Datenschutzkonforme Altersverifikation im Internet

Zuverlässiger Jugendschutz bei datenschutzfreundlicher Ausgestaltung

Julian Hunter [1], Martin Steinebach [2], York Yannikos [3]

Abstract: Die Alterskontrolle im Internet ist eine zentrale Maßnahme zum Schutz Minderjähriger vor für sie ungeeigneten Inhalten. Zum Nachweis oder zur Bestimmung des Alters hat sich neben der klassischen „Vor-Ort-Prüfung“ von Ausweisdokumenten das Videoident-Verfahren als digitale Alternative etabliert, um der Schnelligkeit digitaler Abläufe gerecht zu werden, dessen Zuverlässigkeit aber mittlerweile durch neue und einfachere Umgehungsmöglichkeiten bedroht ist. Es besteht daher Bedarf nach neuen zuverlässigen Mitteln zur Altersverifikation im Internet. Dieser Beitrag beleuchtet unterschiedliche Konzepte zur Altersverifikation sowie deren rechtliche Anforderungen, insbesondere an den Datenschutz.

Keywords: Altersverifikation, Altersbestimmung, Datenschutz, Jugendschutz, KI, Künstliche Intelligenz, TOMs, Data-Protection-by-Design, EU-ID-Wallet, eID, EIDAS

1 Einleitung

Das Thema „Altersverifikation im digitalen Raum“ gewinnt zunehmend an Bedeutung, insbesondere im Kontext des Jugend- und Datenschutzes. In vielen digitalen Bereichen, von Online-Glücksspielen über den Zugang zu jugendgefährdenden Inhalten bis hin zum Versand altersbeschränkter Produkte, stellt sich die Frage, wie das Alter eines Nutzers zuverlässig verifiziert werden kann, ohne dabei übermäßig personenbezogene Daten preiszugeben. Dabei ist zu beachten, dass das Feststellen des Alters über eine einfache Prüfung im Sinne von „über 18 Jahre“ hinausgeht. In einigen Szenarien soll sichergestellt werden, dass eine Person einer bestimmten Altersgruppe angehört, etwa wenn Chaträume nur für eine spezifische Altersgruppe vorgesehen sind. Diese Arbeit betrachtet Ansätze zur Altersüberprüfung einer Person im Internet technisch und insbesondere rechtlich.

[1] Universität zu Köln, Lehrstuhl Recht der Digitalisierung, Albertus-Magnus-Platz, 50923 Köln, Deutschland; Karlsruher Institut für Technologie, Institut für Informationssicherheit und Verlässlichkeit (KASTEL), Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe, Deutschland, julian.hunter@kit.edu, https://orcid.org/0009-0002-2561-5135.
[2] Fraunhofer SIT, Multimedia Sicherheit und IT-Forensik, Rheinstraße 75, 64296 Darmstadt, martin.steinebach@sit.fraunhofer.de, https://orcid.org/0000-0002-0240-0388.
[3] Fraunhofer SIT, Nationales Forschungszentrum für angewandte Cybersicherheit (ATHENE), Rheinstr. 75, 64295 Darmstadt, Deutschland, york.yannikos@sit.fraunhofer.de, https://orcid.org/0009-0001-2751-5253.

doi:10.18420/inf2025_04

2 Hintergrund

Die Alterskontrolle im Internet ist eine wichtige Maßnahme zum Schutz Minderjähriger vor gefährlichen und für sie ungeeigneten Angeboten. Da digitale Angebote jederzeit und ortsunabhängig abrufbar sind, ist eine verlässliche Altersverifikation unerlässlich, um die Entwicklung junger Menschen zu schützen. Auch der Schutz vor anderen Nutzern, insbesondere Cyber-Grooming – dem gezielten Kontaktaufbau Erwachsener zu Minderjährigen mit sexuellen Absichten – erfordert effektive Kontrollmechanismen. Plattformen, die sich speziell an Kinder und Jugendliche richten, müssen daher auch sicherstellen können, dass Erwachsene keinen unberechtigten Zugang erhalten. Neben klassischen Identitätsprüfungen können KI-gestützte Verfahren und verhaltensbasierte Analysen unterstützend wirken.

Eine wirksame Alterskontrolle sollte dabei nicht nur zuverlässig, sondern auch datenschutzkonform erfolgen. Besonders wichtig sind die Grundsätze der Datensparsamkeit und Zweckbindung aus Art. 5 DSGVO. Gleichzeitig sollte das Verfahren nutzerfreundlich gestaltet sein, um die Akzeptanz bei erwachsenen Nutzern zu gewährleisten. Interoperabilität mit bestehenden technischen Standards sichert zudem eine breite Einsetzbarkeit. Ziel ist ein ausgewogenes System, das junge Menschen schützt und zugleich die Rechte und Bedürfnisse aller Nutzer berücksichtigt.

3 Technische Umsetzung

Die Alterskontrolle im digitalen Raum erfordert eine präzise und gleichzeitig datenschutzkonforme technische Umsetzung. Dabei lassen sich zwei zentrale technische Aufgaben unterscheiden: die Bestätigung des Alters gegenüber einem Diensteanbieter durch eine qualifizierte Instanz und die Erkennung des Alters durch technische Verfahren. Die Integration dieser Methoden in digitale Angebote wie Webseiten, Apps und Streaming-Dienste stellt eine weitere Herausforderung dar, da eine zuverlässige Alterskontrolle mit Nutzerfreundlichkeit und gesetzlichen Vorgaben in Einklang gebracht werden muss.

3.1 Bestätigung des Alters

Die Bestätigung des Alters setzt voraus, dass Nutzer ihr Alter über ein bereits vorhandenes Verfahren oder Dokument nachweisen können. Dabei existieren verschiedene Ansätze, die sich hinsichtlich des Datenschutzes, der Verlässlichkeit und der technischen Integration unterscheiden.

Eine Methode zur Altersverifikation ist die Vorlage offizieller Ausweisdokumente wie Personalausweise oder Reisepässe. Dies geschieht etwa über das Videoident-Verfahren (dazu Abschnitt 5.2) oder über die Online-Ausweisfunktion amtlicher Dokumente (dazu

Abschnitt 5.5). Viele Online-Plattformen setzen auf solche Verfahren, um den Zugang zu altersbeschränkten Inhalten zu regulieren. Eine weitere Möglichkeit zur Altersverifikation besteht in der persönlichen Ausweisvorlage vor Ort, etwa durch Banken, die Post oder andere vertrauenswürdige Institutionen (dazu Abschnitt 5.3).

3.2 Erkennung des Alters

Neben der expliziten Altersbestätigung durch Dokumente oder externe Verifikationsstellen werden seit den letzten Jahren auch vermehrt Verfahren zur automatisierten Alterserkennung eingesetzt. Diese Ansätze sind besonders für Plattformen relevant, die große Nutzerzahlen verwalten und dabei möglichst reibungslose Zugangskontrollen gewährleisten wollen.

Künstliche Intelligenz kann anhand von Gesichtserkennung und anderen biometrischen Merkmalen das ungefähre Alter eines Nutzers bestimmen. Moderne Ansätze analysieren Gesichtsstrukturen, Hautbeschaffenheit und andere Merkmale, um eine Alterseinschätzung vorzunehmen [AV21]. Solche Verfahren werden beispielsweise von Videoverifikationsdiensten genutzt, sind jedoch in Bezug auf Datenschutz und Genauigkeit umstritten. Große Technologieunternehmen wie Google oder Meta verfügen über umfangreiche Datenbestände, anhand derer das Alter von Nutzern indirekt geschätzt werden kann [Mc25][Ro25b]. Suchverläufe, Nutzungsmuster und Interaktionen mit bestimmten Inhalten ermöglichen es Algorithmen, das Alter eines Nutzers mit hoher Wahrscheinlichkeit zu bestimmen [Su24]. Diese Methode ist jedoch problematisch, da sie stark von bereits vorhandenen Profildaten abhängt und nicht für neue oder anonymisierte Nutzer geeignet ist.

3.3 Integration in Angebote

Die Altersverifikation muss sicher in unterschiedliche digitale Angebote integriert werden. Dabei muss gewährleistet sein, dass die Altersverifikation zuverlässig und manipulationssicher ist. Hier ist eine sichere Authentifizierung des Nutzers erforderlich, die idealerweise eine einmalige Verifikation mit Speicherung des Ergebnisses für zukünftige Sitzungen ermöglicht, ohne dabei personenbezogene Daten zu speichern, die nicht zwingend erforderlich sind. Zudem muss die Altersverifikation mit verschiedenen Browsern und Betriebssystemen kompatibel sein, um eine breite Anwendbarkeit sicherzustellen.

In mobilen Anwendungen bestehen zusätzliche technische Anforderungen aufgrund der spezifischen Nutzungsumgebung. Altersverifikationen müssen in bestehende App-Ökosysteme integriert werden und dürfen die Nutzungserfahrung nicht unverhältnismäßig einschränken. Insbesondere die Sicherheit von Identitätsnachweisen muss durch verschlüsselte Übertragungswege gewährleistet werden.

Auf Online-Plattformen, die eine Vielzahl unterschiedlicher Dienste und Inhalte anbieten, muss die Altersverifikation in die Plattformarchitektur integriert sein, damit Minderjährige von jugendgefährdenden Inhalten ausgeschlossen werden können, ohne die Nutzung für berechtigte Personen unnötig zu erschweren. Dies erfordert sichere Mechanismen zur Authentifizierung, beispielsweise durch Multi-Faktor-Validierung, sowie technische Maßnahmen zur Altersüberprüfung, die sowohl plattformübergreifend als auch skalierbar sind [YS25].

4 Rechtliche Notwendigkeit einer Altersverifikation

Im deutschen Recht sowie im EU-Recht finden sich zahlreiche Vorschriften, nach denen eine Altersverifikation notwendig sein kann oder sogar verpflichtend ist. Im Bereich des Jugendschutzes sind insbesondere §§ 4-5a des JMStV und § 6a GlüStV zu nennen. Darüber hinaus kann sich eine Notwendigkeit der Altersverifikation aber auch aus der Gestaltung des angebotenen Dienstes ergeben, etwa wenn ein Dienst nach spezifischen Altersgruppen getrennt angeboten werden oder explizit nicht an Kinder gerichtet sein soll (insb. mit Blick auf Art. 25 DSGVO und Art. 28 DSA).

In der Regel erfordert eine Altersverifikation die Verarbeitung personenbezogener Daten, sodass hierauf die Vorschriften der DSGVO Anwendung finden (Art. 2 Abs. 1 DSGVO). Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen“. Darunter fallen folglich alle Daten, die Rückschlüsse auf eine konkrete natürliche Person ermöglichen [Ka25][KK24]. Hierzu zählen auch abgeleitete Daten, also Daten, die aus einer Verarbeitung resultieren [Eu23a][Eu23b], wie etwa die Einordnung in Altersgruppen, sofern sie nicht so weit generalisiert wurden, dass Rückschlüsse auf eine einzelne Person nicht mehr möglich sind (dazu [Bi20], [BD20]).

Im Folgenden gehen wir näher auf einige Bestimmungen ein, nach denen eine Altersverifikation notwendig sein kann, sowie auf deren Anforderungen an die Ausgestaltung der Altersverifikation. Die folgende Darstellung deckt aus Gründen des Umfangs und des datenschutzrechtlichen Schwerpunkts dieses Beitrags nur eine Auswahl möglicher Notwendigkeiten ab, die einen Eindruck über Vorgaben an die Implementierung und Ausgestaltung von Altersverifikationssystemen vermitteln soll. Nicht berücksichtigt werden hier etwa die Einführung einer Altersverifikation durch Anbieter von Video-Sharing-Diensten nach Art. 28b AMVD-RL, umgesetzt in § 5a JMStV, sowie eine Einführung eines Altersverifikation zur Überprüfung der Geschäftsfähigkeit (vgl. § 104 ff. BGB) im Rahmen eines Vertragsschlusses im Internet oder wenn ein Dienst etwa nach Altersgruppen separiert angeboten werden soll (die Ausführungen zur datenschutzrechtlichen Ausgestaltung gelten hier aber entsprechend, dazu noch unter Abschnitt 4.2 und 4.3).

4.1 Unzulässige Angebote (§ 4 Abs. 2 JMStV)

Pornographische Angebote, jugendgefährdende Angebote i.S.d. § 18 Abs 1 JuSchG („indizierte“ Inhalte) oder sonstige Angebote, die „offensichtlich geeignet sind, die Entwicklung von Kindern und Jugendlichen oder ihre Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit [...] schwer zu gefährden“, sind nach § 4 Abs. 2 Satz 2 JMStV nur zulässig, wenn der Anbieter sicherstellt, dass sie nur Erwachsenen zugänglich ist (sog. „geschlossene Altersgruppe“). Hinzu kommt, dass das Zugänglichmachen pornographischer Inhalte gegenüber Minderjährigen nach § 184 Abs. 1 Nr. 2 StGB strafbar ist. Hier ist ein besonders strenger Maßstab an die Effektivität der Altersbeschränkung zu setzen. Eine Altersverifikation verhindert (nur) dann einen Zugang für Minderjährige i.S.d. § 4 Abs. 2 JMStV und § 184 Abs. 1 Nr. 2 StGB, wenn sie eine „effektive Barriere“ zwischen dem Inhalt und dem Minderjährigen darstellt [Bu07]. Dies setzt im Grundsatz voraus, dass das Altersverifikationssystem alle einfachen, naheliegenden und offensichtlichen Umgehungsmöglichkeiten ausschließt, wobei insbesondere die „Anonymität des Internets“ als Faktor zu berücksichtigen ist [Bu07].

Die Volljährigkeitsprüfung muss grundsätzlich persönlich und unter Vorlage eines amtlichen Dokuments erfolgen [Ko22]. Eine Identifikation ohne persönlichen Kontakt, etwa durch Videoidentifikation oder eine automatisierte kamerabasierte Altersermittlung durch Auswertung biometrischer Merkmale eines Live-Kamerabilds, ist nur zulässig, soweit es einen hohen Grad an Zuverlässigkeit aufweist [Ko22][Bu07][Li21].

Über die erstmalige Altersprüfung hinaus muss der Anbieter bei jedem weiteren Zugang durch sichere Authentifizierung sicherstellen, dass Minderjährige die Schutzmaßnahmen nicht durch einfaches Verschaffen von Zugangsdaten umgehen können [Ko22][Uk24].

4.2 Entwicklungsbeeinträchtigende Angebote (§ 5 JMStV)

§ 5 JMStV betrifft Angebote, die geeignet sind, die Persönlichkeitsentwicklung von Kindern oder Jugendlichen zu beeinträchtigen und die deswegen erst ab einem bestimmten Mindestalter freigegeben sind (ab 6, 12, 16 oder 18 Jahren). Anbieter solcher Angebote haben dafür Sorge zu tragen, dass Kinder oder Jugendliche solche Angebote, die nicht ihrer Altersgruppe entsprechen, üblicherweise nicht wahrnehmen. Die Anforderungen an die Effektivität der Altersbeschränkung und Altersverifikation sind daher sichtlich geringer als nach § 4 Abs. 2 JMStV [Ka24][Er21]. Ein Mittel zur Altersverifikation erfüllt schon dann die Anforderungen, wenn es Kindern und Jugendlichen, die das Freigabealter noch nicht erfüllt haben, den Zugang zumindest wesentlich erschwert oder mit einer Alterskennzeichnung versieht, sodass z.B. Eltern ihre Kinder durch Installation eines Jugendschutzfilters i.S.d. § 11 JMStV vor entsprechenden Inhalten schützen können (§ 5 Abs. 3 Nr. 1 JMStV).

4.3 Online-Glücksspiel (§ 6e Abs. 1, § 6a, § 4 Abs. 5 GlüStV 2021)

Bei Online-Glücksspiel ist die Altersbeschränkung mittels einer Registrierungspflicht vorgeschrieben (§ 6a GlüStV 2021). Veranstalter und Vermittler von öffentlichen Online-Glücksspielen müssen für jeden Spieler ein anbieterbezogenes Spielkonto einrichten. Jeder Spieler darf nur über ein einziges Benutzerkonto pro Anbieter verfügen. Daher ist im Rahmen der Registrierung nicht nur eine Altersverifikation notwendig, sondern auch eine Identifikation. § 6a Abs. 2 GlüStV 2021 regelt hierzu, dass Vorname, Nachname, Geburtsname, Geburtsdatum, Geburtsort und Wohnsitz erhoben werden müssen. Dies dient nicht primär der Altersverifikation, sondern zuvorderst der Spielsuchtprävention, insbesondere der Effektivität der Spielsuchtfrüherkennungsmechanismen nach § 6i Abs. 1 GlüStV 2021 [Mi21]. In der behördlichen Erlaubnis zum Angebot von Online-Glücksspiel, die notwendige Voraussetzung für Anbieter ist, bestimmt die Behörde geeignete und zuverlässige Verfahren (§ 6i Abs. 1 Satz 1 a.E. GlüStV 2021). Die Glücksspielbehörde orientiert sich auch an den Richtlinien zur Altersverifikation der Kommission für Jugendmedienschutz [Ge23][Mi21].

Die Gesetzesbegründung erwähnt etwa Videoident, Postident oder die Identifikation mit einer eID als taugliche Identifikationsmöglichkeiten. Nicht zulässig sei hingegen die bloße Bestätigung der Daten durch den Spieler [Mi21][Sc22].

Nach § 6e GlüStV 2021 müssen Veranstalter und Vermittler von Online-Glücksspiel außerdem durch geeignete technische Verfahren zur Identifizierung und Authentizierung sicherstellen, dass minderjährige Spieler vom Spiel ausgeschlossen sind. Dies stellt keine separate Verpflichtung zur Altersverifikation dar, sondern stellt im Nachgang der Registrierung und Altersverifikation eine Verpflichtung zur Authentifizierung und Identifizierung dar [Sc22] um etwa den Zugang Minderjähriger durch weitergegebene oder sonst erlangte Zugangsdaten auszuschließen.

4.4 Altersverifikation als Schutzmaßnahme i.S.d. Art. 25 DSGVO

Anbieter von digitalen Diensten können eine Altersverifikation auch als technische und organisatorische Maßnahme i.S.d. Art. 25 Abs. 1 DSGVO zum Schutz der Rechte und Freiheiten der Nutzer vorsehen („Data Protection by Design“). Dies ist insbesondere dann relevant, wenn die hinter dem Dienst stehende Datenverarbeitung Charakteristika aufweist, die mit hohen Risiken für die Rechte und Freiheiten von Kindern verbunden sind (z.B. umfangreiches Tracking und Profiling zum Zwecke der Personalisierung von Inhalten).

Aus Art. 25 Abs. 1 DSGVO ergibt sich für jeden Verantwortlichen eine Pflicht, bereits vor Beginn der Verarbeitung personenbezogener Daten eine Risikoabwägung vorzunehmen und die Risiken fortlaufend zu reevaluieren [Ha25][NW22][Ma21][Eu25c][Eu20]. In die Abwägung ist einzubeziehen, wie schwer die mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten der

betroffenen Personen sind und wie hoch die Wahrscheinlichkeit ist, dass die Risiken in einen Schaden umschlagen [Ma21]. Hierbei sind insbesondere Art, Umfang, Umstände und Zweck der Verarbeitung zu berücksichtigen [Eu20]. Sind die Risiken der Verarbeitung für Kinder so groß und ist die Eintrittswahrscheinlichkeit möglicher Schäden so hoch, dass ein Ausschluss von Kindern von dem Dienst geboten ist, muss der Anbieter eine Altersverifikation einführen [Eu23].

Das Altersverifikationssystem muss wirksam („geeignet“) sein, um einen entsprechenden Ausschluss Minderjähriger zu gewährleisten. Verlässt sich ein Verantwortlicher auf ein unwirksames Altersverifikationssystem und verarbeitet er infolgedessen unrechtmäßig Daten von Kindern, liegt ein Verstoß gegen Art. 25 Abs. 1 DSGVO vor, wenn er nicht weitere Schutzmaßnahmen getroffen hat, um die Altersverifikation zu ergänzen. Ob eine Maßnahme geeignet ist, richtet sich unter anderem nach dem Stand der Technik und nach dem Risiko für die Rechte und Freiheiten für die betroffenen Personen [Eu23][Eu20], insbesondere wenn es sich bei den Betroffenen um Kinder handelt (vgl. EG 38 DSGVO).

Die „Geeignetheit“ einer Maßnahme ist insbesondere daran zu messen, ob sie die Datenschutzgrundsätze auf wirksame Weise umsetzen kann [Eu20][Eu23] und ob sie den zu erwartenden Risiken für die Rechte der Betroffenen entsprechend ausgestaltet ist [Eu20][Eu23] (ausführlich hierzu noch unter im Abschnitt 4.2).

4.5 Altersverifikation als Maßnahme nach dem Digital Services Act

Art. 28 DSA sieht vor, dass Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, Maßnahmen zur Einhaltung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz von Minderjährigen ergreifen. Für Anbieter von Online-Plattformen, deren Dienste nicht auf Minderjährige abzielen, kann eine Altersverifikation dann ein geeignetes oder sogar notwendiges Mittel sein, um die Plattform für Minderjährige unzugänglich zu machen.

Der Begriff der Zugänglichkeit für Minderjährige i.S.d. Art. 28 DSA unterscheidet sich hierbei von dem nach § 4 Abs. 2 JMStV. Eine Online-Plattform ist nach Erwägungsgrund 71 des DSA Minderjährigen zugänglich, wenn „ihre allgemeinen Geschäftsbedingungen es Minderjährigen gestatten, den Dienst zu nutzen, wenn ihr Dienst sich an Minderjährige richtet oder überwiegend von Minderjährigen genutzt wird oder wenn dem Anbieter in anderer Weise bekannt ist, dass einige seiner Nutzer minderjährig sind, etwa weil er bereits personenbezogene Daten von Nutzern verarbeitet, aus denen das Alter der Nutzer zu anderen Zwecken hervorgeht“.

Eine Pflicht zur Einführung einer Altersverifikation sieht Art. 28 DSA nicht vor. Das ergibt sich nicht zuletzt aus der Formulierung „weil er bereits personenbezogene Daten [...] verarbeitet, aus denen das Alter [...] zu anderen Zwecken hervorgeht“, die dann obsolet wäre, wenn Anbieter in jedem Fall verpflichtet wären, nach Art. 28 DSA

personenbezogene Daten zu erheben, aus denen sich das Alter des Nutzers ergibt (ergo zum Zwecke der Altersverifikation). Zudem bestätigt auch Art. 28 Abs. 3 DSA, dass Anbieter von Online-Plattformen nicht verpflichtet sind, „zusätzliche“ personenbezogene Daten zu verarbeiten, um die Minderjährigkeit eines Nutzers festzustellen [Ho24][Gr23].

Sofern ein Anbieter von Online-Plattformen aber seine Plattform nicht an Minderjährige anbieten möchte und ebenso nicht den zusätzlichen Schutzpflichten aus Art. 28 Abs. 1 DSA unterfallen möchte, muss er dafür Sorge tragen, dass er Minderjährigen den Zugang zur Plattform soweit erschwert, dass sie nicht überwiegend von Minderjährigen genutzt wird. Des Weiteren kann allerdings die Altersverifikation ein nach Art. 28 DSA notwendiges Mittel sein, wenn die Plattform an sich Minderjährigen zugänglich ist, aber Dienste oder Inhalte anbietet, die für Minderjährige nicht geeignet sind [EU25b] (z.B. ein Online-Shop, der neben jugendfreien Produkten auch Spirituosen und Tabakwaren anbietet oder eine Videoplattform, die sowohl jugendfreie als auch altersbeschränkte Inhalte bereitstellt).

4.6 Zwischenfazit

Die zuvor erarbeitete Aufstellung zeigt, dass die Einführung einer Altersverifikation für eine Vielzahl an Anbietern digitaler Dienste relevant ist. Im Folgenden beleuchten wird daher die rechtlichen Anforderungen an die Gestaltung einer Altersverifikation.

5 Geeignete technische und organisatorische Schutzmaßnahmen (Art. 25 DSGVO)

Nach Art. 25 Abs. 1 DSGVO muss der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, um einen angemessenen Schutz für die Rechte und Freiheiten der Betroffenen bei der Verarbeitung ihrer personenbezogenen Daten zu gewährleisten und die in Art. 5 DSGVO genannten Datenschutzgrundsätze wirksam umzusetzen.

Wie bereits oben besprochen (siehe Abschnitt 4.1.4), kann ein Altersverifikationssystem eine technische oder organisatorische Schutzmaßnahme i.S.d. Art. 25 Abs. 1 DSGVO in Bezug auf die darauffolgende Datenverarbeitung zur Bereitstellung des eigentlichen Dienstes darstellen. Da aber auch im Rahmen einer Altersverifikation in der Regel personenbezogene Daten verarbeitet werden, müssen insoweit auch diese durch geeignete technische und organisatorische Maßnahmen geschützt werden.

Der Anbieter muss seine Altersverifikation so ausgestalten, dass nicht mehr Daten erhoben und verarbeitet werden als zur Erreichung des Verarbeitungszwecks erforderlich (Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO)

[Eu25c][Ro25][Ba24][Ha24][Ma21][SH19][Ma22][La22]. Für den Zweck der Durchführung einer Altersverifikation können zum einen Daten über das Alter der betroffenen Person erforderlich sein (z.B. Geburtsdatum) aber auch Daten, die die Feststellung ermöglichen, dass das angegebene Alter zu der handelnden Person gehört. Hier ist im Einzelfall zu prüfen, ob dabei Daten zur eindeutigen Identifizierung der betroffenen Person (z.B. Name und Anschrift) verarbeitet werden müssen oder ob eine Authentizität auch auf anderem Wege sichergestellt werden kann [SH19][Ma22][Bo25][Eu25c].

Der Grundsatz der Datenminimierung steht im engen Verhältnis zum Grundsatz der Zweckbindung. Eine Weiterverarbeitung personenbezogener Daten zu einem anderen Zweck als dem, für den sie erhoben wurden, ist ohne Einwilligung des Betroffenen nur zulässig, wenn sie gesetzlich angeordnet ist und einem Schutzziel aus Art. 23 DSGVO dient oder wenn der Weiterverarbeitungszweck mit dem Erhebungszweck kompatibel ist (vgl. Art. 6 Abs. 4 DSGVO) [AV25][BS25][He24][BP24][Ro25a][Eu25c]. Bei Daten, die zum Zweck der Altersverifikation erhoben wurden, ist das in der Regel zu verneinen [Eu25c], insbesondere wenn es sich um Kopien amtlicher Ausweisdokumente handelt [Pe19][Bu25]. Für personenbezogene Daten Minderjähriger, die für die Zwecke des Jugendschutzes, z.B. zur Altersverifikation, erhoben werden, sieht § 20 TDDDG ein ausdrückliches Weiterverarbeitungsverbot für kommerzielle Zwecke vor. § 20 TDDDG geht Art. 6 Abs. 4 DSGVO vor, soweit er Art. 6a Abs. 2 der AVMD-Richtlinie (RL 2010/13/EU in der Fassung der RL (EU) 2018/1808) umsetzt [Et22][Sc24][SG21]. § 20 TDDDG erfasst alle Anbieter von digitalen Diensten. Hingegen erfasst Art. 6a AMVD-RL nur Anbieter audiovisueller Mediendienste, was im deutschen Recht den Anbietern von Rundfunk und rundfunkähnlichen digitalen Diensten entspricht. Bezogen auf Anbieter sonstiger digitaler Dienste wird § 20 TDDDG von Art. 6 Abs. 4 DSGVO verdrängt [Sc24]. Allerdings wird die Weiterverarbeitung personenbezogener Daten von Kindern zu kommerziellen Zwecken in der Regel erst recht nicht i.S.d. Art. 6 Abs. 4 DSGVO kompatibel mit dem Erhebungszweck sein, da Kinder besonders schutzbedürftig sind (vgl. ErwGr. 38 DSGVO) und die Folgen einer Weiterverarbeitung für sie besonders gravierend sein können [Sc24]. Anbieter einer Altersverifikation müssen folglich Maßnahmen treffen, die gewährleisten, dass die erhobenen Daten nur für die Altersverifikation verarbeitet werden.

Anbieter müssen außerdem Maßnahmen treffen, damit personenbezogene Daten nur so lange in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht, wie für den Verarbeitungszweck erforderlich (Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO) [Ha25][Ba24][NW22]. Das heißt, sobald die Daten zum Zweck der Altersverifikation nicht mehr benötigt werden, sind sie zu löschen oder zu anonymisieren [Ha25]; vgl.[Ma22][Ba24]. Sieht etwa ein Dienst nur einen einmaligen Zugang mit vorangehender Altersverifikation vor (z.B. „Login als Gast“), sind die im Rahmen der Altersverifikation beim Betroffenen erhobenen Daten mit

Abschluss der Altersverifikationsprozesses zu löschen. Erstellt die betroffene Person zur Inanspruchnahme des Dienstes ein Benutzerkonto, so kann die Information über das Alter oder die Altersgruppe der betroffenen Person mit dem Benutzerkonto verknüpft werden. Das Geburtsdatum ist nur zu speichern, sofern die konkrete Angabe dessen für die Erbringung des Dienstes erforderlich ist. Personenbezogene Daten, die der Anbieter von der betroffenen Person zum Nachweis des Alters erhoben hat (z.B. eine Ablichtung eines geschwärzten Ausweisdokuments), sind mit Abschluss des Altersverifikationsprozesses zu löschen. Die Authentifizierung der betroffenen Person kann durch die Anmeldung im Benutzerkonto erfolgen, sodass die Speicherung der Identitäts- und Altersnachweise nicht länger erforderlich ist (vgl. Art. 11 Abs. 1 und EG 57 DSGVO) [Pe19][Ha25a][St25][Fr21][Ka22][Le22]. Die in dem Benutzerkonto gespeicherten Altersinformationen sind so weit zu abstrahieren, dass nur noch Informationen gespeichert sind, die für den jeweiligen Dienst erforderlich sind, etwa das Alter, die Altersgruppe oder nur die Information „volljährig“ [Eu20]. Entscheidet die Altersverifikation nur zwischen „Zugang“ und „kein Zugang“ zum Dienst und ist sie Voraussetzung für die Erstellung eines Benutzerkontos (z.B. zur Feststellung der Volljährigkeit), ergibt sich bereits aus dem Bestehen des Benutzerkontos die erforderliche Altersinformation, sodass keine Speicherung weitere Altersinformationen erforderlich ist.

Der Anbieter hat überdies das Benutzerkonto der betroffenen Person durch technische und organisatorische Maßnahmen gegen Zugriffe durch Dritte absichern (z.B. durch 2-Faktor-Authentifizierung und Passwort-Policen [Bu25a]).

Der Anbieter muss außerdem Maßnahmen zum Schutz der Integrität und Vertraulichkeit, insbesondere zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung oder sonstiger Beeinflussung der Daten treffen. Das schließt insbesondere die Bereitstellung oder die Unterstützung sicherer (insb. Verschlüsselter) Übertragungswege für die Übermittlung personenbezogener Daten zwischen Betroffenem und Verantwortlichem ein [Pe19], aber auch die Absicherung gespeicherter Daten.

Des Weiteren muss der Anbieter Maßnahmen treffen, um seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO nachzukommen. Dazu muss der Anbieter nachweisen können, etwa durch interne Konzepte und Protokolle, dass er die Voraussetzungen der DSGVO einhält [Vo22]. Eine Aufbewahrung der zum Altersnachweis vorgelegten Daten des Betroffenen über den Zeitraum der Altersverifikation hinaus ist auch zur Erfüllung der Rechenschaftspflicht nicht erforderlich.

6 Richtige Auswahl der Maßnahmen

Die Auswahl der Maßnahmen hängt zunächst davon ab, ob sie geeignet ist, die Datenschutzgrundsätze wirksam umzusetzen und den drohenden Risiken für die Rechte der Betroffenen angemessen entgegenwirken [Eu23][Eu20][Eu25a].

Des Weiteren hängt die Wahl auch von dem Stand der Technik und den Implementierungskosten für den Verantwortlichen ab. Verantwortliche sind verpflichtet, den gegenwärtigen technischen Fortschritt auf dem Markt zu berücksichtigen [Eu20][Ba24][NW22]. Anhaltspunkte für den aktuellen Stand der Technik können etwa Leitlinien und Beschlüsse von Behörden (z.B. von den Datenschutzbehörden, der KJM, dem BSI oder der BNetzA, EDSA, ENISA) oder internationale Standards (etwa von der ISO oder CEN/CENELEC) bieten [Ha25][Ba22][NW22][Ha24][Eu25c][Eu20].

Die Aufnahme der Implementierungskosten in die Abwägung soll den Verantwortlichen vor unverhältnismäßig hohen Ressourcenaufwand bewahren, wenn er auf günstigere, aber dennoch wirksame Alternativen zurückgreifen kann. Der Verantwortliche kann jedoch nicht mit Verweis auf zu hohe Kosten jegliche Art wirksamer Maßnahmen verweigern [Eu20][Ma21][Ha24].

7 Beurteilung einzelner Altersverifikationsmaßnahmen

Im Folgenden beurteilen wir unterschiedliche Maßnahmen zur Altersverifikation. Dabei gehen wir auf die derzeit gängigsten Verfahren ein, konkret die Abfrage von Dokumentennummern, die Videoidentifikation, die Vor-Ort-Überprüfung durch Dritte sowie die Altersverifikation mittels elektronischer Identifikation (eID). Die Selbstauskunft über das Alter werden wir hier nicht im Detail besprechen, da sie kein zuverlässiges Mittel zur Bestimmung des Alters darstellt und sich somit für die Zwecke der Altersverifikation nicht eignet [Eu23][Ob24].

7.1 Abfrage von Dokumentennummern

Häufig wird eine Altersverifikation durch die Angabe einer Personalausweis- oder Kreditkartennummer durchgeführt.

Aus der sog. „maschinenlesbaren Zone“ (MRZ) im Personalausweis ergibt sich neben der Ausweisnummer auch das Geburtsdatum. Werden diese Informationen abgefragt, lässt sich hierdurch das Alter der Person genau bestimmen. Die Informationen aus der MRZ entsprechen einem festgelegten Schema und lassen sich daher mathematisch errechnen [Bu25]. Der abgefragte Zahlencode besteht in der ersten Zeile aus der Seriennummer mit Prüfziffer und in der zweiten Zeile aus dem Geburtsdatum mit Prüfziffer sowie dem Gültigkeitsdatum mit Prüfziffer sowie einer Gesamtprüfziffer. Die Prüfziffern ergeben sich aus den vorangegangenen Informationen, sodass die Überprüfung der schematischen Korrektheit der Angaben ohne Hinzuziehung weiterer Informationen möglich ist. Umgekehrt lässt sich die Prüfung aber auch dadurch umgehen, dass man sich mithilfe (u.a. frei im Internet) verfügbarer Mittel einen schematisch korrekte Ziffernfolge mit dem gewünschten Geburtsdatum errechnen lässt.

Melderegisterabgleich anhand der Ausweisnummer ist allerdings nicht zulässig, da die Ausweisnummer nicht in § 44 Abs. 1 BMG als auskunftsfähiges und nicht in § 44 Abs. 3 BMG als identifizierungsfähiges Datum aufgezählt ist [Sc22] (aA wohl [Go17]).

Kreditinstitute sind nach § 11 GwG verpflichtet, beim Vertragsabschluss die Identität des Vertragspartners zu überprüfen. Bei Unsicherheit kann ggf. die Validität der Kreditkartennummer durch das Kreditinstitut verifiziert werden. Eine Übermittlung der Daten, die zum Zweck der Identifizierung nach § 11 GwG erhoben wurden, wozu auch das Geburtsdatum gehört (§ 11 Abs. 4 Nr. 1 lit. c GwG), durch das Kreditinstitut an einen anfragenden Diensteanbieter ist aber (ohne Einwilligung des Betroffenen) nicht zulässig, da keine Zweckkompatibilität vorliegt (vgl. hierzu Abschnitt 4.2).

Kreditinstitute geben Kreditkarten in der Regel nur an volljährige Personen aus. Daher lässt sich aufgrund der Kreditkartennummer jedenfalls vermuten, dass der Inhaber dieser Nummer das 18. Lebensjahr vollendet hat. Es gibt allerdings keine gesetzliche Regelung, die es Kreditinstituten verbietet, eine Kreditkarte mit Einwilligung der gesetzlichen Vertreter auch an Minderjährige auszugeben.

Die Abfrage von Dokumentennummern erfüllt nicht die Anforderung der „effektiven Barriere“ des § 4 Abs. 2 JMStV [Ka04][Bu07]. Da Minderjährige etwa über das soziale Umfeld oder die Eltern schnell an taugliche Dokumentennummern kommen können und sich solche Nummern auch frei im Internet finden oder errechnen lassen können, ist die Abfrage für Minderjährige einfach zu umgehen [Ka04][Bu07]. Auch ist fraglich, ob sie überhaupt geeignet ist, den Zugang für Personen bestimmter Altersgruppen i.S.d. § 5 JMStV wesentlich zu erschweren. Da sich entsprechende Nummern frei über das Internet finden lassen, ist es auch für Minderjährige kein wesentliches Hindernis, eine entsprechende Nummer einzugeben. Da Art. 25 DSGVO und Art. 28 DSA höhere Anforderungen an die Zuverlässigkeit der Altersverifikation stellen als § 5 JMStV ist die Abfrage von Dokumentennummern auch nach diesen Vorschriften keine geeignete Maßnahme.

7.2 Videoidentifikation

Die Videoidentifikation ist ein gängiges Verfahren zur Feststellung der Identität einer Person im Internet. Im Videoident-Verfahren wird ein amtliches Dokument (z.B. der Personalausweis) mittels Videoübertragung von einem geschulten Mitarbeiter auf Echtheit überprüft [Bu17]. Der Mitarbeiter gleicht dabei die auf dem Ausweis befindlichen Informationen mit den angegebenen Informationen ab, prüft Sicherheitsmerkmale (soweit mittels Videoübertragung prüfbar) und gleicht das Gesicht der Person mit dem auf dem Dokument befindlichen Passbild per Webcam ab.

Über das Videobild können allerdings nicht alle Sicherheitsmerkmale überprüft werden, etwa sind Guillochen, UV-Aufdrucke und Oberflächenprägungen sowie taktile (ertastbare) Sicherheitsmerkmale im Videobild nicht oder nicht zuverlässig überprüfbar [Ts22]. Die über das Videobild sichtbaren Sicherheitsmerkmale können hingegen digital

repliziert und somit gefälscht werden (hierzu ausführlich [Ts22]).

Umgekehrt lassen sich durch immer bessere und besser verfügbarere Deepfake-Anwendungen auch Gesichter immer glaubwürdiger replizieren. Folglich können Personen ihr Alter mit einem fremden Ausweisdokument verifizieren und dabei ihr Gesicht im Videobild mit dem des Inhabers des Ausweisdokuments ersetzen. Dabei kann bereits das auf dem Ausweisdokument befindliche Passfoto als Quelldokument für den Deepfake ausreichen [Se22][Se22a].

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat ihren Zuspruch zum Videoident-Verfahren insoweit geändert, als sie die Anwendung zur Identitätsüberprüfung nach § 11 GwG nur noch „als Brückentechnologie“ für zulässig erachtet [Bu22]. Die „Gematik“, die unter Anderem die technischen Spezifikationen für die Telematikinfrastruktur im Gesundheitswesen vorgibt, hat die Nutzung der Videoidentifikation durch Krankenkassen untersagt [Ge22].

Das Videoident-Verfahren erfüllt nicht dasselbe Maß an Zuverlässigkeit wie die persönliche Identifikation. Es sollte daher nicht dort eingesetzt werden, wo ein hohes Maß an Zuverlässigkeit gefordert wird. Gleichwohl entspricht es derzeit noch dem gegenwärtigen Stand der Technik, wenn es darum geht, eine effektive Barriere für die Nutzung von bestimmten Diensten durch Minderjährige zu schaffen [Bu22]. Werden Ausweisdokumente nicht nur in Echtzeit mittels Videoübertragung geprüft, sondern etwa als digitale Kopie übersendet, ist zum einen auf die Möglichkeit der Übersendung einer geschwärzten Kopie hinzuweisen, sofern dies nicht die Überprüfung von Sicherheitsmerkmalen beeinträchtigt, und zum anderen sicherzustellen, dass die Daten nach Abschluss der Altersverifikation gelöscht werden.

7.3 Persönliche Identifikation durch Dritte

Eine Identifikation kann auch durch Dritte durchgeführt werden.

Bei der Postident-Methode wird die Identität einer Person vor Ort entweder in einer Postfiliale oder durch einen Postmitarbeiter an der Haustür (z.B. bei Zusendung einer PIN-Nummer per Post) überprüft. Dadurch, dass die Überprüfung unter Anwesenden geschieht, kann sichergestellt werden, dass alle visuellen Sicherheitsmerkmale des Ausweisdokuments valide sind und dass die ausweisende Person tatsächlich die Person auf dem Ausweisdokument ist.

Das Bank-Ident-Verfahren ist mit dem Postident-Verfahren vergleichbar mit dem Unterschied, dass anstelle der Post eine Bank bzw. ein Kreditinstitut die Identifikation vornimmt. Zur Bestätigung der Identität können Nutzer sich mit ihren Online-Banking-Informationen einloggen und ihre Identität im Internet durch ihre Bank bestätigen. Allerdings erfolgt eine Identifikation bei der Bank nicht immer über persönliche Identifikation, da die BaFin auch Videoident lange als valides Mittel zur Identifikation zugelassen hat und weiterhin aus Brückentechnologie zulässt [Bu22].

Durch zusätzliche Maßnahmen (insb. die Abfrage von PIN-Nummern und die Einrichtung einer 2-Faktor-Authentifinzerung) kann die Authentizität der handelnden Person ausreichend sichergestellt werden.

Die persönliche Identifikation durch Dritte erfüllt ein hohes Maß an Zuverlässigkeit, da Echtheitsmerkmale des Ausweisdokuments durch Inaugenscheinnahme vor Ort überprüft werden und die Identität der sich ausweisenden Person zuverlässig festgestellt werden kann. Es erfüllt daher auch richtigerweise die strengen Anforderungen des § 4 Abs. 2 JMStV [Bu07][Ko22]. Darüber hinaus ist diese Maßnahme datenschutzfreundlich, da keine Ausweisdokumente digital vervielfältigt werden und übersendet werden müssen. Sie ist allerdings im Vergleich zu anderen Maßnahmen aufwändig, da sie entweder einen persönlichen Besuch einer Post- oder Bankfiliale erfordert oder das persönliche Entgegennehmen einer Postsendung.

7.4 Biometrische Altersbestimmung

Bei der biometrischen Altersbestimmung werden mithilfe eines KI-Systems die Gesichtszüge der betroffenen Person über die Handykamera oder Webcam analysiert. Das KI-System schätzt auf Grundlage seiner Trainingsdaten das Alter der betroffenen Person ein.

Sofern biometrische Daten zur eindeutigen Identifizierung verarbeitet werden, sind zusätzlich die Anforderungen des Art. 9 DSGVO zu erfüllen. Zweck der biometrischen Altersbestimmung ist aber meist, eine Altersbestimmung ohne Identifikation der betroffenen Person vorzunehmen. In diesem Fall ist Art. 9 DSGVO nicht anwendbar [AV25a][Pe25].

Die biometrische Altersbestimmung mittels KI bietet allerdings keine verlässliche Maßnahme zur Bestimmung des tatsächlichen Alters, da sie lediglich anhand der Gesichtszüge das „Altaussehen“, nicht aber das Alter selbst bestimmen kann. Sofern der Zweck der Altersbestimmung ist, Minderjährige von einem Dienst auszuschließen, insb. in den Fällen des § 4 Abs. 2 JMStV, in denen rechtlich eine „effektive Barriere“ gefordert ist, sollte eine Alterseinschätzung eher „zu jung“ einschätzen und damit von dem Zugang ausschließen. Diese Maßnahme birgt dann aber die Gefahr der Diskriminierung für „jung aussehende“ Personen, die unrichtig als minderjährig eingestuft werden. Die KJM stuft diese Systeme daher lediglich als „Teillösung“ ein [Ko22a][Ko22b], teils aber wohl auch als ausreichend [Ko22c].

Der Anbieter muss außerdem technische und organisatorische Maßnahmen treffen, dass die zur Alterverifikation erhobenen Daten nicht zum Training der künstlichen Intelligenz weiterverarbeitet werden, da diese Zwecke nicht miteinander kompatibel sind (vgl. dazu auch Art. 57 AI Act). Hierfür ist eine separate Rechtsgrundlage erforderlich, in der Regel eine Einwilligung [Al25].

7.5 Elektronische Identifikation

Mithilfe elektronischer Ausweisdokumente (z.B. der elektronische Personalausweis, der elektronische Aufenthaltstitel oder die eID-Karte) können sich Karteninhaber Anbietern von Diensten im Internet gegenüber digital Identifizieren und ihr Alter nachweisen (§ 18 PAuswG, § 78 Abs. 5 AufenthG, § 12 eIDKG). Die folgenden Ausführungen beziehen sich nur auf den elektronischen Personalausweis, gelten aber ebenso für den elektronischen Aufenthaltstitel und die eID-Karte, da die Vorschriften im Wesentlichen auf das PAuswG verweisen (siehe etwa § 78 Abs. 5 AufenthG und § 12 Abs. 3 Satz 2, § 14, § 15 Abs. 2 eIDKG).

Der elektronische Personalausweis enthält personenbezogene Daten, die der Karteninhaber dem Anbieter übermitteln kann, insbesondere den Vor- und Familiennamen, die Anschrift und das Geburtsdatum (§ 18 Abs. 3 Satz 2 PAuswG).

Voraussetzung für die Übermittlung dieser Daten aufseiten des Anbieters ist ein Berechtigungszertifikat. Dieses kann der Anbieter entweder nach § 21 Abs. 2 PAuswG selbst beantragen oder aber seinerseits einen Anbieter von Identifikationsdiensten in Anspruch nehmen, der über ein Berechtigungszertifikat verfügt (z.B. bietet auch Postident die Möglichkeit der Online-Ausweisfunktion an). Um Daten aus dem elektronischen Personalausweis digital übermitteln zu können, muss der Karteninhaber über die Client-Software („AusweisApp“) sowie über ein Kartenlesegerät oder einen NFC-Chipleser verfügen [Bu20]. Letzterer ist auch in den meisten modernen Smartphones verbaut. Der Karteninhaber kann die personenbezogenen Daten aus seinem elektronischen Personalausweis auch auf einem mobilen Endgerät (i.d.R. Smartphone) speichern um die erforderlichen Daten direkt von seinem Endgerät aus abrufen zu lassen (§ 10a PAuswG).

Die Altersverifikation erfolgt gemäß § 18 Abs. 2 PAuswG durch Übermittlung der relevanten Daten aus dem elektronischen Personalausweis oder aus dem Speicher eines mobilen Endgeräts, sofern der Karteninhaber diese Möglichkeit nach § 10a PAuswG eingerichtet hat. Dabei hat der Nutzer die Möglichkeit, lediglich eine Angabe zu übermitteln, ob ein bestimmtes Alter über- oder unterschritten wird (§ 18 Abs. 3 Nr. 10 PAuswG). Es muss daher nicht zwingend das vollständige Geburtsdatum übertragen werden [Ma21].

Zur Authentifizierung der sich ausweisenden Person wird zudem eine PIN-Nummer abgefragt, die der Karteninhaber entweder von der ausstellenden Behörde per Post zugesendet bekommt oder bei der Behörde vor Ort selbst vergibt. Dadurch soll verhindert werden, dass das elektronische Ausweisdokument durch Unbefugte verwendet wird.

Die elektronische Identifikation steht allerdings erst ab einem gewissen Mindestalter zur Verfügung. Etwa müssen deutsche Staatsbürger sowie Träger eines deutschen Aufenthaltstitels mindestens 16 Jahre alt sein, um die Online-Ausweisfunktion ihres Personalausweises zu nutzen (§ 18 Abs. 1 PAuswG, auch i.V.m. § 78 Abs. 5 AufenthG). Staatsbürger anderer EU- und EWR-Staaten dürfen ab dem 13. Lebensjahr eine eID-Karte beantragen und nutzen (§ 8 Abs. 1 eIDKG). Des Weiteren müssen Nutzer über die

notwendige Hard- und Software verfügen. Das kann etwa für Personen mit geringem Vermögen oder für Personen, die nicht über die nötigen technischen Kenntnisse oder Fähigkeiten verfügen, ein Hindernis darstellen.

Der Anbieter der Altersverifikation hingegen muss eine Berechtigung nach § 21 beantragen und alle 3 Jahre erneuern und seinerseits die technischen Voraussetzungen für das Abfragen von eID-Informationen implementieren.

Die Altersverifikation mittels elektronischer Ausweisdokumente stellt daher eine zuverlässige, aber im Vergleich zu den anderen genannten Möglichkeiten eine aufwändige Maßnahme dar. Sie sollte daher derzeit insbesondere dort eingesetzt werden, wo ein hohes Maß an Zuverlässigkeit über die gemachten Angaben notwendig ist. Wegen des vergleichsweise hohen Aufwands auf Nutzerseite sollte aber daneben derzeit noch eine alternative (zuverlässige) Möglichkeit der Altersverifikation ermöglicht werden, etwa die persönliche Identifikation durch Dritte [Eu25b].

8 Fazit

Wie aufgezeigt eignen sich mehrere Verfahren grundsätzlich zur Durchführung einer Altersverifikation im Internet. Anbieter müssen die Wahl des Mittels unter anderem davon abhängig machen, wie groß die Risiken für die Rechte der Personen sind, die durch die Altersverifikation ausgeschlossen und/oder geschützt werden sollen. Teilweise gibt das Recht Vorgaben über die Einschätzung der Risiken (z.B. § 4 Abs. 2 JMStV), teilweise ist es die Aufgabe des Anbieters, diese Risiken selbst zutreffend einzuschätzen (z.B. Art. 25 DSGVO). Darüber hinaus müssen Anbieter auch regelmäßig reevaluieren, ob die von ihnen genutzte Altersverifikation, unter Berücksichtigung des Stands der Technik und insbesondere der Umgehungsmöglichkeiten, noch das Maß an Schutz bietet. Auch sollten Anbieter in Betracht ziehen, ob nicht eine Implementierung einer Altersverifikation mittels eID praktikabel und finanziell umsetzbar wäre. Bis Ende 2026 sind alle EU-Staaten nach der neuen eIDAS-Verordnung 2.0 (VO (EU) 2024/1183) verpflichtet, ihren Bürgern eine „digitale Brieftasche“ bereitzustellen, welche eine einheitliche Identifikation oder auch spezifische Altersverifikation EU-weit ermöglichen soll. Die EU-Kommission hat hierzu bereits technische Richtlinien veröffentlicht [Eu25].

Danksagungen

Diese Forschungsarbeit wurde unterstützt vom Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE. ATHENE wird gemeinsam vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) gefördert. Dieser Beitrag wurde vom Topic „Engineering Secure Systems“ der Helmholtz-Gemeinschaft mit Unterstützung der

KASTEL Security Research Labs Karlsruhe gefördert.

Literaturverzeichnis

[Al25] Albrecht, J. P.: In (Simitis, Hornung, Spiecker gen. Döhmann, Hrsg.): Datenschutzrecht, 2. Aufl. 2025, Art. 6 DSGVO. Nomos Verlagsgesellschaft, Baden-Baden, 2025.

[AV21] Agbo-Ajala, O.; Viriri, S.: Deep learning approach for facial age classification: a survey of the state-of-the-art. Artificial Intelligence Review, 54(1), S. 179 ff., 2021.

[AV25] Albers, M.; Veit, R.: In: BeckOK Datenschutzrecht, 51. Edition 01.02.2025, Art. 6 DSGVO. Verlag C.H.Beck, München, 2025.

[AV25a] Albers, M.; Veit, R.: In: BeckOK Datenschutzrecht, 51. Edition 01.02.2025, Art. 9 DSGVO. Verlag C.H.Beck, München, 2025.

[Ba24] Baumgartner, U.: In: (Ehmann, Selmayr, Hrsg.): DSGVO, 3. Aufl. 2024, Art. 25. Verlag C.H.Beck, München, 2024.

[BD20] Bischoff, C.; Drechsler, J.: Pseudonymisierung und Anonymisierung im Rahmen klinischer Prüfungen von Arzneimitteln (Teil II). PharmR 2020, 389. 2020.

[Bi20] Bischoff, C.: Pseudonymisierung und Anonymisierung im Rahmen klinischer Prüfungen von Arzneimitteln (Teil I). PharmR 2020, 309. 2020.

[Bo25] Borges, G.: In: BeckOK IT-Recht, 18. Edition 01.04.2025, Art. 25 DSGVO. Verlag C.H.Beck, München, 2025.

[BP24] Buchner, B.; Petri, T.: In (Kühling, Buchner, Hrsg.): DSGVO BDSG, 4. Aufl. 2024, Art. 6 DSGVO. Verlag C.H.Beck, München, 2024.

[BS25] Borges, G.; Steinrötter, B.: In: BeckOK IT-Recht, 18. Edition 01.04.2025, Art. 6 DSGVO. Verlag C.H.Beck, München, 2025.

[Bu07] Bundesgerichtshof, Urt. V. 18.10.2007 - I ZR 102/05. 2007.

[Bu17] Bundesamt für Sicherheit in der Informationstechnik, Rundschreiben 3/2017. 2017.

[Bu20] Bundesamt für Sicherheit in der Informationstechnik, German eID Whitepaper, Version 1.4, 2020.

[Bu22] Bundesanstalt für Finanzdienstleistungsaufsicht, Ergebnis der Evaluierung des Videoidentifizierungsverfahrens i. S. d. Rundschreibens 3/2017 (GW), 2022.

[Bu25] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Recht auf Auskunft, https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte_Auskunftsrecht.html, Stand: 6.6.2025.

[Bu25a] Bundesamt für Sicherheit in der Informationstechnik, Sichere Passwörter erstellen. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-

passwoerter-erstellen_node.html, Stand: 6.6.2025.

[Bu25b] Bundesministerium des Innern und für Heimat, Die maschinenlesbare Zone in deutschen Ausweisen und Pässen, 2025; https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/moderne-verwaltung/ausweise/maschinenlesbare-zone-paesse-ausweise.pdf?__blob=publicationFile&v=17, Stand: 6.6.2025.

[Et22] Ettig, D.: In (Taeger, Gabel, Hrsg.): DSGVO – BDSG – TTDSG, 4. Aufl. 2022, § 20 TTDSG. Dfv Mediengruppe, Frankfurt am Main, 2022.

[Eu20] Europäischer Datenschutzausschuss, Leitlinien 4/2019 zu Artikel 25, Version 2.0, 2020.

[Eu23] Europäischer Datenschutzausschuss, Verbindlicher Beschluss 2/2023. 2023.

[Eu23a] Europäischer Gerichtshof, Urt. v. 4. Mai 2023 - C-487/21. 2023.

[Eu23b] Europäischer Gerichtshof, Urt. v. 22. Juni 2023 – C-579/21. 2023.

[Eu25] Europäische Kommission, https://digital-strategy.ec.europa.eu/de/library/implementing-regulation-european-digital-identity-wallets, Stand: 6.6.2025.

[Eu25a] European Digital Identity Project, Age Verification Solution Technical Specification, 2025, https://github.com/eu-digital-identity-wallet/av-doc-technical-specification, Stand: 6.6.2025.

[Eu25b] Europäische Kommission, Draft Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065. 2025.

[Eu25c] Europäischer Datenschutzausschuss, Statement 1/2025 on Age Assurance. 2025.

[Er21] Erdemir, M.: In (Bornemann, Erdemir, Hrsg.): Jugendmedienstaatsvertrag, 2. Aufl. 2021, § 5 JMStV. Nomos Verlagsgesellschaft, Baden-Baden, 2021.

[Fr21] Frenzel, E. M.: In (Paal, Pauly, Hrsg.): DSGVO BDSG, 3. Aufl. 2021, Art. 11 DSGVO. Verlag C.H.Beck, München, 2021.

[Ge22] Gematik, Pressemitteilung v. 09.08.2022. https://www.gematik.de/newsroom/news-detail/pressemitteilung-gematik-untersagt-bis-auf-weiteres-nutzung-von-videoident-verfahren-in-der-telematikinfrastruktur, Stand: 6.6.2025.

[Ge23] Gemeinsame Glücksspielbehörde der Länder, Glücksspielregulierung in Deutschland für Glücksspiele im Internet, 2023. https://www.gluecksspiel-behoerde.de/images/pdf/231101_Broschuere_Gluecksspielregulierung%20in%20Deutschland.pdf, Stand: 6.6.2025.

[Go17] Gombert, P.: In (Spörl, Sinock, Gombert, Koller, Hrsg.): Melde-, Pass- und Ausweisrecht, Stand November 2017, § 44 BMG. Wolters Kluwer, Hürth, 2017.

[Gr23] Grisse, K.: In (Hofmann, Raue, Hrsg.): Digital Services Act, 1. Aufl. 2023, Art. 28 DSA. Nomos Verlagsgesellschaft, Baden-Baden, 2023.

[Ha24] Hartung, J.: In (Kühling, Buchner, Hrsg.): DSGVO BDSG, 4. Aufl. 2024, Art. 25

DSGVO. Verlag C.H.Beck, München, 2024.

[Ha25] Hansen, M.: In (Simitis, Hornung, Spiecker gen. Döhmann, Hrsg.): Datenschutzrecht, 2. Aufl. 2025, Art. 25 DSGVO. Nomos Verlagsgesellschaft, Baden-Baden, 2025.

[Ha25a] Hansen, M.: In (Simitis, Hornung, Spiecker gen. Döhmann, Hrsg.): Datenschutzrecht, 2. Aufl. 2025, Art. 11 DSGVO. Nomos Verlagsgesellschaft, Baden-Baden, 2025.

[He24] Heberlein, H.: In (Ehmann, Selmayr, Hrsg.): DSGVO, 3. Aufl. 2024, Art. 6. Verlag C.H.Beck, München, 2024.

[Ho24] Holznagel, D.: In (Müller-Terpitz, Köhler, Hrsg.): Digital Services Act, 1. Aufl. 2024, Art. 28 DSA. Verlag C.H.Beck, München, 2024.

[Ka04] Kammergericht Berlin, Urt. v. 26.4.2004 – (5) 1 Ss 436/03. 2004.

[Ka22] Kampert, D.: In (Sydow, Marsch, Hrsg.): DSGVO – BSDG, 3. Aufl. 2022, Art. 11 DSGVO. Nomos Verlagsgesellschaft 2022.

[Ka24] Kaspar, M.: In (Binder, Vesting, Hrsg.): Rundfunkrecht, 5. Aufl. 2024, § 5 JMStV. Verlag C.H.Beck, München, 2024.

[Ka25] Karg, M.: In (Simitis, Hornung, Spiecker gen. Döhmann, Hrsg.): Datenschutzrecht, 2. Aufl. 2025, Art. 4 Nr. 1 DSGVO. Nomos Verlagsgesellschaft, Baden-Baden, 2025.

[KK24] Kühling, J; Klar, M.: In (Kühling, Buchner, Hrsg.): DSGVO BDSG, 4. Aufl. 2024, Art. 4 Nr. 1 DSGVO. Verlag C.H.Beck, München, 2024.

[Ko22] Kommission für Jugendmedienschutz, AVS-Raster v. 12.5.2022.

[Ko22a] Kommission für Jugendmedienschutz, Entscheidung zu „Age Verification“ der Ondato UAB, 2022, https://www.kjm-online.de/themen/technischer-jugendmedienschutz/unzulaessige-inhalte/, Stand: 6.6.2025.

[Ko22b] Kommission für Jugendmedienschutz, Entscheidung zu „facial age estimation“ der KYC AVC UK Ltd., https://www.kjm-online.de/themen/technischer-jugendmedienschutz/unzulaessige-inhalte/, Stand: 6.6.2025.

[Ko22c] Kommission für Jugendmedienschutz, Entscheidung zu „Ageware“ der Biometric Ventures s.r.o., 2022, https://www.kjm-online.de/themen/technischer-jugendmedienschutz/unzulaessige-inhalte/, Stand: 6.6.2025.

[La22] Lang, M.: In (Taeger, Gabel, Hrsg.): DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 25 DSGVO. Dfv Mediengruppe, Frankfurt am Main, 2022.

[Le22] Lee-Wunderlich, H.: In (Taeger, Gabel, Hrsg.): DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 11 DSGVO. Dfv Mediengruppe, Frankfurt am Main, 2022.

[Li21] Liesching, M.: In (Paschke, Berlit, Meyer, Kröner, Hrsg.): Gesamtes Medienrecht, 4. Aufl. 2021, § 4 JMStV. Nomos Verlagsgesellschaft, Baden-Baden, 2021.

[Ma21] Martini, M.: In (Paal, Pauly, Hrsg.): DSGVO BDSG, 3. Aufl. 2021, Art. 25 DSGVO. Verlag C.H.Beck, München, 2021.

[Ma22] Mantz, R.: In (Sydow, Marsch, Hrsg.): DSGVO – BSDG, 3. Aufl. 2022, Art. 25 DSGVO. Verlag C.H.Beck, München, 2022.

[Mc25] McConvey, J. R.: YouTube, Meta lean into age assurance in 2025, https://www.biometricupdate.com/202502/youtube-meta-lean-into-age-assurance-in-2025, Stand: 6.6.2025.

[Mi21] Ministerium für Inneres und Sport Sachsen-Anhalt, Erläuterungen zum GlüStV 2021, 2021.

[NW22] Nolte, N.; Werkmeister, C.: In (Gola, Heckmann, Hrsg.): DSGVO BDSG, 3. Aufl. 2022, Art. 25 DSGVO. Verlag C.H.Beck, München, 2022.

[Ob24] Oberverwaltungsgericht Niedersachsen, Beschl. v. 23.1.2024 – 14 LA 1/24. 2024.

[Pe19] Petrlic, R.: Identitätsprüfung bei elektronischen Auskunftsersuchen nach Art. 15 DSGVO, DuD 2019, 71. 2019.

[Pe25] Petri, T.: In (Simitis, Hornung, Spiecker gen. Döhmann, Hrsg.): Datenschutzrecht, 2. Aufl. 2025, Art. 9 DSGVO. Nomos Verlagsgesellschaft, Baden-Baden 2025.

[Ro25] Roßnagel, A.: In (Simitis, Hornung, Spiecker gen. Döhmann, Hrsg.): Datenschutzrecht, 2. Aufl. 2025, Art. 5 DSGVO. Nomos Verlagsgesellschaft, Baden-Baden 2025.

[Ro25a] Roßnagel, A.: In (Simitis, Hornung, Spiecker gen. Döhmann, Hrsg.): Datenschutzrecht, 2. Aufl. 2025, Art. 6 Abs. 4 DSGVO. Nomos Verlagsgesellschaft, Baden-Baden 2025.

[Ro25b] Roth, E.: Google will use machine learning to estimate a user's age, https://www.theverge.com/news/610512/google-age-estimation-machine-learning, Stand: 6.6.2025.

[Sc22] Schmitz, T.: In (Hamacher, Krings, Otto, Hrsg.): Glücksspielrecht, 1. Aufl. 2022, § 6a GlüStV. Nomos Verlagsgesellschaft, Baden-Baden 2022.

[Sc22a] Schwabenbauer, T.: In (Engelbrecht, Schwabenbauer, Hrsg.): Bundesmeldegesetz, 1. Aufl. 2022, § 44 BMG. Verlag C.H.Beck, München, 2022.

[Sc24] Schürmann, K.: In (Auernhammer, Hrsg.): DSGVO – BDSG, 8 Aufl. 2024, § 20 TTDSG. Wolters Kluwer, Hürth, 2024.

[Se22] Sensity B.V. Deepfakes vs Biometric KYC Verification. https://sensity.ai/blog/deepfake-detection/deepfakes-vs-kyc-biometric-verification/, Stand: 6.6.2025.

[Se22a] Sensity B.V. ID Verification Spoofing. https://www.youtube.com/watch?v=SU9K1LsgX7c, Stand: 6.6.2025.

[SG21] Schreiber, K.; Gottwald, B.: Jugendschutz durch Datenschutz. MMR 2021, 467. 2021.

[SH19] Spindler, G./Horváth, A. Z.: In (Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 25 DSGVO. Verlag C.H.Beck, München, 2019.

[St25] Steinrötter, B.: In: BeckOK IT-Recht, 18. Edition 01.04.2025, Art. 11 DSGVO. Verlag C.H.Beck, München, 2025.

[Su24] Suh, J. H.: Multi-label prediction-based fuzzy age difference analysis for social profiling of anonymous social media. Applied Sciences, 14(2), S. 790 ff., 2024.

[Ts22] Tschirsich, M.: Praktischer Angriff auf Video-Ident, Version 1.2, 2022.

[Uk24] Ukrow, J.: In (Cole, Oster, Wagner, Hrsg.): MStV – JMStV, 102. Lfg. 12/2024, § 4 JMStV. C.F.Müller, Heidelberg, 2024.

[Vo22] Voigt, P.: In (Taeger, Gabel, Hrsg.): DSGVO BDSG TTDSG, 4. Aufl. 2022, Art. 5 DSGVO. Verlag C.H.Beck, München, 2022.

[YS25] Yannikos, Y.; Steinebach, M.: Datensparsame Altersverifikation. BzKJAKTUELL 2/2025. Bundeszentrale für Kinder- und Jugendmedienschutz. https://www.bzkj.de/bzkj/service/publikationen/bzkj-aktuell/datensparsame-altersverifikation-265314, Stand: 6.6.2025.