Technical Supplement zum öffentlichen Appell gegen die indirekte Identitätsbindung gewöhnlicher VPN-Nutzung in der Europäischen Union

Anlage, Vertiefung zur Verwendung durch Kommission, Parlament, Rat, DSA-Koordinatoren und Datenschutzaufsichten

1. Zweck und Evidenzstandard

Dieser Anhang verdichtet die technische und rechtliche Befundlage, auf der der öffentliche Appell aufbaut. Es trennt strikt zwischen verifizierter Tatsache, starker Indikation, plausibler Inferenz und spekulativem, aber strategisch relevantem Risiko. Der Maßstab ist bewusst eng: Nicht jeder politisch denkbare Eskalationspfad wird als bestehende Norm ausgegeben; umgekehrt wird das Fehlen eines fertigen „VPN-ID-Gesetzes“ nicht mit dem Fehlen einer realen Gefahr verwechselt.

2. Was heute offiziell gilt

Heute existiert in der Europäischen Union keine allgemeine Rechtsnorm, die gewöhnliche VPN-Nutzung als solche einer Alters- oder Identitätsverifikation unterstellt. Die einschlägigen DSA-Leitlinien und die unionsweite Altersverifikationsinitiative zielen offiziell auf gesetzlich altersbeschränkte Inhalte und auf Plattformen, die für Minderjährige zugänglich sind, nicht auf allgemeine Sicherheits- und Privatsphäre Werkzeuge.[1]

Gleichzeitig baut die Kommission eine unionsweite Alters- und Attributinfrastruktur auf:

- EU Age Verification Scheme
- Trusted Proof-of-Age Providers List
- Trusted Solutions List
- offizielle App-Verteilung und
- technische Interoperabilität mit künftigen EU Digital Identity Wallets.

Mitgliedstaaten sollen mindestens eine EU Digital Identity Wallet bereitstellen; die Altersverifikationslösung ist ausdrücklich als vorgelagerte oder integrierbare Mini-Wallet beschrieben.[2]

---

1 Vgl. **Europäische Kommission**, „*Commission publishes guidelines on the protection of minors*“, 14 July 2025, sowie „*The EU approach to age verification*“, 29 April 2026. Die offizielle Zielrichtung betrifft altersbeschränkte Inhalte und Plattformen im Minderjährigenschutz, nicht allgemeine Sicherheitswerkzeuge.
https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors,
https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification.

2 Vgl. **Europäische Kommission**, „*Commission sets out a common approach for EU-wide Age Verification technologies*“, 29 April 2026; „*The EU approach to age verification*“, 29 April 2026; sowie „*EU Digital Identity Wallet implementation*“. Die Kommission benennt *EU Age Verification Scheme*, *Trusted Proof-of-Age Providers List*, *Trusted Solutions List* und die Interoperabilität mit künftigen *EU Digital Identity Wallets* ausdrücklich:
https://digital-strategy.ec.europa.eu/en/library/commission-sets-out-common-approach-eu-wide-age-verification-technologies,
https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification,
https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation.

Die offizielle Formel „*privacy-preserving*“ beschreibt dabei vor allem die Präsentationsschicht. Der anfragende Dienst soll möglichst wenig sehen, typischerweise nur ein Attribut wie „*über einem Schwellenwert*“. Der Eintritt in dieses System erfolgt jedoch nicht aus reiner Anonymität, sondern über starke Nachweisquellen wie eID, Pass, ID-Karte, Banking-App oder persönliche Vorsprache.[3]

3. Warum VPNs nun in den Fokus geraten

Der kritische politische Bruch liegt im neuen Framing. Die Kommissions-FAQ nennt VPNs ausdrücklich als technische Umgehungsmöglichkeit für Alterskontrollen. Die einschlägige EPRS-Hintergrundnotiz beschreibt VPNs als „***loophole***“ und referiert Forderungen, den Zugang zu VPNs auf Erwachsene zu beschränken. Damit wird ein neutrales Schutzwerkzeug erstmals auf EU-Ebene semantisch in die Nähe eines regulatorischen Störobjekts gerückt.[4]

Diese Sprachverschiebung fällt in ein politisches Umfeld, das unionsweit strengere und harmonisierte Altersregime diskutiert. Die Jutland-Erklärung und die Kommunikation der Kommission zum Minderjährigenschutz zeigen einen deutlichen Druck in Richtung einer breiteren, unionsweit kohärenten Altersverifikationspraxis. Genau in einem solchen Umfeld entsteht Mission Creep: Was zunächst für Pornografie oder ähnliche Erwachseneinhalte gebaut wird, kann als nächstes gegen Social Media, Kommunikationsdienste und schließlich gegen technische Umgehungs- oder Schutzwerkzeuge in Stellung gebracht werden.[5]

Der wahrscheinlichste Umsetzungsweg ist nicht das offene Verbot, sondern die Kette aus App-Store-Governance, offiziellen App-Whitelists, Trusted-Listen, Wallet-Abhängigkeiten, Standard-APIs und Intermediärdruck. Die Kommission sagt selbst, dass sie mit App-Stores zusammenarbeiten will, damit nur offizielle Altersverifikations-Apps, als echt kenntlich gemacht und Imitate entfernt werden. Diese Logik kann später ohne großen normativen Lärm ausgeweitet werden.[6]

---

3 **Europäische Kommission**, “*Commission sets out a common approach for EU-wide Age Verification technologies*”, 29. April 2026: https://digital-strategy.ec.europa.eu/en/library/commission-sets-out-common-approach-eu-wide-age-verification-technologies
Europäische Kommission, „*The EU approach to age verification*“, 29.04.2026, zu: ***EU Age Verification Scheme***, ***Trusted Proof-of-Age Providers List*** und ***Trusted Age Verification Solutions List***: https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification ; FAQ der Kommission vom 29.04.2026, Abschnitt „*How does the EU age verification app work?*“, zur Initialzertifizierung über biometrischen Pass oder Ausweis, nationale eID, Banking-App oder persönliche Vorsprache: https://digital-strategy.ec.europa.eu/en/faqs/eu-age-verification-solution.

4 Zur derzeit fehlenden expliziten EU-Norm für gewöhnliche VPN-Nutzung und zum neuen Framing als Umgehungskanal vgl. Europäische Kommission, EU Age Verification Solution, FAQ vom 29. April 2026, Abschnitt „***Can the age verification app be bypassed***?“, wonach eine Umgehung etwa durch die Nutzung eines VPN technisch möglich sein kann: https://digital-strategy.ec.europa.eu/en/faqs/eu-age-verification-solution ; sowie EPRS, „*Virtual private networks and the protection of children online*“, 20 January 2026, wonach manche Stimmen verlangen, den Zugang zu VPN-Diensten auf Nutzer oberhalb einer digitalen Volljährigkeit zu beschränken. Die EPRS-Notiz ist eine Hintergrundnotiz und keine offizielle Position des Parlaments, https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA%282026%29782618.

5 Zur politischen Eskalationsrichtung im Minderjährigenschutz vgl. „*The Jutland Declaration: Shaping a Safe Online World for Minors*“, Oktober 2025: https://www.digmin.dk/Media/638956829775203140/DIGMIN_The%20Jutland%20Declaration%20Shaping%20a%20Safe%20Online%20World%20for%20Minors%20101025.pdf ; zur unionsweiten Aktionslinie ferner **Europäische Kommission**, „*Action plan against cyberbullying – protecting children online*“, https://digital-strategy.ec.europa.eu/en/policies/cyberbullying. Gerade deshalb ist es zentral, die Grenze zwischen Inhaltsregulierung und Werkzeug-Permissionierung offenzuhalten.

6 Die **Kommission** erklärt in ihrer FAQ ausdrücklich, sie werde mit Apple, Google und anderen App-Stores zusammenarbeiten, um nur offizielle Versionen der Altersverifikations-App auf die Whitelist zu setzen und Imitate zu

4. Technische Realität der VPN-Nutzung

VPNs sind für normale Nutzer kein Randwerkzeug für dubiose Zwecke, sondern ein alltägliches Sicherheitsmittel. Sie schützen in fremden Netzen, reduzieren ISP- und Werbeprofiling, erschweren triviale Korrelation, helfen auf Reisen und sichern Kommunikation für Journalisten, Forscher, Geschäftsreisende, Hinweisgeber und gewöhnliche sicherheitsbewusste Nutzer. Große empirische Untersuchungen nennen je nach Sample ca. 82 % bis 92 % Schutz- und Sicherheitsmotive.[7]

Eine identitätsgebundene Onboarding- oder Zugangspflicht kehrt dieses Schutzprofil um. Sobald Attestationen, Tokens oder Wallet-Nachweise mit einem VPN-Dienst verknüpft werden, entsteht eine neue Identity-to-Service-Mapping-Schicht. Das erhöht das Risiko von Breaches, Insider-Missbrauch, compelled disclosure und nachträglicher Korrelation. Genau deshalb insistiert der Europäische Datenschutzausschuss darauf, dass Altersabsicherung die am wenigsten intrusive wirksame Methode sein und keine zusätzlichen Mittel schaffen darf, Personen zu identifizieren, zu lokalisieren, zu profilieren oder zu verfolgen.[8]

Hinzu kommt das Problem der Ineffizienz. Ein hartes Identitätsregime träfe primär regeltreue europäische Anbieter und gewöhnliche Nutzer. Ernsthaft motivierte Ausweicher würden auf Self-Hosting, ausländische Anbieter, Tor oder kundenspezifische Tunnel ausweichen. Das Ergebnis wäre daher nicht Risikominderung, sondern Risikoverlagerung bei gleichzeitiger Schwächung normaler digitaler Selbstverteidigung.[9]

5. Rechtliche und verfassungsrechtliche Anker

Der härteste unionsrechtliche Anker liegt gegen generalisierte Retentions-, Logging- und Traceability-Regime. Nach der Rechtsprechung des Gerichtshofs der Europäischen Union sind allgemeine und unterschiedslose Verkehrs- und Standortdateneingriffe mit der Grundrechtecharta regelmäßig nicht vereinbar. Für eine pauschale Personalisierung gewöhnlicher VPN-Nutzung wäre diese Linie höchst problematisch.[10]

Daneben greifen die Grundrechte auf Privatheit, Datenschutz, Kommunikationsvertraulichkeit und Informationsfreiheit. Art. 7, 8, 11 und 52 der Charta zwingen zu Datenminimierung, Verhältnismäßigkeit und strikter Erforderlichkeit. Auch der EGMR verlangt für Zugriffe auf

---

markieren oder zu entfernen. Das zeigt, dass App-Stores und offizielle Listen als regulatorische Hebel bereits ausdrücklich mitgedacht werden. Vgl. FAQ der Kommission vom 29. April 2026, Abschnitt "*How do I know if an app is an official version or a scam?*": https://digital-strategy.ec.europa.eu/en/faqs/eu-age-verification-solution.

7 Ramesh et al., „*All of them claim to be the best*": Multi-perspective study of VPN users and VPN providers, USENIX Security 2023, wonach ca. 92 Prozent der befragten Nutzer VPNs zur Sicherung oder zum Schutz ihrer Online-Aktivitäten einsetzen: https://www.usenix.org/system/files/sec23summer_147-ramesh-prepub.pdf.

8 Vgl. **European Data Protection Board**, „*Statement on age assurance*", angenommen im Februar 2025. Der EDPB betont den least intrusive approach und warnt davor, durch Altersabsicherung zusätzliche Mittel zur Identifikation, Lokalisierung, Profilierung oder Verfolgung natürlicher Personen zu schaffen. https://www.edpb.europa.eu/news/news/2025/edpb-adopts-statement-age-assurance-creates-task-force-ai-enforcement-and-gives_en.

9 Vgl. erneut Ramesh et al., USENIX Security 2023. Die Untersuchung der Anbieter- und Nutzerseite zeigt, dass alternative Setups und Ausweichpfade technisch offenbleiben; ein hartes Identitätsregime belastet daher primär regeltreue Anbieter und gewöhnliche Nutzer. https://www.usenix.org/system/files/sec23summer_147-ramesh-prepub.pdf.

10 Vgl. EuGH, Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u. a., verb. Rs. C-293/12 und C-594/12, ECLI:EU:C:2014:238; EuGH, Urteil vom 21. Dezember 2016, Tele2 Sverige AB und Watson u. a., verb. Rs. C-203/15 und C-698/15, ECLI:EU:C:2016:970; EuGH, Urteil vom 6. Oktober 2020, Privacy International, Rs. C-623/17, ECLI:EU:C:2020:790; EuGH, Urteil vom 6. Oktober 2020, La Quadrature du Net u. a., verb. Rs. C-511/18, C-512/18 und C-520/18, ECLI:EU:C:2020:791. Diese Linie bildet den stärksten unionsrechtlichen Anker gegen allgemeine und unterschiedslose Kommunikations- und Identitätsdateneingriffe.

Teilnehmerinformationen und Kommunikationsdaten klare gesetzliche Grundlagen sowie starke Schutzvorkehrungen; zugleich anerkennt seine Rechtsprechung die abschreckende Wirkung von Überwachungsregimen auf Recherche, Kommunikation und freie Rede.[11]

Nicht jede Form eines eng begrenzten, nicht verlinkbaren Altersattributs wäre automatisch rechtswidrig. Deutlich angreifbarer wird es aber dort, wo aus einem funktionsbezogenen Nachweis ein personengebundener Erlaubnisvorgang für ein legales Alltagswerkzeug wird. Genau diese Schwelle darf bei VPNs nicht überschritten werden.[12]

6. Verdichtete Risikomatrix

Szenario	Mechanismus	Evidenzstufe	Bewertung
Direkte Alters- oder ID-Pflicht für gewöhnliche VPN-Dienste	VPNs werden als Umgehungslücke selbst in Altersregime einbezogen	2	Rechtlich hochproblematisch; politisch derzeit noch nicht offen ausgesprochen
Indirekte Normalisierung über Scheme, Wallet und Trusted-Listen	Nur noch scheme-konforme Nachweise, offizielle Apps oder vertrauenslistengestützte Provider gelten als akzeptabel	2	Institutionell sehr plausibel; nach aussen als Interoperabilität und Sicherheit verkleidbar
Gatekeeping über App-Stores, Betriebssysteme und Browser	Distribution, Kennzeichnung und technische Schnittstellen werden als Vollzugshebel genutzt	2 bis 3	Hohe praktische Wirksamkeit ohne offenes Verbot
Spillover über Zahlungen, Hosting oder KYC-nahe Infrastrukturen	Kommerzielle und infrastrukturelle Druckpunkte werden nachgelagert genutzt	4	Strategisch relevant, derzeit aber schwächer belegt

Erläuterung der Evidenzstufen:

Die in dieser Matrix verwendeten Evidenzstufen bezeichnen nicht die politische Brisanz eines Szenarios, sondern den Grad seiner gegenwärtigen quellenmäßigen Absicherung.

---

11 Vgl. **Charta der Grundrechte der Europäischen Union**, insbesondere Art. 7, 8, 11 und 52, sowie **EGMR**, Benedik v. Slovenia, Nr. 62357/14, Urteil vom 24. April 2018, HUDOC 001-182455, und **EGMR**, Big Brother Watch and Others v. the United Kingdom [GK], Nrn. 58170/13, 62322/14 und 24960/15, Urteil vom 25. Mai 2021, HUDOC 001-210077. Diese Rechtsprechung unterstreicht gesetzliche Grundlage, Schutzvorkehrungen und chilling effects.

12 Zur Unterscheidung zwischen eng funktionsbezogenen, nicht verlinkbaren Attributnachweisen und einer allgemeinen personengebundenen Zugangsschicht vgl. den least-intrusive-Ansatz des **EDPB** sowie die offizielle Architektur der **Kommission** zur EU Age Verification Solution. Gerade die Übertragung eines eng umrissenen Nachweises auf ein allgemeines Sicherheitswerkzeug ist der kritische Kipppunkt. https://www.edpb.europa.eu/news/news/2025/edpb-adopts-statement-age-assurance-creates-task-force-ai-enforcement-and-gives_en, https://digital-strategy.ec.europa.eu/en/faqs/eu-age-verification-solution.

- **Evidenzstufe 1** steht für verifizierte Tatsachen, die sich unmittelbar aus geltenden Rechtsakten, offiziellen Dokumenten, technischen Spezifikationen oder eindeutigen institutionellen Aussagen ergeben.
- **Evidenzstufe 2** bezeichnet starke Indikationen, bei denen offizielle Materialien, Governance-Bausteine oder dokumentierte politische Signale bereits klar in eine bestimmte Richtung weisen, ohne dass die Endstufe schon ausdrücklich normiert wäre.
- **Evidenzstufe 3** meint plausible Inferenz: ein Risiko oder Entwicklungspfad, der sich aus der Kombination bestehender Bausteine, Vollzugslogiken und institutioneller Anreize nachvollziehbar ableiten lässt, aber noch nicht unmittelbar als offizielles Vorhaben belegt ist.
- **Evidenzstufe 4** schließlich bezeichnet ein spekulatives, jedoch strategisch relevantes Folgerisiko, das im aktuellen Aktenstand noch schwach belegt ist und deshalb nicht als gegenwärtige Tatsache, sondern nur als mögliche spätere Eskalation verstanden werden darf.

Die Matrix trennt damit bewusst zwischen gesicherter Lage, glaubhafter Entwicklungstendenz und weiterreichender Projektion. Das wahrscheinlichste Risiko ist nicht die plakatierte Totalmaßnahme, sondern die graduelle Normalisierung über Governance, Standards, Soft Law, App-Distribution und Intermediärdruck.

Gerade deshalb muss der Widerspruch früh ansetzen und sich gegen die Infrastruktur der späteren Eskalation richten, nicht erst gegen ihren letzten, formalisierten Schritt.

7. Regulatorische Folgerungen

1. Braucht es eine ausdrückliche Klarstellung, dass gewöhnliche VPN-Dienste und andere legale Privatsphäre- und Sicherheitswerkzeuge nicht in unionsweite Altersverifikations- oder Wallet-Regime hineingezogen werden dürfen.
2. Müssen App-Stores, Betriebssysteme, Browser, Zahlungsdienstleister, Hosting-Anbieter und vergleichbare Intermediäre von einer faktischen Verifikations- oder Trusted-List-Durchsetzung ferngehalten werden.
3. Sind Logging-, Audit- oder Retentionsarchitekturen abzulehnen, die Identität und VPN-Nutzung strukturell zusammenführen.
4. Muss gegen konkret rechtswidrige Inhalte oder Handlungen zielgerichtet, funktionsspezifisch und verhältnismäßig vorgegangen werden, statt ein legales Schutzwerkzeug insgesamt zu permissionieren.[13]

8. Fazit

Die belastbarste öffentliche Kurzform lautet daher: Noch existiert keine allgemeine EU-Norm für eine VPN-Ausweispflicht. Aber die EU errichtet eine Alters- und Attributinfrastruktur, rahmt VPNs offen als Umgehungskanal und schafft damit die institutionellen Voraussetzungen für eine spätere indirekte Identitätsbindung gewöhnlicher VPN-Nutzung. Genau gegen diese Eskalationsbahn richtet sich der Appell.

---

[13] Zu diesen regulatorischen Folgerungen stützen insbesondere der EDPB-Ansatz der Datenminimierung, die DSA-Leitlinien zum Schutz Minderjähriger, die Kommissionsmaterialien zum EU Age Verification Scheme sowie die einschlägige EuGH-Rechtsprechung gegen generalisierte Eingriffe. Sie tragen eine präventive Klarstellung gegen spätere Repurposing- oder Mission-Creep-Schritte, ohne bereits bestehende Verbotsnormen zu behaupten.