Verpflichtung zum Jugendschutz nicht schlichtweg entziehen, indem die Angebote einfach mit „Nur für Erwachsene“ gekennzeichnet werden.

Hinzu kommt, dass die Betreiber von Metaversen selbst zwar die Altersverifikation einbinden und Nutzungsschranken durchsetzen müssen, allerdings nicht maßgeblich an der Entwicklung von Altersverifikationsmecha-

nismen beteiligt sind, insbesondere wenn unabhängige Dritte eingebunden werden müssen. Es wird somit standardisierte Lösungen brauchen, deren Entwicklung durch *Politik und Gesetzgeber* vorangetrieben werden müssen. Dadurch treffen die datenschutzrechtlichen Anforderungen aber nicht ausschließlich die Betreiber von Metaversen, sondern besonders die *an der Entwicklung* von (SSI-basierten) Altersverifikationen *Beteiligten*. Insofern könnte die allgemeine Einführung von Altersverifikationssystemen auch ein Impuls für aktuelle Diskussionen im Rahmen der DSGVO-Reform sein, Anbieter bzw. Hersteller von Hard- und Software stärker „in das etablierte System datenschutzrechtlicher Pflichten“ einzubinden (DSK 2026, S. 4 f.).

9. Fazit

Kinder und Jugendliche sind in Metaversen besonderen Risiken ausgesetzt. Aus ethischer Perspektive können Altersverifikationsmaßnahmen dazu beitragen, sie vor diesen Risiken zu schützen, gleichzeitig aber auch ihre Teilhabe und Befähigung zum kritischen Umgang mit den entsprechenden Anwendungen fördern. Neben „Walled Garden“-Formaten, in denen Kinder und Jugendliche unter sich sind und sich im geschützten Raum bewegen und austauschen können, erlauben Altersverifikationssysteme, Zugänge zu Metaversen altersdifferenziert und teils auch eigenverantwortlich zu öffnen.

Dazu müssen entsprechende Altersverifikationssysteme aus ethischer Sicht u. a. Kriterien wie die Vermeidung von Diskriminierung sowie Datensparsamkeit erfüllen. Letzteres fordert der aktuelle Rechtsrahmen bereits anhand des weiten Anwendungsbereichs der DSGVO, der sich auch auf Verifikationsmaßnahmen erstreckt, sowie anhand des DSA, der die Anbieter von Online-Plattformen zum Einsatz von Altersverifikationsverfahren verpflichtet, wenn Plattformen mittlere bis hohe Risiken für die Entwicklung von Minderjährigen bergen. Durch die Immersion und Interaktion wird dies auf Metaversen regelmäßig zutreffen, sodass entsprechende Pflichten lediglich eine ausreichend effektive Rechtsdurchsetzung erfordern.

Doch selbst Altersverifikationssysteme, die den hier aufgeführten ethischen und rechtlichen Kriterien genügen, können nicht alle Gefahren für Kinder und Jugendliche in Metaversen beseitigen. Weitere Maßnahmen wie Inholdemoderation durch Betreiber sowie eine Sensibilisierung von Kindern und Jugendlichen können sie nicht ersetzen. Für einen wirksamen und nachhaltigen Schutz bei gleichzeitiger kritischer Befähigung braucht

es daher ein Zusammenspiel von technischen Maßnahmen, rechtlichen Rahmenbedingungen und pädagogischer Unterstützung.

Literatur

- Al-kfairy, Mousa; Alrabae, Saed und Alfandi, Omar (2025): Navigating the ethical landscape of metaverse. Challenges, solutions and governance initiatives. *IEEE Access*, Vol. 13, S. 79996–80018, 2025, <https://doi.org/10.1109/ACCESS.2025.3564498>.
- Booth, Robert (2025): Hack of age verification firm may have exposed 70,000 Discord users' ID photos. *The Guardian* vom 09.10.2025 URL: <https://www.theguardian.com/media/2025/oct/09/hack-age-verification-firm-discord-users-id-photos> (besucht am 29.01.2026).
- Brailovskaia, Julia; Buchmann, Johannes; Hertwig, Ralph; Metzinger, Thomas; Montag, Christian; Sadeghi, Ahmad-Reza; Schneider, Silvia; Spiecker gen. Döhm, Indra und Waldherr, Annie (2025): Soziale Medien und die psychische Gesundheit von Kindern und Jugendlichen. Diskussion Nr. 40, Halle (Saale): Nationale Akademie der Wissenschaften Leopoldina, URL: https://levana.leopoldina.org/servlets/MCRFileNodeServlet/leopoldina_derivate_01077/2025_Leopoldina_Diskussion_40.pdf (besucht am 29.01.2026).
- Council of Europe and IEEE (2024): The Metaverse and its impact on human rights, the rule of law and democracy. URL: <https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0> (besucht am 29.01.2026).
- Croll, Jutta und Krause, Thorsten (2024): Das Metaversum schlägt zurück?! Eine kinderrechtliche Perspektive. *merz. Zeitschrift für Medienpädagogik*, 68(3), S. 50–56. <https://doi.org/10.21240/merz/2024.3.16>.
- Datenschutzkonferenz (2026): Entschließung vom 10. März 2026. Stellungnahme zum Digital Fitness Check. Vorschläge zu Modifikationen der DSGVO. URL: https://www.datenschutzkonferenz-online.de/media/en/2026-03-10_DSK_Entschliessung-Digital_Fitness_Check.pdf.
- Dreyer, Stephan (21.03.2025): Virtuelle Schranken oder offene Scheunentore. Fünf Thesen zu verpflichtenden Altersüberprüfungen als Instrument des Jugendmedienschutzes. Mediendiskurs. URL: <https://mediendiskurs.online/beitrag/virtuelle-schranken-oder-offene-scheunentore-beitrag-772/> (besucht am 29.01.2026).
- Europäische Kommission (2025): Mitteilung der Kommission. Leitlinien (C/2025/5519) für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065. (C/2025/5519). URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:C_202505519 (besucht am 29.01.2026).
- Fiani, Cristina; Saeghe, Pejman; McGill, Mark und Khamis, Mohamed (2024): Exploring the perspectives of social VR-aware non-parent adults and parents on children's use of social virtual reality, *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 54, S. 1–25 <https://doi.org/10.1145/3652867>

- Fu, Yue; Schwamm, Samuel; Baughan, Amanda; Powell, Nicole M.; Kronberg, Zoe; Owens, Alicia; Izenman, Emily R.; Alsabeh, Dania; Hunt, Elizabeth; Rich, Michael; Bickham, David; Radesky, Jenny und Hiniker, Alexis (2025): Understanding children's avatar making in social online games. <https://doi.org/10.48550/arXiv.2502.18705>.
- Geissler, Ines und Schlindwein, Lisa (2025): Datenschutz in Metaversen. In: Selzer, Annika (Hrsg.), *Aktuelle Entwicklungen des Rechtsrahmens der Cybersicherheit und Privatheit*, Sammelband. Wiesbaden: Springer-Vieweg, S. 1–10. https://doi.org/10.1007/978-3-658-49640-1_1.
- Jandt, Silke (2025): Gesetzliches Mindestalter für soziale Netzwerke in Deutschland? *Zeitschrift für Rechtspolitik ZRP*, 3/2025, S. 69–72.
- Kim, Soyeon (2023): Emergence of the metaverse and psychiatric concerns in children and adolescents. *Journal of the Korean Academy of Child and Adolescent Psychiatry*, 34(4), S. 215–222. <https://doi.org/10.5765/jkacap.230047>
- Krell, Felix und Wettmann, Nico (2023): Corporeal interactions in VRChat. Situational intensity and body synchronization. *Symbolic Interaction*, 46(2), S. 1–23. <https://doi.org/10.1002/symb.629>.
- Kunz, Thomas und Waldmann, Ulrich (2025a): SSI-basierte Altersverifikation und Herkunftsnachweise für Avatare zum Schutz von Minderjährigen in Metaversen. In: Lucke, Ulrike; Stieglitz, Stefan; Uebernickel, Falk; Lamprecht, Anna-Lena und Klein, Maik (Hrsg.): *INFORMATIK 2025*. Bonn: Gesellschaft für Informatik, S. 173–187. https://doi.org/10.18420/inf2025_10.
- Kunz, Thomas und Waldmann, Ulrich (2025b): Online-Altersverifikation zur Gewährleistung des Minderjährigenschutzes. *Datenschutz und Datensicherheit*, 49(6), S. 384–389. <https://doi.org/10.1007/s11623-025-2108-1>.
- Livingstone, Sonja; Stoilova, Mariya und Nandagiri, Rishita (2019): *Children's data and privacy online. Growing up in a digital age*. London: London School of Economics and Political Science.
- Meineck, Sebastian (28.04.2025): Die trügerische Sicherheit von Alterskontrollen im Netz. Mediendiskurs. URL: <https://mediendiskurs.online/beitrag/die-truegerische-sicherheit-von-alterskontrollen-im-netz-beitrag-772/> (besucht am 29.01.2026).
- Meta (2025): Content-Richtlinien für Meta Horizon Worlds. URL: <https://www.meta.com/de-de/help/quest/481214418021533/> (besucht am 29.01.2026).
- Niestadt, Maria (2024): Protecting children in virtual worlds (the metaverse). URL: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762294/EPRS_ATA\(2024\)762294_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762294/EPRS_ATA(2024)762294_EN.pdf) (besucht am 29.01.2026).
- OECD (2021): Children in the digital environment. Revised typology of risks. URL: [https://one.oecd.org/document/DSTI/CDEP/DGP\(2020\)3/FINAL/en/pdf](https://one.oecd.org/document/DSTI/CDEP/DGP(2020)3/FINAL/en/pdf) (besucht am 15.04.2026).
- Open Letter (2026): Joint statement of security and privacy scientists and researchers on Age Assurance. URL: <https://csa-scientist-open-letter.org/ageverif-Feb2026> (besucht am 16.03.2026).

- Schellenberg, Stefan und Mikat, Claudia (2022): Die harten Inhalte finden sich auf Webseiten, nicht in Apps. Mediendiskurs, veröffentlicht im Februar 2022 URL: <https://mediendiskurs.online/beitrag/die-harten-inhalte-finden-sich-auf-webseiten-nicht-in-apps-beitrag-1024/> (besucht am 29.01.2026).
- Schnell, Rainer; Hill, Paul B. und Esser, Elke (2008): Methoden der empirischen Sozialforschung. München: Oldenbourg.
- Schumm, Daria; Müller, Katharina O. und Stiller, Burkhard (2025): Are we there yet? A study of decentralized identity applications. <https://doi.org/10.48550/arXiv.2503.15964>
- Sporny, Manu; Longley, Dave; Sabadello, Markus; Reed, Drummond; Steele, Orie und Allen, Christopher (2022): Decentralized identifiers (DIDs) v1.0. W3C recommendation. URL: <https://www.w3.org/TR/did-1.0/> (besucht am 29.01.2026).
- Sporny, Manu; Longley, Dave; Chadwick, David und Herman, Ivan (2025): Verifiable credentials data model v2.0. W3C recommendation. URL: <https://www.w3.org/TR/vc-data-model-2.0/> (besucht am 29.01.2026).
- Standards Australia (2024): Virtual fight for kids' safety. Standards Australia releases landmark draft standard to protect children in the metaverse. URL: <https://www.standards.org.au/news/virtual-fight-for-kids-safety-standards-australia-releases-landmark-draft-standard-to-protect-children-in-the-metaverse> (besucht am 29.01.2026).
- Stapf, Ingrid; Meinert, Judith; Heesen, Jessica; Krämer, Nicole; Ammicht Quinn, Regina; Bieker, Felix; Friedewald, Michael; Geminn, Christian; Martin, Nicholas; Nebel, Maxi; Ochs, Carsten; Watzinger, Lea und Bauer, Andreas (2023): Privacy and children's rights. Plattform Privatheit. <https://doi.org/10.24406/publica-793>.
- Stapf, Ingrid und Hecktor, Jana (2026): Digital Wellbeing von Kindern. Ethische Perspektiven auf die Social Media-Debatte angesichts aktueller Entwicklungen der KI. *Communicatio Socialis*, 59(1), S. 127–139.
- Stapf, Ingrid und Heesen, Jessica (2026): Digitale Kommunikation. Medienethik, Medienkompetenz. In: Bobbert, Monika und Sautermeister, Jochen (Hrsg.): *Handbuch Ethik und Psychologie*. Wiesbaden: Springer VS, S. 611–628.
- Steenbergen, Marina (2026): Die Altersfeststellung nach den Art. 28 DSA-Leitlinien im Metaverse. Das Ende der „Über-18-Jahre“-Buttons? *Datenschutz und Datensicherheit (DuD)*, 50(3), S. 152–157.
- UNICEF (2023): The metaverse, extended reality and children. URL: <https://www.unicef.org/innocenti/media/756/file/UNICEF-Innocenti-Rapid-Analysis-Metaverse-XR-and-children-2023.pdf> (besucht am 29.01.2026).
- VRChat (2025): Age Verification. URL: https://wiki.vrchat.com/wiki/Age_Verification (besucht am 29.01.2026).
- Wienrich, Karolin (15.11.2023): Psychologische Folgen. Vortrag im Rahmen der Veranstaltung „Lost in ‚Metaverse‘? Zur Verschränkung realer und digitaler Welten“. Deutscher Ethikrat, URL: <https://www.ethikrat.org/fileadmin/PDF-Dateien/Veranstaltungen/herbsttagung-2023-11-15-transkript.pdf> (besucht am 29.01.2026).
- Witzleb, Normann (2025): Children's privacy in XR applications. A rights-based approach. *Santa Clara High Technology Law Journal*, 41(1), S. 67–133. <https://doi.org/10.2139/ssrn.5287183>

