Technisches Papier zur Altersfeststellung

Bundesverband Digitale Wirtschaft (BVDW) e. V.
November 2026

Executive Summary

Die Altersfeststellung soll künftig eine wichtige Rolle für den Kinder- und Jugendschutz im digitalen Raum übernehmen. Über ihre konkrete Ausgestaltung, technische Implementierung und Einbettung in bestehende regulatorische Strukturen sind jedoch noch zahlreiche Fragen offen. Im Mittelpunkt steht dabei die Frage, wie Altersgrenzen und altersbezogene Schutzmaßnahmen wirksam umgesetzt werden können, ohne Datenschutz, Nutzungsfreundlichkeit, digitale Teilhabe und den offenen Zugang zu digitalen Angeboten unverhältnismäßig einzuschränken. Das vorliegende Papier ordnet die verfügbaren Verfahren, ihre technischen Grundlagen sowie die damit verbundenen regulatorischen und praktischen Anforderungen ein.

Als übergeordneten Begriff verwendet das Papier in Anlehnung an den Kommissionsvorschlag für einen EU Kids Act die **Altersfeststellung**. Sie umfasst unterschiedliche Methoden, mit denen das Alter einer Person bestimmt, geschätzt oder überprüft werden kann. Davon zu unterscheiden ist die reine Eigenerklärung des Alters. Das Papier differenziert zwischen drei grundlegenden Methoden:

- Die **Altersüberprüfung** stützt sich auf belastbare Nachweise, etwa ein amtliches Identitätsdokument, eine bereits geprüfte Banking-Identität oder eine digitale Altersbescheinigung. Sie ermöglicht eine verlässliche Aussage, ist aber regelmäßig mit einem höheren Aufwand und teilweise mit der Verarbeitung sensibler personenbezogener Daten verbunden.
- Die **Altersschätzung** leitet das wahrscheinliche Alter oder eine Altersspanne aus verhaltensbezogenen Merkmalen oder etwa dem Gesicht ab. Sie kommt ohne Identitätsnachweis aus, liefert jedoch probabilistische Ergebnisse und erfordert insbesondere in der Nähe relevanter Altersgrenzen geeignete Sicherheitsabstände.
- Die **Altersinferenz** erschließt das Alter mittelbar aus bereits vorhandenen Informationen, etwa aus Vertrags-, Zahlungs-, Konto- oder Mobilfunkdaten. Sie kann ohne zusätzliche Handlung der Nutzerinnen und Nutzer erfolgen, ihre Belastbarkeit hängt jedoch wesentlich von der Qualität und Aussagekraft der verwendeten Informationen ab.

Von der eingesetzten Methode ist das Ergebnis zu unterscheiden, das an einen digitalen Dienst übermittelt wird. Für eine altersbezogene Entscheidung benötigt der Dienst in der Regel weder die Identität noch das genaue Geburtsdatum einer Person. Häufig genügt ein **Alterssignal**, das lediglich bestätigt, ob eine bestimmte Altersgrenze erreicht oder unterschritten wurde. Diese Trennung zwischen Methode, zugrunde liegenden Daten und übermitteltem Ergebnis ist für eine datensparsame Ausgestaltung von besonderer Bedeutung.

Die Verfahren unterscheiden sich hinsichtlich ihrer Aussagesicherheit, ihres technischen und organisatorischen Aufwands, ihrer Zugänglichkeit und ihrer Auswirkungen auf den Datenschutz. Keine einzelne Methode erfüllt sämtliche Anforderungen gleichermaßen und schließt Umgehungen vollständig aus. Dokumentenbasierte Verfahren können eine hohe Belastbarkeit erreichen, setzen aber geeignete Identitätsnachweise voraus. Schätzverfahren sind niedrigschwelliger, weisen jedoch methodenbedingte Fehlertoleranzen auf. Inferenzverfahren können vorhandene Daten nutzen, verlieren aber beispielsweise bei gemeinsam genutzten Konten, Familientarifen oder fremden Zahlungsmitteln an Aussagekraft. Entscheidend ist daher nicht allein die Wahl einer bestimmten Technologie, sondern ihre Eignung für den jeweiligen Zweck und ihre Einbettung in ein Gesamtsystem. Auch gestufte oder kombinierte Verfahren können sinnvoll sein, um die Schwächen einzelner Methoden auszugleichen und strengere Prüfungen auf unklare oder besonders risikobehaftete Fälle zu begrenzen.

Der Kommissionsvorschlag für einen EU Kids Act knüpft die Zulässigkeit verschiedener Altersfeststellungslösungen an ihren jeweiligen Verwendungszweck. Die regulatorische

Eignung einer Methode kann deshalb nicht abstrakt beurteilt werden, sondern nur im Verhältnis zum konkreten Anwendungsfall und zum jeweils erforderlichen Sicherheitsniveau.

Eine zentrale Herausforderung besteht darin, Altersfeststellung und Identifizierung voneinander zu trennen. Verfahren sollen eine altersbezogene Aussage ermöglichen, ohne zugleich die Identität der Nutzerinnen und Nutzer offenzulegen, ihr Verhalten nachzuverfolgen oder Daten über verschiedene Dienste hinweg zu verknüpfen. Aus den Vorgaben des EU Kids Act lassen sich dafür drei wesentliche Gestaltungsprinzipien ableiten: die Übermittlung ausschließlich des benötigten Altersattributs, die technische und organisatorische Trennung zwischen prüfender Stelle und genutztem Dienst sowie der Einsatz kryptographischer Verfahren, mit denen sich eine Altersvorgabe bestätigen lässt, ohne die zugrunde liegenden Identitätsdaten offenzulegen. Bei bescheinigungsbasierten Verfahren der Altersüberprüfung lassen sich diese Prinzipien technisch vergleichsweise klar abbilden. Bei Schätz- und Inferenzverfahren bleibt hingegen teilweise offen, wie einzelne Anforderungen, insbesondere das Prinzip des Zero-Knowledge-Proofs, konkret umgesetzt werden sollen. Hier kommen der Verarbeitung auf dem Endgerät, der unmittelbaren Löschung der Eingangsdaten und der ausschließlichen Weitergabe des Ergebnisses besondere Bedeutung zu.

Die EUDI-Wallet kann künftig einen wichtigen Baustein für die datensparsame Bereitstellung digitaler Altersnachweise bilden. Sie soll es ermöglichen, einzelne Attribute wie „über 18“ vorzulegen, ohne Identität oder Geburtsdatum offenzulegen. Offene Standards sollen gewährleisten, dass entsprechende Nachweise über Anbieter-, Plattform- und Ländergrenzen hinweg genutzt werden können. Die Wallet stellt jedoch nicht für alle Nutzerinnen und Nutzer und Anwendungsfälle unmittelbar eine verfügbare oder geeignete Lösung dar. Gerade in der Übergangsphase und für Personen ohne Wallet, geeignetes Endgerät oder verfügbaren Identitätsnachweis müssen alternative Zugangswege bestehen bleiben. Die parallele Verfügbarkeit verschiedener Verfahren ist daher sowohl für die praktische Umsetzbarkeit als auch für die digitale Inklusion relevant.

Aus den untersuchten Verfahren und Anforderungen ergibt sich ein **risikobasierter und gestufter Ansatz.** Das erforderliche Sicherheitsniveau sollte sich am konkreten Gefährdungspotenzial eines Dienstes, Inhalts oder einer Funktion orientieren. Besonders risikobehaftete Angebote können belastbarere Verfahren erfordern, während bei geringeren Risiken niedrigschwelligere Lösungen angemessen sein können. Dabei sollte Altersfeststellung möglichst dort ansetzen, wo ein spezifischer Schutzbedarf besteht, beispielsweise bei Inhalten ab 18 Jahren, Direktnachrichten mit unbekannten Personen, Live-Streaming oder In-App-Käufen. Eine einheitliche Prüftiefe für alle Dienste und Funktionen würde den unterschiedlichen Risiken und Nutzungskontexten nicht ausreichend Rechnung tragen.

Von Bedeutung ist zudem, wie groß der von einer Prüfung betroffene Kreis der Nutzerinnen und Nutzer ist. Je umfassender Altersfeststellung zur Voraussetzung für den Zugang zu digitalen Angeboten wird, desto stärker fallen die damit verbundenen Belastungen auch für Erwachsene ins Gewicht. Ein höheres Schutzniveau darf deshalb nicht automatisch mit einer umfangreicheren Erhebung personenbezogener Daten gleichgesetzt werden.

Regulatorische Vorgaben sollten auf nachvollziehbaren Qualitäts- und Wirkungsanforderungen beruhen und ausreichend technologieoffen ausgestaltet sein. Offene und interoperable Schnittstellen können verhindern, dass einzelne Anbieter, Betriebssysteme oder technische Infrastrukturen dauerhaft bevorzugt werden. Gleichzeitig sind klare und praktikable Anforderungen erforderlich, damit auch kleine und mittlere Unternehmen entsprechende Lösungen umsetzen können. Da digitale Dienste regelmäßig grenzüberschreitend angeboten werden, ist eine europäisch abgestimmte Ausgestaltung nationalen Sonderwegen vorzuziehen. Unterschiedliche nationale Anforderungen erhöhen Umsetzungskosten, schaffen Rechtsunsicherheit und führen zu einem uneinheitlichen Schutzniveau.

Altersfeststellung ist schließlich als ein Baustein eines umfassenderen Kinder- und Jugendschutzes zu verstehen. Sie kann altersbezogene Schutzmaßnahmen technisch unterstützen, ersetzt jedoch weder eine sichere und altersgerechte Gestaltung digitaler

Dienste noch Medienkompetenz, Bildungsangebote oder die Begleitung durch Erziehungsberechtigte. Ziel sollte daher eine Gesamtarchitektur sein, die Schutz, Befähigung und digitale Teilhabe miteinander verbindet. Die praktische Erfahrung der Digitalen Wirtschaft mit der Entwicklung, Implementierung und Anwendung unterschiedlicher Verfahren kann einen wichtigen Beitrag dazu leisten, den weiteren Rechtsrahmen wirksam, datenschutzfreundlich, technologieoffen und praktikabel auszugestalten.

Inhalt

1. Wofür ist dieses Dokument gedacht? 6
2. Über die Digitale Wirtschaft 6
3. Terminologie – Abgrenzung zentraler Begrifflichkeiten 6
4. Mögliche Methoden 9
5. Datenschutzaspekte 19
6. Die EUDI-Wallet 20
7. Vergleichender Blick auf andere Länder 21
8. Herausforderungen und Spannungsfelder 22
9. Fazit 23

Technisches Papier zur Altersfeststellung

1. Wofür ist dieses Dokument gedacht?

Dieses Dokument bietet einen strukturierten und faktenbasierten Überblick über die Begriffe, Methoden, technischen Funktionsweisen und Einsatzbereiche der Altersfeststellung. Es soll zu einer sachlichen Einordnung der aktuellen politischen und regulatorischen Debatte beitragen und ein gemeinsames Verständnis der verfügbaren Verfahren sowie ihrer jeweiligen Rahmenbedingungen schaffen. Dabei verfolgt das Papier ausdrücklich einen technischen Ansatz: Es bewertet weder einzelne Methoden noch leitet es regulatorische Präferenzen ab, sondern schafft eine Grundlage für eine differenzierte, technologieoffene und praxisnahe Debatte über wirksamen Kinder- und Jugendschutz, Datenschutz, technische Umsetzbarkeit und Verhältnismäßigkeit.

Gerade in einem Umfeld, in dem die Debatte häufig zwischen den Zielen eines wirksamen Kinder- und Jugendschutzes einerseits und Fragen des Datenschutzes, der technischen Umsetzbarkeit und der Verhältnismäßigkeit andererseits geführt wird, schafft das Papier Transparenz über bestehende Verfahren, regulatorische Anforderungen und aktuelle technologische Entwicklungen.

2. Über die Digitale Wirtschaft

Die Digitale Wirtschaft ist ein zentraler Treiber für Innovation, Wertschöpfung und Wettbewerbsfähigkeit in Deutschland und Europa. Zu ihr gehören nicht nur Plattformen und Technologieanbieter, sondern ein breit vernetztes Ökosystem aus Medienhäusern, digitalen Diensten, Spieleanbietern, Werbungtreibenden, Agenturen, Start-ups sowie Daten- und Infrastrukturanbietern. Digitale Angebote prägen heute nahezu alle Lebensbereiche, auch den Alltag von Kindern und Jugendlichen: vom Lernen über Kommunikation und Unterhaltung bis zur gesellschaftlichen Teilhabe.

Damit trägt die Digitale Wirtschaft eine besondere Verantwortung für den Schutz Minderjähriger. Viele Unternehmen der Branche setzen bereits heute Maßnahmen um, die altersgerechte Angebote ermöglichen, etwa sichere Voreinstellungen, Instrumente für Erziehungsberechtigte oder Verfahren zur Altersfeststellung.

Die Altersfeststellung ist dabei eine arbeitsteilige Aufgabe. Beteiligt sind nicht nur die Anbieter, deren Dienste Altersgrenzen durchsetzen müssen, sondern auch spezialisierte Anbieter von Verfahren zur Altersfeststellung, Identitäts- und Vertrauensdienste sowie Betriebssysteme und App-Stores, die Alterssignale bereitstellen oder weitergeben können. Welche Lösung im Einzelfall geeignet ist, hängt vom jeweiligen Dienst, seinen Risiken und seinen Nutzerinnen und Nutzern ab. Die Digitale Wirtschaft verfügt über umfangreiche praktische Erfahrung mit der Entwicklung, Implementierung und Anwendung von Verfahren zur Altersfeststellung. Diese Expertise kann einen wichtigen Beitrag zu einer faktenbasierten und praxisnahen Ausgestaltung der politischen und regulatorischen Debatte leisten.

3. Terminologie – Abgrenzung zentraler Begrifflichkeiten

In der fachpolitischen, wissenschaftlichen und unternehmerischen Debatte über den digitalen Kinder- und Jugendschutz werden unterschiedliche Begriffe für Verfahren verwendet, mit denen das Alter von Nutzerinnen und Nutzern bestimmt, geschätzt oder überprüft wird.

Begriffe wie Altersverifikation, Altersprüfung, Altersnachweis und Altersfeststellung werden häufig synonym gebraucht, obwohl sie Verschiedenes bezeichnen. Diese begriffliche Unschärfe erschwert sowohl den Vergleich technischer Lösungen als auch ihre rechtliche und politische Einordnung.

Das Papier legt deshalb eine einheitliche Begriffssystematik zugrunde. Ausgangspunkt ist die Terminologie des Kommissionsvorschlags für einen EU Kids Act (COM(2026) 681 final). Der Entwurf verwendet in seiner deutschen Fassung „Altersfeststellung" als übergeordneten Begriff. Definiert wird er als „eine Reihe von Methoden, die zur Bestimmung, Schätzung oder Überprüfung des Alters einer natürlichen Person verwendet werden können, einschließlich Altersschätzung und Altersüberprüfung und unter Ausschluss der Eigenerklärung der Nutzer" (Art. 3 Abs. 5 lit. i). Die reine Eigenerklärung der Nutzerinnen und Nutzer wird hiervon abgegrenzt. Damit bildet der Vorschlag einen zentralen europäischen Referenzpunkt für die in diesem Papier verwendete Terminologie. Ergänzend berücksichtigt das Papier ein 2024 gemeinsam von BMFSFJ, BfDI, BzKJ, Bundesnetzagentur und der Landesanstalt für Medien NRW erarbeitetes Punktepapier. Dort wird „Altersprüfung" als Überbegriff für Methoden verwendet, mit denen das Alter oder eine Altersspanne einer Person bestimmt wird. Innerhalb dieses Oberbegriffs unterscheidet das Papier insbesondere zwischen Altersverifikation und Altersschätzung bzw. Altersplausibilitätsprüfung; die reine Selbstangabe des Alters wird ebenfalls abgegrenzt. Die deutsche und die europäische Begriffsverwendung sind damit nicht vollständig deckungsgleich, folgen aber einer vergleichbaren funktionalen Systematik: Ein technologieoffener Oberbegriff umfasst unterschiedliche Verfahren, die sich nach der Art und Grundlage der Altersbestimmung unterscheiden. Dieses Papier verwendet in Anlehnung an den aktuellen Kommissionsvorschlag „Altersfeststellung" als Oberbegriff. „Altersprüfung" stellt eine ebenfalls gebräuchliche deutsche Bezeichnung dar. Ergänzend werden technische und internationale Referenzrahmen, insbesondere ISO/IEC 27566-1, herangezogen, soweit diese für die nähere technische Differenzierung der Verfahren relevant sind. Internationale Begriffsverwendungen, etwa durch britische Aufsichtsbehörden, können ergänzend berücksichtigt werden, sind für die in diesem Papier zugrunde gelegte Begriffssystematik jedoch nicht maßgeblich.

Innerhalb dieses Oberbegriffs unterscheidet dieses Papier drei grundlegende Methoden: Altersüberprüfung, Altersschätzung und Altersinferenz. Die Abgrenzung richtet sich danach, auf welcher Informationsgrundlage eine Altersaussage getroffen wird und welchen Grad an Sicherheit sie erreichen kann.

1. **Die Altersüberprüfung (Age Verification)** stellt anhand von Identifizierungsdokumenten oder anderen hinreichend belastbaren Quellen mit hoher Sicherheit fest, ob eine Person ein bestimmtes Alter erreicht hat (Art. 3 Abs. 5 lit. h). Gegenstand der Überprüfung muss dabei nicht zwingend das genaue Geburtsdatum sein. Häufig genügt die Aussage, dass eine bestimmte Altersgrenze, beispielsweise 16 oder 18 Jahre, erreicht oder nicht erreicht wurde.
   Die Altersüberprüfung ist damit ein nachweisbasiertes Verfahren. Ihre Aussage beruht auf einer Quelle, die bereits eine verlässliche Information über das Alter enthält oder aus der sich die Erfüllung einer Altersvorgabe belastbar ableiten lässt. Je nach Verfahren kann dies beispielsweise ein amtliches Identitätsdokument, ein digitaler Identitätsnachweis oder eine von einer vertrauenswürdigen Stelle ausgestellte Bescheinigung über das Erreichen einer Altersgrenze sein.
   Die Begriffe Altersverifikation, Altersüberprüfung und Altersnachweis werden zum Teil synonym gebraucht. Dieses Papier verwendet grundsätzlich den Begriff Altersüberprüfung für die Methode. Ein Altersnachweis bezeichnet demgegenüber eher den Beleg oder das Ergebnis, das bei einer solchen Überprüfung verwendet oder erzeugt wird.

2. **Die Altersschätzung (Age Estimation)** bezeichnet Verfahren, die das Alter oder eine Altersspanne anhand bestimmter Merkmale mit einer gewissen Wahrscheinlichkeit bestimmen. Anders als bei der Altersüberprüfung beruht die Altersaussage nicht auf einem bereits vorhandenen Altersnachweis. Als Grundlage können beispielsweise das Gesicht oder verhaltensbezogene Merkmale dienen. Ein bekanntes Anwendungsbeispiel ist die algorithmische Auswertung eines Gesichtsbildes zur Schätzung des ungefähren Alters. Das Ergebnis ist ~~regelmäßig~~ keine abschließende Feststellung des genauen Alters, sondern eine Wahrscheinlichkeitsaussage oder die Zuordnung zu einer Altersspanne. Altersschätzungsverfahren müssen deshalb insbesondere im Bereich relevanter Altersgrenzen sorgfältig ausgestaltet werden. Je näher das geschätzte Alter an einer

rechtlich oder technisch festgelegten Schwelle liegt, desto größer kann das Risiko einer fehlerhaften Zuordnung sein. Ein System kann deshalb unter anderem mit Sicherheitsabständen arbeiten oder bei uneindeutigen Ergebnissen eine zusätzliche Methode der Altersfeststellung vorsehen. Ofcom unterscheidet ausdrücklich zwischen Altersüberprüfung und Altersschätzung und lässt grundsätzlich auch eine Kombination beider Methoden zu.

3. Als dritte Methode führt ISO/IEC 27566-1 die **Altersinferenz (Age Inference) ein:** Dies umfasst Verfahren, bei denen das Alter oder das Erreichen einer Altersgrenze aus bereits vorhandenen, verlässlichen Informationen erschlossen wird. Grundlage können beispielsweise bestehende Konto-, Vertrags- oder andere Nutzungsdaten sein, sofern diese einen hinreichend belastbaren Rückschluss auf das Alter zulassen. Die Altersaussage beruht damit weder auf einem eigens für diesen Zweck vorgelegten Nachweis noch auf der unmittelbaren Auswertung des Gesichts. Vielmehr wird sie mittelbar aus Informationen abgeleitet, die bereits in einem anderen Zusammenhang vorliegen. ISO/IEC 27566-1 führt die Altersinferenz als eigenständige Methode innerhalb des übergeordneten Konzepts der Altersfeststellung. Der Entwurf des EU Kids Act verwendet den Begriff Altersinferenz demgegenüber nicht ausdrücklich. Das Papier übernimmt ihn dennoch, da er eine in der Praxis relevante Verfahrenskategorie beschreibt und eine klarere Abgrenzung gegenüber Altersüberprüfung und Altersschätzung ermöglicht. Die Belastbarkeit einer Altersinferenz hängt entscheidend von der Qualität und Aussagekraft der verwendeten Ausgangsinformationen ab.

Von den Methoden zu unterscheiden ist das Ergebnis, das an einen Dienst übermittelt wird. Der Entwurf bezeichnet es allgemein als Alterssignal (Age Signal). Es bezieht sich in der Regel nicht auf das genaue Alter, sondern darauf, ob eine bestimmte Altersvorgabe (Age Threshold) erreicht ist (Art. 3 Abs. 5 lit. j). Ein solches Signal kann entsprechend sowohl das Erreichen als auch das Unterschreiten einer relevanten Altersgrenze abbilden.

Die Trennung zwischen Methode und Ergebnis ist insbesondere aus Datenschutzsicht relevant. Ein Dienst benötigt für eine altersbezogene Zugangsentscheidung nicht die vollständige Identität oder das genaue Geburtsdatum einer Person. Häufig genügt die Information, dass die für den jeweiligen Dienst oder Inhalt maßgebliche Altersgrenze erreicht oder nicht erreicht wurde. Neben den Methoden unterscheidet der Entwurf Lösungen nach ihrem regulatorischen Status. EU-Altersüberprüfungslösungen sind nach einem EU-weiten Verfahren zertifiziert und gelistet (Art. 3 Abs. 5 lit. k). Die EUDI-Wallet ist eine mögliche Form einer solchen Lösung. Für bestimmte Zwecke lässt der Entwurf auch andere Lösungen zu, sofern sie seine Anforderungen erfüllen (Art. 29 Abs. 4). Das Papier bezeichnet sie in Anlehnung an Erwägungsgrund 57 als alternative Lösungen zur Altersfeststellung.

Die in diesem Papier gewählte Systematik stellt eine begriffliche Ordnung für die weitere Untersuchung dar. Sie bedeutet nicht, dass sämtliche Unternehmen, Aufsichtsbehörden, Gesetzgeber und wissenschaftlichen Einrichtungen dieselben Begriffe in gleicher Weise verwenden.

Im deutschen Jugendmedienschutz hat sich beispielsweise der Begriff Altersverifikationssystem (AVS) etabliert. Er wird insbesondere im Zusammenhang mit geschlossenen Benutzergruppen nach dem Jugendmedienschutz-Staatsvertrag verwendet. Die Kommission für Jugendmedienschutz (KJM) versteht darunter Systeme, die eine zumindest einmalige Identifizierung zur Volljährigkeitsprüfung mit einer Authentifizierung beim einzelnen Nutzungsvorgang verbinden. Der Begriff AVS bezeichnet in diesem regulatorischen Zusammenhang somit eine besonders spezifische und strenge Form der Alterskontrolle. Er ist enger gefasst als der in diesem Papier verwendete Oberbegriff Altersfeststellung.

Auch international unterscheiden sich die Begriffsverständnisse. Während ISO/IEC 27566-1 Altersüberprüfung, Altersschätzung und Altersinferenz unter dem Oberbegriff Age Assurance systematisiert, beschränkt Ofcom den Begriff in seiner regulatorischen Anwendung im

Wesentlichen auf Altersüberprüfung und Altersschätzung. Das ICO verwendet wiederum ein breiteres Verständnis, das neben dokumentenbasierten und biometrischen Verfahren auch Eigenerklärungen, technische Gestaltungsmaßnahmen und tokenisierte Altersprüfungen durch Dritte erfasst.

In der Unternehmenspraxis richtet sich die Bezeichnung eines Verfahrens häufig stärker nach seiner konkreten Funktion, technischen Umsetzung oder Nutzeroberfläche als nach einer einheitlichen regulatorischen Systematik. Unterschiedliche Unternehmen können daher vergleichbare Verfahren verschieden bezeichnen oder denselben Begriff für technisch unterschiedliche Lösungen verwenden. Zudem können mehrere Methoden miteinander kombiniert werden, beispielsweise indem zunächst vorhandene Informationen für eine Altersinferenz genutzt werden und nur in Zweifelsfällen eine Altersschätzung oder Altersüberprüfung erfolgt.

Das Zusammenspiel solcher Verfahren lässt sich mit dem aus der Sicherheitsforschung bekannten Schweizer-Käse-Modell veranschaulichen. Jede Methode gleicht dabei einer Käsescheibe: Sie fängt einen Großteil der Fälle ab, weist aber auch Löcher auf. Bei der Altersinferenz entstehen sie etwa durch gemeinsam genutzte Konten, bei der Altersschätzung durch Unschärfen in der Nähe der Altersgrenze und bei der Altersüberprüfung durch fehlende Dokumente oder die Weitergabe von Zugangsdaten. Keine einzelne Scheibe ist lückenlos. Werden mehrere Scheiben hintereinandergelegt, liegen die Löcher jedoch an unterschiedlichen Stellen, sodass sich die Schwächen eines Verfahrens durch die Stärken eines anderen ausgleichen lassen.

Die Wirksamkeit der Altersfeststellung ergibt sich deshalb weniger aus der Perfektion einer einzelnen Methode als aus ihrer sinnvollen Kombination. Auch Ofcom kommt zu dem Ergebnis, dass keine einzelne Methode Umgehungen vollständig ausschließt, und spricht sich für gestaffelte Schutzebenen aus.

Welche Lösung eingesetzt wird, hängt unter anderem vom Geschäftsmodell, vom Risikoprofil des Dienstes, von der betroffenen Nutzendengruppe, von der maßgeblichen Altersgrenze und vom erforderlichen Sicherheitsniveau ab. Die Bezeichnung eines Verfahrens allein lässt deshalb noch keine abschließende Aussage über seine technische Funktionsweise, seine Belastbarkeit oder seine regulatorische Eignung zu.

Auch in der wissenschaftlichen und normativen Debatte stehen zunehmend nicht nur einzelne technische Methoden im Mittelpunkt. Untersucht werden vielmehr vollständige Systeme der Altersfeststellung und deren Eigenschaften, darunter Genauigkeit, Datenschutz, Sicherheit, Zugänglichkeit und Akzeptanz. ISO/IEC 27566-1 folgt ebenfalls einem solchen systemischen Ansatz und beschreibt einen gemeinsamen Rahmen für altersbezogene Zugangsentscheidungen, ohne eine einzelne technische Methode vorzuschreiben.

4. Mögliche Methoden

Verfahren der Altersfeststellung werden nicht nur zur Umsetzung des EU Kids Act eingesetzt. In Deutschland verlangt bereits der Jugendmedienschutz-Staatsvertrag für bestimmte Inhalte eine geschlossene Benutzergruppe für Erwachsene (§ 4 Abs. 2 Satz 2 JMStV). Altersgrenzen gelten außerdem etwa für Glücksspiel oder den Versand altersbeschränkter Waren. Auf europäischer Ebene verpflichtet Art. 28 des Digital Services Act (DSA) Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, zu geeigneten und verhältnismäßigen Schutzmaßnahmen. Ein Alterssignal kann dabei in beide Richtungen wirken: Es kann bestätigen, dass eine Altersgrenze erreicht ist, aber ebenso zeigen, dass eine Person unterhalb dieser Grenze liegt und deshalb bestimmte Schutzmaßnahmen greifen müssen, etwa das Verbot profilierungsbasierter Werbung gegenüber Minderjährigen nach Art. 28 Abs. 2 DSA.

Die folgenden Ausführungen konzentrieren sich auch deshalb maßgeblich auf den Kommissionsvorschlag für einen EU Kids Act, weil dieser die Anforderungen an Altersfeststellung unionsweit systematisch regeln würde. Die beschriebenen Methoden sind

jedoch auch für die übrigen Zwecke relevant.

Der Entwurf des EU Kids Act schreibt kein bestimmtes technisches Verfahren vor. Ob eine Methode zulässig ist, hängt vielmehr vom Zweck der jeweiligen Pflicht ab und davon, ob sie bestimmte materielle Anforderungen erfüllt. Daraus ergeben sich zwei Wege.

1. Für die in Art. 6 geregelte Beschränkung der eigenständigen Einrichtung und Nutzung von Konten durch Minderjährige unter 15 Jahren auf den dort erfassten Online-Diensten sozialer Netzwerke und Video-Sharing-Plattform-Diensten ist ausschließlich eine zertifizierte EU-Altersüberprüfungslösung zu verwenden. Die Beschränkung greift nur, wenn der betreffende Dienst ein Risiko für die Privatsphäre, die Sicherheit oder den Schutz Minderjähriger unter 15 Jahren darstellt. Die Lösung muss eine EU-Altersnachweisbescheinigung verwenden, die von einem Dritten bereitgestellt wird, dessen Konformität mit der EU-Altersüberprüfungsregelung zertifiziert ist und der in den maßgeblichen EU-Listen geführt wird oder anhand dieser überprüft werden kann (Art. 29 Abs. 2). Art. 6 Abs. 2 lässt unter den dort genannten Voraussetzungen begrenzte, von Erziehungsberechtigten eingerichtete Konten für Minderjährige über 13 und unter 15 Jahren zu.

2. Für die Pflicht zur sicheren Gestaltung nach Art. 8 Abs. 1 sowie für die Pflichten der Anbieter von Geschäften für Software-Anwendungen (App-Stores) nach Art. 16 Abs. 2 und 3 können dagegen auch andere Lösungen zur Altersfeststellung als die in Art. 29 Abs. 2 genannte EU-Altersüberprüfungslösung eingesetzt werden. Voraussetzung ist, dass der Anbieter nachweist, dass diese Lösungen die Anforderungen der Art. 27 und 28 erfüllen (Art. 29 Abs. 4).

Für bestehende Konten sieht Art. 32 abgestufte Ausnahmen vor. Bei Konten, die möglicherweise einer Person unter 15 Jahren gehören, kann eine erneute Altersüberprüfung entfallen, wenn der Anbieter mit hoher Sicherheit feststellen kann, dass der Nutzer das Mindestalter nach Art. 6 erreicht hat (Art. 32 Abs. 1 und 2; Erwägungsgrund 61). Anbieter im Anwendungsbereich von Art. 8 Abs. 1 und Anbieter von Geschäften für Software-Anwendungen müssen das Alter nicht ermitteln, wenn sie mit hoher Sicherheit feststellen können, dass der Nutzer nicht minderjährig ist (Art. 32 Abs. 3). Die in diesem Kapitel dargestellten Methoden sind daher nicht pauschal zulässig oder unzulässig; ihre Eignung ergibt sich jeweils aus dem Verwendungszweck und den einschlägigen Voraussetzungen.

Unabhängig vom gewählten Weg gelten für die Verfahren gemeinsame grundlegende Anforderungen. Sie bilden das Raster, entlang dessen die Methoden im Folgenden beschrieben werden. Art. 27 verlangt ein hohes Maß an Genauigkeit, Zuverlässigkeit, Sicherheit, Robustheit, Nicht-Intrusivität, Schutz der Privatsphäre und Datenschutz sowie Nichtdiskriminierung. Erwägungsgrund 50 konkretisiert diese Kriterien: Genauigkeit ist unter realen Bedingungen anhand öffentlich zugänglicher Parameter zu bewerten, Robustheit bezeichnet die Widerstandsfähigkeit gegen Umgehung, und Nicht-Intrusivität bedeutet, dass weder Identität noch genaues Alter offengelegt werden, wenn die Erfüllung einer Altersvorgabe genügt. Art. 28 enthält ergänzende Datenschutzvorgaben. Altersfeststellungslösungen dürfen weder die Identifizierung noch das Lokalisieren, Tracking, die gezielte Ansprache, Werbung oder Profiling ermöglichen (Abs. 1). Anbieter und für sie tätige Stellen dürfen nicht mehr personenbezogene Daten erheben oder verarbeiten, als für die Prüfung der Altersvorgabe unbedingt erforderlich ist; eine Weiterverarbeitung, Weitergabe oder Verknüpfung mit zusätzlichen Daten sowie eine Verknüpfung mit Daten aus anderen Diensten ist grundsätzlich ausgeschlossen (Abs. 2). Art. 28 Abs. 3 verlangt den Einsatz von Verfahren nach dem Stand der Technik und sieht vor, dass jede Maßnahme der Altersfeststellung als Zero-Knowledge-Proof ausgestaltet sein muss. Die Speicherung eines Alterssignals auf Kontoebene ist nur den in Art. 28 Abs. 4 ausdrücklich genannten Anbietern nach Art. 8 Abs. 1 und Art. 16 Abs. 4 und nur zur Vermeidung wiederholter Altersfeststellungen gestattet; gespeichert werden darf nur das hierfür notwendige Minimum. Hinzu kommt ein kostenloser elektronischer Beschwerdemechanismus gegen fehlerhafte Ergebnisse (Art. 29 Abs. 5).

Die nachfolgende Übersicht dient der strukturierten Beschreibung der Methoden nach einer einheitlichen Systematik.

4.1 Altersüberprüfung

Unter Altersüberprüfung werden Verfahren verstanden, die das Alter einer Person anhand eines verlässlichen, überprüfbaren Nachweises oder einer maßgeblichen Datenquelle bestätigen. Grundlage können amtliche Dokumente wie Personalausweis, Reisepass oder Führerschein oder andere zuverlässige Quellen mit bereits geprüften Altersdaten sein. Ein Identitätsabgleich kann ergänzend erforderlich sein, etwa um das Lichtbild eines Dokuments mit der vorlegenden Person abzugleichen. Anders als bei der Altersschätzung beruht die Altersaussage auf einer bereits vorliegenden Information und nicht auf einer statistischen Schätzung; die Belastbarkeit hängt jedoch von der Zuverlässigkeit der Quelle und der korrekten Zuordnung zur betroffenen Person ab.

Diese Verfahren können ein hohes Maß an Aussagesicherheit erreichen und kommen daher vor allem dort zum Einsatz, wo für eine altersbezogene Entscheidung ein besonders belastbares Sicherheitsniveau erforderlich ist. Zugleich sind sie mit praktischen und datenschutzrechtlichen Herausforderungen verbunden. Für Nutzerinnen und Nutzer bedeuten sie einen höheren Aufwand. Zudem werden personenbezogene Daten aus Identitätsdokumenten verarbeitet, sofern nicht nur ein Altersattribut übermittelt wird. Für Anbieter entstehen technische und rechtliche Anforderungen, die sich verschärfen, wenn Nutzerinnen und Nutzer aus verschiedenen Staaten mit unterschiedlichen Dokumenten und Rechtsrahmen stammen.

In der Praxis werden insbesondere folgende Verfahren eingesetzt:

Elektronisches Auslesen hoheitlicher Dokumente

Merkmal	Beschreibung
Ausgewertetes Merkmal	Im Chip gespeicherte Daten von Personalausweis, Reisepass oder Aufenthaltstitel.
Funktionsweise	Auslesen der Chipdaten, etwa über die Online-Ausweisfunktion, und kryptographische Prüfung der Echtheit.
Art der Aussage	Deterministisch.
Einordnung EU Kids Act	Für Art. 6 nur als Bestandteil einer zertifizierten EU-Altersüberprüfungslösung; alternative Lösungen nur für Art. 8 Abs. 1 und Art. 16 Abs. 2 und 3 (Art. 29 Abs. 2 und 4).
Besonderheiten	Hohe Fälschungssicherheit, setzt ein eID-fähiges Dokument voraus, das insb. jüngere Minderjährige häufig nicht besitzen.
Datenschutz und Datensicherheit	Kann als eingriffsintensiv wahrgenommen werden; erfordert hohe Anforderungen an Datensicherheit und Nicht-Nachverfolgbarkeit.

Optische Dokumentenprüfung mit biometrischem Abgleich

Merkmal	Beschreibung

Ausgewertetes Merkmal	Ausweisdokument und Live-Bild der Person
Funktionsweise	Erfassung des Dokuments und Prüfung seiner Echtheitsmerkmale; Abgleich des Lichtbilds mit einem Live-Bild, einschließlich Lebenderkennung.
Art der Aussage	Deterministisch.
Einordnung EU Kids Act	Für Art. 6 nur als Bestandteil einer zertifizierten EU-Altersüberprüfungslösung; alternative Lösungen nur für Art. 8 Abs. 1 und Art. 16 Abs. 2 und 3 (Art. 29 Abs. 2 und 4).
Besonderheiten	Ohne Chip-Lesegerät nutzbar. Die Robustheit gegen gefälschte oder fremde Dokumente hängt von Dokumentenprüfung, Echtheitsmerkmalen und Lebenderkennung ab. Erfordert ein geeignetes Identitätsdokument; die Verfügbarkeit und Akzeptanz solcher Dokumente kann insbesondere bei Minderjährigen begrenzt sein.
Datenschutz und Datensicherheit	Es können vollständige Ausweisdaten und Bilddaten verarbeitet werden. Entscheidend sind Datenminimierung, unmittelbare Löschung nach der Prüfung und die Weitergabe nur des erforderlichen Ergebnisses an den Dienst. Eine zentrale Speicherung kann zusätzliche Sicherheitsrisiken begründen.

Video- oder Präsenzidentifizierung

Merkmal	Beschreibung
Ausgewertetes Merkmal	Ausweisdokument.
Funktionsweise	Prüfung des Dokuments durch eine geschulte Person per Videoverbindung oder vor Ort, etwa in einer Postfiliale.
Art der Aussage	Deterministisch.
Einordnung EU Kids Act	Wie beim elektronischen Auslesen; die persönliche Prüfung wird als möglicher Weg zur Ausstellung von Altersnachweisbescheinigungen genannt (Erwägungsgrund 60).
Besonderheiten	Höherer organisatorischer und zeitlicher Aufwand; vor allem für eine einmalige Ersterhebung geeignet. Erfordert ein geeignetes Identitätsdokument; ein fehlender Personalausweis ist dabei nicht mit dem Fehlen jeder anderen Nachweismöglichkeit gleichzusetzen.

Datenschutz und Datensicherheit	Ausweisdaten werden durch Dritte eingesehen; bei Videoverfahren fallen Aufzeichnungen an, deren Speicherung zu begrenzen ist. Werden Prüfung und Dienst getrennt, erfährt der Dienst nur das Ergebnis.

Bestätigung durch Stellen mit geprüften Identitätsdaten

Merkmal	Beschreibung
Ausgewertetes Merkmal	Kundinnen- und Kundendaten von Kreditinstituten oder anderen Stellen mit gesetzlicher Identifizierungspflicht
Funktionsweise	Bestätigung auf Anfrage, dass eine Altersgrenze erreicht ist, etwa über eine Banking-App oder Open Banking
Art der Aussage	deterministisch, soweit die Quelle eine geprüfte Identität voraussetzt
Einordnung EU Kids Act	Für Art. 6 nur, wenn der betreffende Dritte als konformer Anbieter einer EU-Altersnachweisbescheinigung zertifiziert und in den EU-Listen geführt wird; alternative Lösungen nur für Art. 8 Abs. 1 und Art. 16 Abs. 2 und 3 (Art. 29 Abs. 2 und 4).
Besonderheiten	Rückgriff auf bereits geprüfte Identitäten; setzt eine Kundinnen- und Kundenbeziehung voraus
Datenschutz und Datensicherheit	Die Altersaussage ist strikt von Finanzdaten zu trennen. Die bestätigende Stelle sollte nicht erfahren, für welchen Dienst die Prüfung erfolgt.

Vorlage eines digitalen Altersnachweises

Merkmal	Beschreibung
Ausgewertetes Merkmal	Zuvor ausgestellte Altersnachweisbescheinigung, z. B. in der EU-App zur Altersüberprüfung oder der EUDI-Wallet („d-you“).
Funktionsweise	Der Nachweis ist auf dem Endgerät hinterlegt und wird bei Bedarf vorgelegt; übermittelt wird nur, ob die Altersvorgabe erreicht ist.
Art der Aussage	Deterministisch; Wiederverwendung des Ergebnisses einer vorherigen Ersterhebung.
Einordnung EU Kids Act	Als zertifizierte EU-Altersüberprüfungslösung auch für Art. 6 nutzbar (Art. 29 Abs. 3).
Besonderheiten	Keine erneute Prüfung nötig; setzt ein geeignetes Endgerät und eine vorherige Ersterhebung voraus; ihre Verfügbarkeit hängt stark von der Ausgabe und den Zugangsvoraussetzungen der jeweiligen

	nationalen Wallet ab.
Datenschutz und Datensicherheit	Bei entsprechendem Protokoll- und Datenschutzdesign kann die Vorlage so erfolgen, dass der Dienst weder Identität noch Geburtsdatum erhält und einzelne Nutzungen nicht verknüpft werden können. Ob der Aussteller den Nutzungskontext erfährt, hängt ebenfalls von der konkreten technischen Umsetzung ab.

4.2 Altersschätzung

Unter Altersschätzung werden Verfahren verstanden, die das Alter einer Person aus ihrem Gesicht oder verhaltensbezogenen Merkmalen ableiten, ohne auf einen Identitätsnachweis zurückzugreifen. Am weitesten verbreitet ist die Auswertung eines Live-Bildes des Gesichts mithilfe trainierter KI-Modelle. Daneben werden etwa Stimme, Handgeometrie oder Interaktionsmuster herangezogen. Anders als bei der Altersüberprüfung beruht die Altersaussage nicht auf einem bereits vorliegenden Altersnachweis, sondern auf einer Wahrscheinlichkeit mit einer gewissen Fehlertoleranz. Der Entwurf des EU Kids Act nennt die Altersschätzung als Methode der Altersfeststellung, definiert sie jedoch nicht näher (Erwägungsgrund 53).

Diese Verfahren kommen ohne Ausweisdokumente aus und sind für Nutzerinnen und Nutzer meist mit geringerem Aufwand verbunden. Sie stehen daher auch Personen offen, die über kein geeignetes Dokument verfügen, und werden vor allem dort eingesetzt, wo eine niedrigschwellige Prüfung ausreicht oder ein strengeres Verfahren nur bei unklarem Ergebnis folgen soll. Zugleich bringt die probabilistische Aussage besondere Anforderungen mit sich. In der Nähe einer Altersgrenze ist das Ergebnis weniger eindeutig, weshalb in der Praxis mit Sicherheitspuffern oder ergänzenden Prüfungen gearbeitet wird. Die KJM hat bei einzelnen geprüften Systemen feste Sicherheitspuffer vorgesehen: Bei der „SafePassage Module-Only Solution“ war für den Zugang zu Inhalten ab 18 Jahren ein fester Puffer von fünf Jahren, also ein Schätzwert von mindestens 23 Jahren, vorgeschrieben. Andere von der KJM geprüfte Konzepte sehen abweichende Schwellenwerte und Ausweichprüfungen vor. Hinzu kommt die Frage, ob die Schätzgenauigkeit zwischen verschiedenen Gruppen von Nutzerinnen und Nutzern variiert, was im Hinblick auf das Kriterium der Nichtdiskriminierung (Art. 27) relevant ist. Die Verfahren verarbeiten personenbezogene Daten und können – je nach konkreter technischer Ausgestaltung und Verarbeitungszweck – auch biometrische Daten im Sinne von Art. 4 Nr. 14 DSGVO betreffen. Den Eingangsdaten kommt deshalb besondere Bedeutung für Datenminimierung und zeitnahe Löschung zu. Für die Zugangsbeschränkung nach Art. 6 ist die Altersschätzung nach dem Entwurf nicht als Ersatz für die dort vorgeschriebene zertifizierte EU-Altersüberprüfungslösung zulässig. Für die Pflichten nach Art. 8 Abs. 1 und Art. 16 Abs. 2 und 3 kann sie als alternative Lösung eingesetzt werden, sofern die Anforderungen der Art. 27 und 28 erfüllt sind (Art. 29 Abs. 4).

In der Praxis werden insbesondere folgende Verfahren eingesetzt:

Gesichtsbasierte Altersschätzung

Merkmal	Beschreibung
Ausgewertetes Merkmal	Gesichtsmerkmale.
Funktionsweise	Ein trainiertes Modell schätzt das Alter anhand eines Live-Bildes.

Art der Aussage	Probabilistisch, Ausgleich der Fehlertoleranz über Sicherheitspuffer.
Einordnung EU Kids Act	Nicht als Ersatz für die EU-Altersüberprüfungslösung nach Art. 6; alternative Lösung für Art. 8 Abs. 1 und Art. 16 Abs. 2 und 3 nur bei Erfüllung der Art. 27 und 28 (Art. 29 Abs. 4).
Besonderheiten	Am weitesten verbreitetes Schätzverfahren; je nach Ausgestaltung kann eine Lebenderkennung erforderlich sein. Genauigkeit und mögliche Abweichungen zwischen Nutzergruppen sind zu prüfen.
Datenschutz und Datensicherheit	Es werden personenbezogene Bilddaten verarbeitet. Ob die Verarbeitung biometrische Daten im Sinne von Art. 4 Nr. 14 DSGVO betrifft, hängt von der konkreten technischen Verarbeitung und davon ab, ob sie der eindeutigen Identifizierung dient. Wesentlich sind Datenminimierung, kurze Speicherfristen bzw. unmittelbare Löschung und – soweit technisch möglich – lokale Verarbeitung. Die Anwendung von Art. 28 Abs. 3 des Entwurfs ist gesondert zu klären.

Stimmbasierte Altersschätzung

Merkmal	Beschreibung
Ausgewertetes Merkmal	Stimmmerkmale.
Funktionsweise	Ein Modell schätzt das Alter anhand einer kurzen Sprachaufnahme.
Art der Aussage	Probabilistisch.
Einordnung EU Kids Act	Nicht als Ersatz für die EU-Altersüberprüfungslösung nach Art. 6; alternative Lösung für Art. 8 Abs. 1 und Art. 16 Abs. 2 und 3 nur bei Erfüllung der Art. 27 und 28 (Art. 29 Abs. 4).
Besonderheiten	Ohne Kamera nutzbar; Genauigkeit abhängig von Aufnahmebedingungen.
Datenschutz und Datensicherheit	Sprachaufnahmen sind personenbezogene Daten und können weitere Informationen enthalten. Eine Verarbeitung über den für die Schätzung erforderlichen Umfang hinaus ist zu vermeiden; Eingangsdaten sollten nach der Prüfung zeitnah gelöscht werden. Ob biometrische Daten im Sinne der DSGVO vorliegen, hängt von der technischen Verarbeitung und vom Zweck ab.

Weitere biometrische Schätzverfahren

Merkmal	Beschreibung
Ausgewertetes Merkmal	Merkmale wie Handgeometrie.
Funktionsweise	Ein Modell schätzt das Alter anhand von Merkmalen, die sich mit dem Alter verändern.
Art der Aussage	Probabilistisch.
Einordnung EU Kids Act	Nicht als Ersatz für die EU-Altersüberprüfungslösung nach Art. 6; alternative Lösung für Art. 8 Abs. 1 und Art. 16 Abs. 2 und 3 nur bei Erfüllung der Art. 27 und 28 (Art. 29 Abs. 4).
Besonderheiten	Bislang weniger verbreitet; Anforderungen an Lebenderkennung und Genauigkeit gelten entsprechend.
Datenschutz und Datensicherheit	Die Verarbeitung von Merkmalen der Hand kann personenbezogene und – je nach technischer Verarbeitung und Identifizierungszweck – biometrische Daten betreffen. Datenminimierung, Zweckbindung und kurze Speicherfristen sind sicherzustellen.

Verhaltens-, Nutzungs- und kontobasierte Alterseinschätzung

Merkmal	Beschreibung
Ausgewertetes Merkmal	Interaktions- und Nutzungsmuster sowie im Dienst vorhandene Angaben von Nutzerinnen und Nutzern, z. B. Tipp- oder Bewegungsverhalten, konsumierte oder veröffentlichte Inhalte sowie Altersangaben im Profil.
Funktionsweise	Ein Modell schätzt aus der Art der Nutzung und/oder vorhandenen nutzerbezogenen Informationen eine wahrscheinliche Alterszuordnung oder Altersspanne.
Art der Aussage	Bei Verhaltensmerkmalen probabilistisch (Altersschätzung); bei verifizierten, altersimplizierenden Informationen mittelbar (Altersinferenz).
Einordnung EU Kids Act	Nicht als Ersatz für die EU-Altersüberprüfungslösung nach Art. 6; für Art. 8 Abs. 1 und Art. 16 Abs. 2 und 3 nur dann als alternative Lösung zu prüfen, wenn die Anforderungen der Art. 27 und 28 erfüllt sind (Art. 29 Abs. 4).
Besonderheiten	Ohne aktive Mitwirkung möglich; fließende Grenze zur Altersinferenz.
Datenschutz und Datensicherheit	Die Auswertung kann je nach konkreter Ausgestaltung mit dem Verbot der Lokalisierung, des Trackings, der gezielten Ansprache und des Profilings nach Art. 28 Abs. 1 sowie mit den

	Datenverknüpfungsbeschränkungen nach Abs. 2 in Konflikt geraten.

4.3 Altersinferenz

Unter Altersinferenz werden Verfahren verstanden, die aus dem Vorliegen oder der Gültigkeit einer bereits verfügbaren Information mittelbar auf das Erreichen oder Unterschreiten einer Altersgrenze schließen. Grundlage können etwa überprüfbare Vertrags- oder Zahlungsnachweise, verifizierte Angaben von Mobilfunkanbietern oder andere belastbare Kontextinformationen sein. Entscheidend ist, dass die verwendete Information tatsächlich einen Rückschluss auf die maßgebliche Altersgrenze zulässt und der betreffenden nutzenden Person zugeordnet werden kann. Die bloße Existenz eines Kontos oder einer E-Mail-Adresse bei einem Dienst mit Mindestalter belegt für sich genommen weder das Alter noch die Identität der aktuellen Nutzerin oder des aktuellen Nutzers.

Die internationale Norm ISO/IEC 27566-1 führt die Altersinferenz als eigenständige Methode neben Altersüberprüfung und Altersschätzung. Sie grenzt sie insbesondere von der Schätzung anhand biologischer oder verhaltensbezogener Merkmale ab: Eine Inferenz stützt sich auf das Vorliegen oder die Gültigkeit einer Information, aus der sich mittelbar ein Alter ableiten lässt. Andere Regulierungsansätze, etwa in Singapur, verwenden teilweise weiter gefasste Kategorien, die auch Kontoaktivität oder Nutzungsdaten umfassen können. Der Entwurf des EU Kids Act verwendet den Begriff Altersinferenz nicht ausdrücklich, erkennt aber bestimmte vorhandene Signale für bestehende Konten an, etwa das Datum der Kontoerstellung oder zuvor rechtmäßig erworbene Kreditkartendaten (Erwägungsgrund 61).

Diese Verfahren greifen auf vorhandene Daten zurück und erfordern von Nutzerinnen und Nutzern daher meist keine zusätzliche Handlung. Sie können insbesondere bei Bestandskonten eingesetzt werden, um mit geringem Aufwand Hinweise darauf zu gewinnen, ob das Mindestalter bereits erreicht ist. Zugleich hängt die Belastbarkeit der Aussage maßgeblich von der Qualität der zugrunde liegenden Quelle ab. Entscheidend ist etwa, ob ein Vertrag tatsächlich Volljährigkeit voraussetzt und ob Vertragsinhaberin bzw. Vertragsinhaber und tatsächliche nutzende Person identisch sind, etwa bei Familientarifen oder gemeinsam genutzten Zahlungsmitteln. Werden Rückschlüsse aus dem Nutzungsverhalten gezogen, ist zudem zu prüfen, ob es sich nach der gewählten Systematik noch um eine Altersinferenz oder bereits um eine Altersschätzung anhand verhaltensbezogener Merkmale handelt. Eine laufende Auswertung von Nutzungsdaten kann außerdem mit dem Verbot von Tracking, gezielter Ansprache und Profiling nach Art. 28 Abs. 1 sowie den Beschränkungen der Datenverknüpfung nach Abs. 2 kollidieren. Für sehr große Online-Plattformen sieht Art. 32 Abs. 4 einen Umsetzungsplan gegenüber der zuständigen Behörde vor; die Aussagekraft vorhandener Altersindikatoren ist dabei anhand geeigneter Nachweise und gegebenenfalls statistischer Leistungsdaten zu erläutern (Erwägungsgrund 62). Für Art. 6 ist die Altersinferenz kein Ersatz für die dort vorgeschriebene zertifizierte EU-Altersüberprüfungslösung. Als alternative Lösung kommt sie für Art. 8 Abs. 1 sowie Art. 16 Abs. 2 und 3 nur in Betracht, wenn die Anforderungen der Art. 27 und 28 erfüllt sind (Art. 29 Abs. 4).

In der Praxis werden insbesondere folgende Verfahren eingesetzt:

Zahlungs- und Vertragsdaten

Merkmal	Beschreibung
Ausgewertetes Merkmal	Verträge, die Volljährigkeit voraussetzen, z. B. Kreditkarten.
Funktionsweise	Aus dem Bestehen des Vertrages wird auf die Volljährigkeit der Inhaberin bzw. des Inhabers

	geschlossen.
Art der Aussage	Mittelbar, nur aussagekräftig, wenn der Vertrag tatsächlich Volljährigkeit voraussetzt (z. B. keine Debitkarte).
Einordnung EU Kids Act	Für Bestandskonten als mögliches Signal in Erwägungsgrund 61 erwähnt; als alternative Lösung für Art. 8 Abs. 1 und Art. 16 Abs. 2 und 3 nur bei Erfüllung der Anforderungen der Art. 27 und 28 (Art. 29 Abs. 4).
Besonderheiten	Eingeschränkt bei Nutzung fremder Zahlungsmittel.
Datenschutz und Datensicherheit	Es werden Zahlungsdaten verarbeitet, die besonders schutzbedürftig sind. Die Altersaussage ist von weiteren Finanzinformationen zu trennen.

Abfrage bei Mobilfunkanbietern

Merkmal	Beschreibung
Ausgewertetes Merkmal	Vertragsdaten des Mobilfunkanbieters.
Funktionsweise	Der Anbieter bestätigt, ob die Vertragsinhaberin oder der Vertragsinhaber volljährig ist oder für den Anschluss Altersbeschränkungen bestehen.
Art der Aussage	Mittelbar, abhängig davon, ob Vertragsinhaberin bzw. Vertragsinhaber und Nutzerin bzw. Nutzer identisch sind.
Einordnung EU Kids Act	Für Art. 8 Abs. 1 und Art. 16 Abs. 2 und 3 als alternative Lösung möglich, sofern die Anforderungen der Art. 27 und 28 erfüllt sind (Art. 29 Abs. 4).
Besonderheiten	Eingeschränkt bei Familien- und Prepaid-Tarifen.
Datenschutz und Datensicherheit	Die Abfrage erfolgt über die Rufnummer und kann Rückschlüsse auf die Identität ermöglichen; übermittelt werden sollte nur die Altersaussage.

Konto- und Nutzungsdaten

Merkmal	Beschreibung
Ausgewertetes Merkmal	Beim Anbieter vorhandene Kontoinformationen, z. B. Datum der Kontoerstellung.
Funktionsweise	Aus dem Alter des Kontos oder vorhandenen Kontoinformationen wird auf das Mindestalter geschlossen.
Art der Aussage	Mittelbar.

Einordnung EU Kids Act	Das Datum der Kontoerstellung wird für Bestandskonten in Erwägungsgrund 61 als mögliches Signal genannt; die Anforderungen an den Umgang mit solchen Signalen und die Umsetzungsplanung sehr großer Online-Plattformen ergeben sich insbesondere aus Art. 32 Abs. 4 und den einschlägigen Erwägungsgründen.
Besonderheiten	Ohne zusätzliche Datenerhebung; eingeschränkt bei gemeinsam genutzten Konten.
Datenschutz und Datensicherheit	Es werden nur bereits vorhandene Daten genutzt. Werden Nutzungsdaten ausgewertet, ist die Abgrenzung zum unzulässigen Profiling (Art. 28 Abs. 1) zu beachten.

E-Mail-basierte Inferenz

Merkmal	Beschreibung
Ausgewertetes Merkmal	Nutzungshistorie einer E-Mail-Adresse.
Funktionsweise	Aus der Verwendung der Adresse bei Diensten, die ein Mindestalter voraussetzen, wird auf das Alter geschlossen.
Art der Aussage	Mittelbar.
Einordnung EU Kids Act	Für Art. 8 Abs. 1 und Art. 16 Abs. 2 und 3 als alternative Lösung möglich, sofern die Anforderungen der Art. 27 und 28 erfüllt sind (Art. 29 Abs. 4).
Besonderheiten	Ohne Mitwirkung möglich; abhängig von der Qualität der zugrunde liegenden Datenquellen.
Datenschutz und Datensicherheit	Die Abfrage greift auf Daten Dritter zurück; zu beachten sind Datenminimierung und das Verknüpfungsverbot (Art. 28 Abs. 2).

5. Datenschutzaspekte

Verfahren der Altersfeststellung stehen in einem Spannungsverhältnis. Sie sollen Minderjährige schützen, können dafür aber die Verarbeitung von Daten aller Nutzerinnen und Nutzer erfordern. Zentral ist dabei die Unterscheidung zwischen Altersfeststellung und Identifizierung. Für eine altersbezogene Zugangsentscheidung muss ein Dienst in der Regel nicht wissen, wer eine Person ist, sondern nur, ob sie eine bestimmte Altersgrenze erreicht hat.

Der Kommissionsvorschlag für einen EU Kids Act greift diesen Gedanken mit Vorgaben auf, die über die allgemeinen Grundsätze der DSGVO hinausgehen. Nach Art. 28 Abs. 1 dürfen Lösungen zur Altersfeststellung weder die Identifizierung noch das Lokalisieren, Tracking, die gezielte Ansprache, Werbung oder Profiling ermöglichen. Nach Art. 28 Abs. 2 dürfen Anbieter und für sie tätige Stellen nicht mehr personenbezogene Daten erheben, speichern oder verarbeiten, als zur Prüfung der jeweiligen Altersvorgabe unbedingt erforderlich ist. Eine Weiterverarbeitung, Weitergabe oder Verknüpfung mit zusätzlichen Daten sowie eine Verknüpfung mit Daten aus anderen Diensten desselben Anbieters oder Dritter ist grundsätzlich ausgeschlossen. Die DSGVO bleibt daneben anwendbar. Für die Überwachung

der datenschutzrechtlichen Pflichten nach Art. 27, 28 und 29 sind die Datenschutzaufsichtsbehörden nach Art. 34 Abs. 6 zuständig.

Aus diesen Vorgaben lassen sich drei zentrale Architekturprinzipien ableiten:

1. Das erste Prinzip ist die Datenminimierung auf der Ergebnisebene: Dem Dienst wird im Idealfall nicht das Geburtsdatum übermittelt, sondern nur die Aussage, ob eine Altersvorgabe erreicht ist. Wie weit dieses Prinzip umgesetzt werden kann, hängt vom Verfahren ab. Bei bescheinigungsbasierten Verfahren ist es technisch angelegt. Bei anderen Verfahren fallen beim prüfenden Dienstleister zunächst weitere Daten an, etwa vollständige Ausweisdaten oder ein Gesichtsbild, die nach Abschluss der Prüfung grundsätzlich zeitnah zu löschen sind, soweit keine andere Rechtsgrundlage eine begrenzte Aufbewahrung erlaubt. Aus Sicht der Datenminimierung sollte nicht das genaue Alter dauerhaft gespeichert werden, sondern – soweit eine Speicherung rechtlich zulässig ist – nur die Information, ob die jeweilige Nutzungsvoraussetzung erfüllt ist. Dabei sind zwei Ebenen zu unterscheiden: Ein digitaler Altersnachweis wird auf dem Endgerät der Nutzerin oder des Nutzers vorgehalten, etwa in einer App oder Wallet. Eine Speicherung eines Alterssignals auf Kontoebene ist nach Art. 28 Abs. 4 des Entwurfs jedoch nur den dort bezeichneten Anbietern gestattet (Anbietern nach Art. 8 Abs. 1 und Art. 16 Abs. 4). Sie darf ausschließlich der Vermeidung wiederholter Altersfeststellungen dienen und muss auf die hierfür unbedingt notwendigen Informationen beschränkt bleiben.

2. Das zweite Prinzip ist die Trennung der Rollen. Die Stelle, die das Alter prüft, soll nicht erfahren, für welchen Dienst die Prüfung erfolgt, und der Dienst soll nicht erfahren, wer die Person ist. Frankreich hat dieses Prinzip als „double anonymat“ verbindlich vorgegeben. Die Kommission beschreibt ihre eigene Lösung als „doppelblind“, nicht rückverfolgbar und unverknüpfbar.

3. Das dritte Prinzip ist der Zero-Knowledge-Proof: Ein kryptographisches Verfahren ermöglicht es, die Gültigkeit einer Aussage nachzuweisen, ohne die zugrunde liegenden Daten offenzulegen. Die EU-Referenzlösung für den Altersnachweis nutzt entsprechende kryptographische Verfahren; technische Komponenten und Implementierungen sind teilweise quelloffen dokumentiert. Art. 28 Abs. 3 des Kommissionsvorschlags verlangt den Einsatz von Verfahren nach dem Stand der Technik und sieht vor, dass jede Maßnahme der Altersfeststellung als Zero-Knowledge-Proof ausgestaltet sein muss.

Diese Prinzipien lassen sich technisch nicht auf alle Methoden in gleicher Weise übertragen. Bei bescheinigungsbasierten Verfahren der Altersüberprüfung ist ein kryptographischer Nachweis eines bereits bestätigten Altersattributs besonders naheliegend. Altersschätzungen erzeugen ihr Ergebnis dagegen erst durch die Auswertung biologischer oder verhaltensbezogener Merkmale; ihnen liegt nicht notwendigerweise ein bereits signiertes Altersattribut zugrunde. Bei Altersinferenz hängt die Umsetzbarkeit davon ab, ob die zugrunde liegenden Informationen als verifizierte und kryptographisch prüfbare Nachweise vorliegen. Das in der Referenzlösung verwendete Modell lässt sich deshalb auf Schätz- und nicht bescheinigungsbasierte Inferenzverfahren nicht ohne Weiteres übertragen. Zero-Knowledge-Verfahren sind jedoch nicht grundsätzlich auf signierte Altersbescheinigungen beschränkt: Denkbar sind auch kryptographische Nachweise über die korrekte Durchführung einer Modellberechnung; solche Ansätze sind technisch anspruchsvoll und von der einfachen Prüfung eines signierten Attributs zu unterscheiden. Unabhängig von der konkreten Umsetzung sollten Eingangsdaten möglichst lokal verarbeitet, minimiert und zeitnah gelöscht sowie nur das erforderliche Ergebnis weitergegeben werden. Wie Art. 28 Abs. 3 auf die unterschiedlichen Verfahren anzuwenden ist, bedarf weiterer technischer Konkretisierung.

6. Die EUDI-Wallet

Die Europäische Brieftasche für die digitale Identität (EUDI-Wallet) beruht auf der überarbeiteten eIDAS-Verordnung. Die Mitgliedstaaten müssen mindestens eine EUDI-Wallet nach Maßgabe der eIDAS-Verordnung bereitstellen; die unionsrechtliche Bereitstellungsfrist läuft nach den einschlägigen Durchführungsrechtsakten bis Ende 2026. Die deutsche

staatliche Wallet „d-you“ soll Anfang Januar 2027 starten und Bürgerinnen und Bürgern sowie Einwohnerinnen und Einwohnern Deutschlands kostenlos und freiwillig zur Verfügung stehen. Mit der Wallet lassen sich Identitätsdaten und weitere Nachweise auf einem geeigneten Endgerät speichern und einzelne Attribute gezielt vorlegen, etwa nur die Aussage „über 18“. Verifizierte Altersattribute können von qualifizierten Vertrauensdiensteanbietern in Form qualifizierter elektronischer Attributsbescheinigungen bereitgestellt werden. Als zugrunde liegende Datenquellen können je nach Ausgestaltung auch Behörden oder andere Stellen mit verlässlich geprüften Informationen dienen. Offene Standards wie ISO/IEC 18013-5 (mDoc), OpenID for Verifiable Presentations (OpenID4VP) und die W3C Digital Credentials API sollen die Interoperabilität entsprechender Nachweise über Länder-, Plattform- und Anbietergrenzen hinweg unterstützen. Sie gewährleisten den Zugang über sämtliche Browser- und App-Umgebungen jedoch nicht für sich allein; maßgeblich sind auch die konkrete Implementierung und die Unterstützung durch die beteiligten Systeme. Bis Wallets flächendeckend verbreitet sind, erprobt die Kommission mit dem EU-Konzept für die Altersüberprüfung (Blueprint) eine mit der Wallet interoperable Referenzlösung, die 2026 in mehreren Mitgliedstaaten pilotiert wird. Nach dem EU Kids Act gilt eine Wallet, die die Anforderungen der EU-Altersüberprüfungsregelung erfüllt, als zertifizierte EU-Altersüberprüfungslösung (Art. 29 Abs. 3). Sie nimmt damit im Regelungsmodell des Entwurfs eine besondere Stellung ein, ist aber nicht die einzige mögliche Form der Altersfeststellung. Gerade in der Übergangsphase stehen daneben weitere Verfahren zur Verfügung, etwa Banking-Identitäten, Zahlungsdaten oder Schätzverfahren. So können auch Personen ohne Wallet ihr Alter nachweisen.

7. Vergleichender Blick auf andere Länder

Auch außerhalb der Europäischen Union wird die Regulierung der Altersfeststellung vorangetrieben. Die Begriffe stimmen dabei weitgehend mit der hier verwendeten Systematik überein. Die Regulierungsansätze unterscheiden sich jedoch darin, an welcher Stelle sie ansetzen und wie viel Spielraum sie den Anbietern bei der Wahl der Methode lassen.

Das Vereinigte Königreich verlangt nach dem Online Safety Act eine „highly effective age assurance“. Maßgeblich ist, ob ein Verfahren technisch genau, robust, zuverlässig und fair ist. Die Regulierungsbehörde Ofcom nennt dazu eine nicht abschließende Liste geeigneter Methoden: Open Banking, Ausweisabgleich, gesichtsbasierte Altersschätzung, Abfragen bei Mobilfunkanbietern, Kreditkartenprüfungen, digitale Identitätsdienste und E-Mail-basierte Altersschätzung. Eigenerklärungen gelten dagegen ausdrücklich nicht als ausreichend. Ofcom betont, dass kein einzelnes Verfahren sämtliche Umgehungsversuche ausschließt, und empfiehlt deshalb eine am Risiko orientierte Auswahl geeigneter Maßnahmen. Die britische Regierung plant zudem, den Zugang zu bestimmten sozialen Medien für Personen unter 16 Jahren nach australischem Vorbild zu beschränken. Die ersten Regelungen sollen bis Ende 2026 vorgelegt und die Maßnahmen im Frühjahr 2027 umgesetzt werden.

Australien hat Ende 2024 als erstes Land eine gesetzliche Mindestaltersgrenze von 16 Jahren für die Nutzung bestimmter sozialer Netzwerke beschlossen. Die Regelung ist am 10. Dezember 2025 in Kraft getreten. Die Anbieter müssen „angemessene Schritte“ ergreifen, um zu verhindern, dass Personen unter 16 Jahren Konten auf den erfassten Diensten führen. Die Pflicht trifft die Plattformen, nicht die Kinder oder ihre Eltern. Bei der Wahl der Methode haben die Anbieter einen erheblichen Spielraum. Die australische Datenschutzbehörde unterscheidet dabei ausdrücklich zwischen Altersüberprüfung, Altersschätzung und Altersinferenz.

Andere Staaten verlagern die Altersfeststellung stärker auf die Ebene der App-Stores und Betriebssysteme. In Singapur müssen die von der zuständigen Aufsichtsbehörde benannten App-Distributionsdienste seit dem 31. März 2026 Altersfeststellungsmaßnahmen implementieren, um Nutzerinnen und Nutzer unter 18 Jahren vom Zugriff auf Apps auszuschließen, die nicht ihrer Altersfreigabe entsprechen. Die Dienste können zwischen Altersüberprüfung, Altersschätzung und Altersinferenz oder einer Kombination dieser Verfahren wählen. In den USA wurden in mehreren Bundesstaaten Regelungen zur Alterskategorisierung auf Ebene der App-Stores beschlossen oder vorgeschlagen;

Anwendungsbeginn und gerichtlicher Status unterscheiden sich jedoch. Kalifornien baut mit dem Digital Age Assurance Act auf ein Alterssignal des Betriebssystems, das ab dem 1. Januar 2027 schrittweise bereitgestellt werden soll. Brasilien bezieht mit dem ECA Digital (Lei nº 15.211/2025), das seit dem 17. März 2026 gilt, digitale Produkte und Dienste ein, die sich an Kinder und Jugendliche richten oder von ihnen genutzt werden können. Für den Zugang zu gesetzlich verbotenen Produkten oder Diensten reicht eine bloße Eigenerklärung des Alters nicht aus.

Der Vergleich zeigt, dass ähnliche Methoden in unterschiedliche Regulierungslogiken eingebettet werden. Das Vereinigte Königreich knüpft an die Wirksamkeit der Verfahren an, Australien setzt auf einen offenen Sorgfaltsmaßstab, und andere Staaten verlagern bestimmte Pflichten auf App-Stores und Betriebssysteme. Der Entwurf des EU Kids Act unterscheidet dagegen nach dem regulatorischen Status der Lösung. In den hier betrachteten Ansätzen reicht eine bloße Eigenerklärung häufig nicht aus; Reichweite und konkrete Ausgestaltung unterscheiden sich jedoch erheblich.

8. Herausforderungen und Spannungsfelder

Die vorangegangenen Kapitel zeigen, dass Altersfeststellung kein technisches Randthema ist. Sie kann eine wichtige Voraussetzung für altersbezogene Schutzmaßnahmen im digitalen Raum sein, soweit diese an das tatsächliche Alter der nutzenden Person anknüpfen. Altersgrenzen, altersgerechte Voreinstellungen und Funktionsbeschränkungen können verlässliche Altersinformationen voraussetzen, müssen aber nicht in jedem Fall eine gesonderte Altersfeststellung erfordern. Altersfeststellung ist daher als möglicher Bestandteil digitaler Schutzinfrastrukturen zu verstehen und nicht als pauschale Zugangsvoraussetzung für sämtliche digitalen Angebote. Zu solchen Schutzinfrastrukturen können auch elternunterstützte Mechanismen gehören. Technische Lösungen sollten daher, soweit dies im jeweiligen Anwendungskontext sinnvoll und regulatorisch gefordert ist, auch die Einbindung von Erziehungsberechtigten mitdenken.

Die Altersfeststellung betrifft zudem nicht nur Kinder und Jugendliche. Um Minderjährige zuverlässig zu erkennen, müssen auch Erwachsene ihr Alter nachweisen. Die Möglichkeit, legale Informationen und Angebote auch anonym oder pseudonym zu nutzen, ist dabei ein wesentliches Merkmal eines freien Internets und eng mit der Meinungs- und Informationsfreiheit verbunden. Die Herausforderung besteht daher darin, wirksamen Jugendschutz mit Datenschutz, einem offenen Zugang zu digitalen Angeboten und den Freiheitsrechten der Nutzerinnen und Nutzer in Einklang zu bringen.

Keine Methode erfüllt alle Anforderungen gleichermaßen. Die Verfahren unterscheiden sich hinsichtlich Genauigkeit, Zuverlässigkeit, Robustheit, Datenschutz, Aufwand und Zugänglichkeit; zugleich kann keine einzelne Methode Umgehungen vollständig ausschließen. Welches Verfahren geeignet ist und welches Sicherheitsniveau erforderlich ist, sollte sich daher nach dem konkreten Gefährdungspotenzial eines Dienstes, Inhalts oder einer Funktion richten. Höhere Risiken können strengere Anforderungen rechtfertigen, während Angebote mit geringerem Gefährdungspotenzial nicht automatisch derselben Prüftiefe unterliegen sollten.

Bei dieser Abwägung ist auch zu berücksichtigen, wie viele und welche Nutzerinnen und Nutzer von einer Prüfung betroffen sind. Eine Altersfeststellung kann gezielt für den Zugang zu bestimmten Inhalten oder Funktionen eingesetzt werden. Sie kann aber auch als allgemeine Zugangsvoraussetzung ausgestaltet sein und damit große Teile der Bevölkerung erfassen, einschließlich Erwachsener ohne jugendschutzrechtlichen Schutzbedarf. Je größer der betroffene Personenkreis und je umfassender die Zugangswirkung, desto stärker sind die Anforderungen an Verhältnismäßigkeit, Datensparsamkeit, Zugänglichkeit und Nutzungsfreundlichkeit.

Ein solcher Ansatz setzt deshalb in erster Linie beim erforderlichen Ergebnis an: Für einen konkreten Anwendungsfall muss ein angemessenes Sicherheitsniveau erreicht werden. Dies ermöglicht es, unterschiedliche technische Lösungen anhand des jeweiligen Schutzbedarfs einzusetzen, ohne für sämtliche Anwendungsfälle ein einheitliches Verfahren vorauszusetzen. Altersfeststellung kann entsprechend gezielt dort greifen, wo ein spezifisches Gefährdungspotenzial besteht, etwa beim Live-Streaming, Direktnachrichten mit Unbekannten, In-App-Käufen oder dem Abruf von Inhalten ab 18 Jahren. Gestufte und kombinierte Verfahren, wie sie auch die internationale Norm ISO/IEC 27566-1 vorsieht, tragen diesem Gedanken Rechnung.

Regulatorische Vorgaben sollten deshalb technologieoffen formuliert sein und sich an überprüfbaren Qualitäts- und Wirkungsanforderungen orientieren. Eine dauerhafte Festlegung auf einzelne Verfahren kann angesichts der technischen Entwicklung schnell veralten und Innovationen begrenzen. Technologieoffenheit setzt allerdings hinreichend konkrete Maßstäbe voraus, damit Anbieter verlässlich beurteilen können, welche Lösungen die regulatorischen Anforderungen erfüllen. Ebenso wichtig ist das Vertrauen der Nutzerinnen und Nutzer. Intransparente oder als übermäßig eingriffsintensiv wahrgenommene Verfahren können Akzeptanzprobleme und Ausweichverhalten begünstigen und dadurch ihre Schutzwirkung mindern.

Die Altersfeststellung ist zudem eine Aufgabe des gesamten digitalen Ökosystems. Betriebssysteme, App-Stores, Identitätsdienste, Plattformen und staatliche Stellen tragen jeweils eigene Verantwortung. Diese Verantwortlichkeiten müssen klar verteilt sein. Betriebssysteme und App-Stores können Alterssignale bereitstellen, die Diensteanbieter kennen jedoch Risiken ihrer eigenen Angebote und Funktionen am besten. Eine einseitige Verlagerung der Verantwortung auf eine einzelne Ebene würde dem nicht gerecht. Staatliche Identitätsinfrastrukturen wie die EUDI-Wallet sind ein wichtiger Baustein, entbinden jedoch nicht von der Aufgabe, Zugänglichkeit für alle sicherzustellen, insbesondere für Kinder und Jugendliche ohne Ausweisdokumente, für Menschen ohne geeignete Endgeräte und für Menschen mit Behinderungen. Die parallele Verfügbarkeit mehrerer Verfahren ist daher auch ein Gebot digitaler Inklusion.

Da digitale Dienste grenzüberschreitend angeboten werden, ist eine europäische Harmonisierung einer Vielzahl nationaler Einzellösungen vorzuziehen. Unterschiedliche Anforderungen erhöhen die Umsetzungskosten, schaffen Rechtsunsicherheit und führen zu einem uneinheitlichen Schutzniveau. Die gegenseitige Anerkennung von Nachweisen und die Anschlussfähigkeit an internationale Standards sind dafür wesentlich. Rechtssicherheit ist zugleich eine Voraussetzung für Investitionen. Solange offen bleibt, welche Verfahren als konform gelten, wird die Umsetzung verzögert, und Anbieter mit größeren Ressourcen werden begünstigt. Die Anforderungen müssen daher auch für kleine und mittlere Unternehmen praktikabel sein.

Schließlich ist die Altersfeststellung zwar notwendig, aber nicht hinreichend. Sie ermöglicht Schutzmaßnahmen, ersetzt jedoch weder eine sichere Gestaltung der Dienste noch Medienkompetenz, die Begleitung durch Erziehungsberechtigte oder Bildungsangebote. Ihre Wirksamkeit sollte zudem regelmäßig evaluiert werden, damit regulatorische Vorgaben auf Evidenz beruhen und an technische und gesellschaftliche Entwicklungen angepasst werden können.

9. Fazit

Die Altersfeststellung ist zu einem Schlüsselelement des digitalen Kinder- und Jugendschutzes geworden. Dieses Papier zeigt, dass es dafür nicht die eine Lösung gibt, sondern ein breites Spektrum an Verfahren der Altersüberprüfung, Altersschätzung und Altersinferenz. Diese Verfahren unterscheiden sich in ihrer Aussagesicherheit, ihrem Aufwand und ihren Auswirkungen auf den Datenschutz. Ihre Wirksamkeit hängt deshalb weniger von einer einzelnen Technik ab als davon, wie sie ausgewählt, kombiniert und ausgestaltet werden.

Daraus folgt zunächst die Notwendigkeit eines risikobasierten, gestuften Ansatzes. Eine

einheitliche Lösung für alle Dienste würde weder den unterschiedlichen Risiken noch den Bedürfnissen der Nutzerinnen und Nutzer gerecht. Sinnvoll ist eine Kaskade, in der sich die Belastbarkeit der Altersaussage nach dem Risikograd eines Dienstes oder einer Funktion richtet.

Zweitens müssen Datenschutz und Datensicherheit von Beginn an in die Technologie eingebaut werden. Verfahren, die nur das erforderliche Altersattribut übermitteln, Nutzungen über verschiedene Dienste hinweg nicht verknüpfbar machen und auf Zero-Knowledge-Proofs setzen, zeigen, dass wirksamer Schutz und Privatsphäre vereinbar sind. Die Speicherung von Ausweiskopien oder anderer sensibler Daten auf zentralen Servern ist dagegen zu vermeiden, weil sie neue Sicherheitsrisiken schafft und das Vertrauen der Nutzerinnen und Nutzer untergräbt.

Drittens braucht es offene und interoperable Schnittstellen. Standards und Spezifikationen wie die W3C Digital Credentials API, ISO/IEC 18013-5 oder OpenID4VP können die Einbindung von Wallets und Nachweisen unterschiedlicher Anbieter über Betriebssystem- und Anbietergrenzen hinweg erleichtern. Sie können technische Abhängigkeiten reduzieren und Wettbewerb sowie Innovation fördern. Voraussetzung ist jedoch, dass die Standards interoperabel umgesetzt und von den beteiligten Systemen tatsächlich unterstützt werden.

Viertens ist der europäische Binnenmarkt zu schützen. Digitale Dienste werden grenzüberschreitend angeboten. Nationale Sonderwege im Jugendschutz führen zu rechtlicher Zersplitterung, höheren Kosten und einem uneinheitlichen Schutzniveau. Der Digital Services Act bildet bereits einen gemeinsamen europäischen Rahmen für den Schutz Minderjähriger auf Online-Plattformen. Dieser sollte kohärent angewendet und durch neue unionsweite Vorgaben, insbesondere zur Altersfeststellung, widerspruchsfrei ergänzt werden.

Schließlich muss eine echte Balance zwischen Schutz, Befähigung und Teilhabe gelingen. Jugendschutz darf nicht dazu führen, dass Kinder und Jugendliche von digitalen Angeboten ausgeschlossen werden, die für Bildung, Kommunikation und gesellschaftliche Teilhabe wichtig sind. Technische Altersfeststellung ist deshalb nur ein Baustein. Sie muss Hand in Hand gehen mit altersgerechter Gestaltung der Dienste, der Förderung von Medienkompetenz und der Begleitung durch Erziehungsberechtigte.

Die Digitale Wirtschaft verfügt über umfangreiche Erfahrung mit den hier beschriebenen Verfahren. Sie ist bereit, diese Expertise in die weitere Ausgestaltung des Rechtsrahmens einzubringen, damit Altersfeststellung wirksam, datenschutzfreundlich und praktikabel wird.

Bundesverband Digitale Wirtschaft (BVDW) e.V.

Der Bundesverband Digitale Wirtschaft (BVDW) e. V. ist die Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Mit seinen Mitgliedern aus der gesamten Digitalen Wirtschaft gestaltet der BVDW bereits heute die Zukunft – durch kreative Lösungen und modernste Technologien. Als Impulsgeber, Wegweiser und Beschleuniger digitaler Geschäftsmodelle setzt der Verband auf faire und klare Regeln und tritt für innovationsfreundliche Rahmenbedingungen ein. Dabei hat der BVDW immer Wirtschaft, Gesellschaft und Umwelt im Blick. Neben der DMEXCO, der führenden Fachmesse für Digitales Marketing und Technologien, und dem Deutschen Digital Award richtet der BVDW auch den CDR-Award, die erste Preisverleihung im DACH-Raum für Digitale Nachhaltigkeit und Verantwortung sowie eine Vielzahl von Fachveranstaltungen aus.

Zur Entstehung dieses Papiers

Das vorliegende Papier ist in einem gemeinsamen Arbeitsprozess mehrerer Working Groups des BVDW entstanden. Expertinnen und Experten aus Mitgliedsunternehmen haben ihre Perspektiven eingebracht. Damit bündelt das Papier die Sicht derjenigen, die Altersgrenzen in ihren Diensten umsetzen.

Grundlage der Arbeit waren die praktischen Erfahrungen der beteiligten Unternehmen mit der Entwicklung, Implementierung und Anwendung von Verfahren der Altersfeststellung. Diese Praxisperspektive wurde mit einer Auswertung des aktuellen Rechtsrahmens, insbesondere des Digital Services Act und des Kommissionsvorschlags für den EU Kids Act, sowie internationaler Standards und regulatorischer Ansätze verbunden. Ziel war es, ein gemeinsames Verständnis der verfügbaren Verfahren zu schaffen und die Debatte um eine fundierte, technologieoffene Perspektive aus der Digitalen Wirtschaft zu ergänzen. Das Papier gibt die gemeinsame Sicht der beteiligten Working Groups wieder und nicht notwendigerweise die Position jedes einzelnen Mitgliedsunternehmens.

Ansprechpartner: **Fabian Miller**, Junior Public Affairs Manager – Data Society, miller@bvdw.org

www.bvdw.org

Impressum

Erscheinungsort und -datum	Berlin, 19. November 2026
Herausgeber	Bundesverband Digitale Wirtschaft (BVDW) e.V. Obentrautstraße 55, 10963 Berlin, +49 30 2062186 - 0, info@bvdw.org, www.bvdw.org Vorstand gem. § 26 BGB Carsten Rasner
Präsident	Dirk Freytag
Vizepräsident*innen	Thomas Duhr, Anke Herbener, Corinna Hohenleitner, Dr. Moritz Holzgraefe, Björn Kaspring, Julian Simons
Kontakt	politik@bvdw.org Vereinsregisternummer Amtsgericht Charlottenburg VR 42449 B
Rechtshinweise	Alle in dieser Veröffentlichung enthaltenen Angaben und Informationen wurden vom Bundesverband Digitale Wirtschaft (BVDW) e.V. sorgfältig recherchiert und geprüft. Diese Informationen sind ein Service des Verbandes. Für Richtigkeit, Vollständigkeit und Aktualität können weder der Bundesverband Digitale Wirtschaft (BVDW) e.V. noch die an der Erstellung und Veröffentlichung dieses Werkes beteiligten Unternehmen die Haftung übernehmen. Die Inhalte dieser Veröffentlichung und / oder Verweise auf Inhalte Dritter sind urheberrechtlich geschützt. Jegliche Vervielfältigung von Informationen oder Daten, insbesondere die Verwendung von Texten, Textteilen, Bildmaterial oder sonstigen Inhalten, bedarf der vorherigen Zustimmung durch den Bundesverband Digitale Wirtschaft (BVDW) e.V. bzw. die Rechteinhaber (Dritte).

EU-Transparenzregister-Nummer: 479540331468-69 Deutsches Lobbyregister: R000257