Öffentlicher Appell gegen die indirekte Identitätsbindung gewöhnlicher VPN-Nutzung in der Europäischen Union

An die *Europäische Kommission*,[1] das *Europäische Parlament*,[2] den *Rat der Europäischen Union*,[3] das *European Board for Digital Services*,[4] die nationalen *Digital Services Coordinators*,[5] das *European Data Protection Board*,[6] und die zuständigen nationalen Datenschutzaufsichtsbehörden[7].

Virtuelle private Netzwerke sind kein Erwachseneninhalt, kein Glücksspieldienst und kein amtliches Verfahren. Sie sind legale Sicherheits- und Privatsphäre Werkzeuge. Für die gewöhnliche Nutzung solcher Werkzeuge, insbesondere für den Schutz der Verbindung in fremden Netzen, gegen ISP-Profiling, gegen triviale Korrelation und für sicheren Zugriff auf Informationen, muss anonyme Nutzung als Regelfall offenbleiben. Empirische Forschung zeigt, dass VPNs ganz überwiegend zu Schutz- und Sicherheitszwecken eingesetzt werden, nicht als Randwerkzeug für Missbrauch.[8]

Heute existiert in der Europäischen Union noch keine allgemeine Rechtsnorm, die gewöhnliche VPN-Nutzung als solche einer Alters- oder Identitätsprüfung unterstellt. Genau darin liegt aber die Gefahr nicht mehr allein. Auf EU-Ebene ist nun erstmals ausdrücklich sichtbar, dass VPNs als „***loophole***“ im Kontext von Altersverifikationsregimen gerahmt werden. Die Kommission erklärt in ihrer eigenen FAQ, dass Altersverifikation technisch etwa durch die Nutzung eines VPN umgangen werden kann; eine EPRS-Hintergrundnotiz hält fest, dass manche Stimmen deshalb eine Beschränkung des Zugangs zu VPN-Diensten auf Personen oberhalb einer digitalen Volljährigkeit fordern.[9]

Parallel dazu errichtet die Kommission eine unionsweite Alters- und Attributinfrastruktur mit EU:

- Age Verification Scheme
- Trusted-Provider-Listen
- Trusted-Solution-Listen

---

1 **Europäische Kommission**: Offizielle Übersichtsseite: https://commission.europa.eu/index_en.

2 **Europäische Parlament**: Offizielle Übersichtsseite: https://www.europarl.europa.eu/portal/de/contact.

3 **Rat der Europäischen Union**: Offizielle Übersichtsseite: https://www.consilium.europa.eu/en/council-eu/.

4 **European Board for Digital Services**: Das Europäische Gremium für digitale Dienste ist das im DSA eingerichtete Kooperations- und Beratungsgremium. Es setzt sich aus den nationalen Digital Services Coordinators zusammen und wird von der Europäischen Kommission geleitet. Offizielle Seite: https://digital-strategy.ec.europa.eu/en/policies/dsa-board.

5 **Digital Services Coordinators**: Die nationalen Digital Services Coordinators sind die je Mitgliedstaat benannten Behörden für Anwendung, Überwachung und Durchsetzung des DSA. Offizielle Übersichtsseite: https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs.

6 **European Data Protection Board**: Offizielle Übersichtsseite: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en.

7 Ebd.

8 Zur Schutzfunktion von VPNs und ihrer typischen Nutzung vgl. European Parliamentary Research Service: „*Virtual private networks and the protection of children online*“, 20 January 2026, https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA%282026%29782618 ; ferner 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.

9 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, siehe Fn. 8.

- offizieller App-Verteilung und
- enger technischer Anlehnung an die künftigen EU Digital Identity Wallets.

Offiziell heißt das euphemistisch „***privacy-preserving***". Der Einstieg in diese Architektur erfolgt jedoch gerade nicht aus reiner Anonymität, sondern über starke Nachweisquellen wie biometrischen Pass oder Ausweis, nationale eID, Banking-App oder persönliche Vorsprache.[10]

Wer gewöhnliche VPN-Nutzung in eine solche Kette hineinzieht, verschiebt die Architektur von einem neutralen Schutzwerkzeug zu einem personengebundenen Erlaubnisvorgang. Aus datensparsamer Verbindungssicherung wird eine neue Korrelationsschicht; aus Schutz vor Profilbildung wird ein neues Mapping zwischen Identität und Privatsphäre Werkzeug. Genau vor dieser Logik warnt der Europäische Datenschutzausschuss, wenn er verlangt, dass Altersabsicherung die am wenigsten intrusive wirksame Maßnahme sein und keine zusätzlichen Mittel schaffen darf, natürliche Personen zu identifizieren, zu lokalisieren, zu profilieren oder zu verfolgen.[11]

Wir verlangen deshalb einen engen, aber klaren Minimalstandard:

(1) Darf die gewöhnliche, legale Nutzung von VPN-Diensten weder direkt noch indirekt von staatlich anschlussfähiger Alters- oder Identitätsverifikation abhängig gemacht werden. Was bei eng umrissenen Erwachsenenangeboten diskutiert wird, darf nicht auf allgemeine Sicherheits- und Privatsphäre Werkzeuge übergreifen.[12]

(2) Dürfen gewöhnliche VPN-Dienste nicht als „*adult-only*"-Dienst, allgemeines Umgehungswerkzeug oder regulatorisches Störobjekt umdefiniert werden. Der Umstand, dass ein legales Werkzeug missbraucht werden kann, rechtfertigt nicht seine personengebundene Permissionierung.[13]

(3) Dürfen App-Stores, Betriebssysteme, Browser, Zahlungsdienstleister, Hosting-Anbieter oder andere Intermediäre nicht faktisch dazu gedrängt werden, den Zugang zu VPN-Diensten nur noch über Trusted-Lists, offizielle App-Whitelists, Wallet-Abhängigkeiten oder gleichwertige Verifikationsketten zu öffnen.[14]

---

10 **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.

11 **European Data Protection Board**, *Statement on age assurance*, 11 February 2025, angenommen am 12 February 2025. Der EDPB betont unter anderem, dass die am wenigsten intrusive wirksame Methode zu wählen ist und dass Altersabsicherung keine zusätzlichen Mittel schaffen darf, Personen zu identifizieren, zu lokalisieren, zu profilieren oder zu verfolgen: https://www.edpb.europa.eu/news/news/2025/edpb-adopts-statement-age-assurance-creates-task-force-ai-enforcement-and-gives_en.

12 Zur derzeitigen Zielrichtung der unionsweiten Altersverifikation auf altersbeschränkte Inhalte und Dienste, nicht auf allgemeine Sicherheitstools, vgl. **Europäische Kommission**, „*The EU approach to age verification*", 29 April 2026; ferner „*Commission publishes guidelines on the protection of minors*", 14 July 2025, zu „*proportionate and appropriate measures*" nach Art. 28 DSA: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors.

13 Das **EPRS**-Dokument beschreibt VPNs einerseits als Mittel für sichere und verschlüsselte Verbindungen, Tracking-Schutz und Zugang zu blockierten Informationen, andererseits aber als Umgehungskanal für Alterskontrollen; genau diese begriffliche Verschiebung ist der kritische Punkt. Vgl. **EPRS**, "*Virtual private networks and the protection of children online*", 20 January 2026: https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA%282026%29782618.

14 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 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.

(4) Müssen Altersverifikations- und Digital-Identity-Schemes technisch und rechtlich von legalen Privatsphäre- und Sicherheitswerkzeugen getrennt bleiben. Was zur Absicherung bestimmter altersbeschränkter Inhalte geschaffen wurde, darf nicht in eine generische Zugangsschicht für alltägliche Infrastruktur umschlagen.[15]

(5) Dürfen Identitätsdaten, Attestationen, Token oder daraus abgeleitete Personenanker nicht mit der Nutzung gewöhnlicher VPN-Dienste verknüpft, auf Vorrat gespeichert oder in Logging-, Audit- oder Retentionsregime überführt werden, die faktisch eine rückführbare Identitätsbindung erzeugen.[16]

(6) Müssen jede ausnahmsweise, eng zielgerichtete Maßnahme gegen konkret bestimmte rechtswidrige Handlungen oder Dienste spezifisch, verhältnismäßig, richterlich und gesetzlich kontrollierbar und technisch datensparsam sein. Blanket-artige Zugangsgates für alle Nutzer sind mit europäischem Datenschutz- und Grundrechtsdenken unvereinbar.[17]

(7) Müssen Kommission, Parlament, Rat, Aufsichtsbehörden und Koordinatoren ausdrücklich klarstellen, dass unionsweite Altersverifikations- und Wallet-Infrastrukturen nicht gegen gewöhnliche VPN-Nutzung repurposed werden dürfen, weder offen durch Gesetz noch verdeckt durch Vollzug, Soft Law, Zertifizierung, App-Store-Governance oder Intermediärhaftung.[18]

Die Berufung auf „*Kinderschutz*“, „*Missbrauchsabwehr*“ und „*Plattformintegrität*“ ersetzt in diesem Kontext keine belastbare Rechtfertigung. Sie fungiert vielmehr als politische Legitimationsformel für den Ausbau personengebundener Zugangskontrollen. Ein legales Schutzwerkzeug, das der Sicherung von Kommunikation, Recherche, Reisen, geschäftlicher Vertraulichkeit und alltäglicher digitaler Selbstverteidigung dient, darf nicht in eine erlaubnispflichtige Ausnahme überführt werden. Wer VPNs zur bloßen „*Lücke*“ erklärt, verschiebt den Regulierungsansatz vom Umgang mit einzelnen Inhalten hin zur Kontrolle des Schutzmittels selbst.[19]

---

15 Die **Kommission** beschreibt die Altersverifikationslösung als eigenständige App oder als in nationale EU Digital Identity Wallets integrierbare Lösung; gleichzeitig verlangt die **European Digital Identity Regulation**, dass die Mitgliedstaaten bis Ende 2026 mindestens eine Wallet anbieten. Vgl. **Europäische Kommission**, “*Commission urges Member States to rollout EU age verification app*”, 29 April 2026: https://digital-strategy.ec.europa.eu/en/news/commission-urges-member-states-rollout-eu-age-verification-app ; sowie „*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.

16 Zu den harten unionsrechtlichen Ankern gegen allgemeine, unterschiedslose Retentions- und Traceability-Regime vgl. **EuGH**, Digital Rights Ireland, Urteil vom 8. April 2014, Pressemitteilung Nr. 54/14: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf ; **EuGH**, Tele2 Sverige und Watson, Urteil vom 21. Dezember 2016, Pressemitteilung Nr. 145/16: https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf ; ferner **EuGH**, Privacy International, Urteil vom 6. Oktober 2020, Pressemitteilung Nr. 123/20: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf.

17 Relevante Rechtsanker sind insbesondere Art. 7, 8, 11 und 52 der Charta der Grundrechte der Europäischen Union sowie die datenschutzrechtliche Logik der Datenminimierung und Verhältnismäßigkeit. Offizieller Text der Charta: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT ; zum least-intrusive-Ansatz zusätzlich der **EDPB**, „*Statement on age assurance*“, 11 February 2025, https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf.

18 Gerade weil DSA-Leitlinien formal nicht selbst Gesetz sind, in der Vollzugspraxis aber als Referenzpunkt dienen können, ist eine ausdrückliche Klarstellung nötig. Vgl. **Europäische Kommission**, “*Guidelines under the Digital Services Act*”, https://digital-strategy.ec.europa.eu/en/policies/dsa-guidelines.

19 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.

Wir fordern die genannten Stellen deshalb auf, diesen Minimalstandard ausdrücklich anzuerkennen, regulatorisch abzusichern und in allen einschlägigen Leitlinien, Empfehlungen, Schemata, Listen- und Zertifizierungsarchitekturen sowie künftigen Gesetzgebungsvorhaben sichtbar umzusetzen. Gewöhnliche VPN-Nutzung darf in Europa weder direkt noch indirekt in eine identitätsgebundene Ausnahme verwandelt werden.[20]

[20] Die hier verlangte Klarstellung ist präventiv: Sie behauptet kein bereits beschlossenes VPN-ID-Gesetz, sondern wendet sich gegen die institutionell sichtbare Möglichkeit einer späteren Einbeziehung gewöhnlicher VPN-Dienste in Altersverifikations-, Wallet-, Trusted-List- oder Intermediärketten. Genau diese präzise Warnung ist nach heutigem Aktenstand belastbarer als jede grobe Verbotsbehauptung.