BRIEFING-DOKUMENT

Die geplante EU-Chatkontrolle: Stand, Einordnung und Handlungsoptionen

Erstellt für: **WerteUnion – Bundesvorstand** | Stand: **13. Juli 2026** | Themenfeld: **Digitalpolitik / Grundrechte**

1. Executive Summary

- Die EU verhandelt zwei getrennte, aber oft vermischte Vorhaben: die „Chatkontrolle 1.0“ (freiwilliges Scannen unverschlüsselter Inhalte, seit 2021) und die „Chatkontrolle 2.0“ (dauerhafte CSA-Verordnung mit möglicher Pflicht zum Client-Side-Scanning verschlüsselter Kommunikation).
- Die freiwillige Regelung (1.0) lief am 3. April 2026 aus, wurde aber am 9. Juli 2026 über ein Eilverfahren des EU-Parlaments verfahrensrechtlich reaktiviert – gegen eine relative, aber nicht absolute Mehrheit der Abgeordneten.
- Die verpflichtende Chatkontrolle 2.0 mit Client-Side-Scanning gilt aktuell als politisch eher unwahrscheinlich: Der Ratsstand vom 26.11.2025 enthält keine verpflichtenden Aufdeckungsanordnungen für Ende-zu-Ende-verschlüsselte Dienste.
- Die Trilog-Verhandlungen zur dauerhaften Verordnung sind für die Sommerpause ausgesetzt; nächster politischer Trilog: 29. September 2026.
- **Zentrales Risiko:** nicht die offene Verabschiedung einer Scan-Pflicht, sondern die schrittweise Wiederbelebung ausgelaufener Ausnahmeregeln über Verfahrenstricks, ohne breite demokratische Legitimation.
- **Deutsche Position uneinheitlich:** BMJ (SPD) lehnt anlasslose Kontrolle klar ab, BMI drängte hingegen auf schnelle Wiederherstellung der freiwilligen Regelung; die deutsche Ratsdelegation zeigt sich gegenüber einer „ergänzenden“ Pflicht-Chatkontrolle offen.

2. Ausgangslage: Zwei Vorhaben, ein Streit

2.1 Chatkontrolle 1.0 – freiwillige Interims-Verordnung

Seit 2021 erlaubt eine Ausnahme von der ePrivacy-Richtlinie Anbietern wie Meta, Google, Microsoft oder Apple, automatisiert und freiwillig nach Missbrauchsdarstellungen in unverschlüsselten, online gespeicherten Inhalten zu suchen und diese über das NCMEC (National Center for Missing & Exploited Children, USA) an europäische Behörden zu melden. Diese Regelung wurde bereits einmal verlängert.

Eine zweite Verlängerung scheiterte am 17. März 2026 in den Trilog-Verhandlungen. Am 26. März 2026 stimmte das EP mit 228 zu 311 Stimmen final gegen die Verlängerung; am 3. April 2026 lief die Rechtsgrundlage aus. Damit war die Ausnahmeregelung tot – bis zum Verfahrenstrick am 7./9. Juli 2026 (siehe Zeitleiste).

2.2 Chatkontrolle 2.0 – dauerhafte CSA-Verordnung

Seit Mai 2022 verhandelt die EU über eine dauerhafte Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSA-VO). Kernstreitpunkt ist die Frage, ob und wie Anbieter zum Scannen von Inhalten verpflichtet werden können – im Zweifel auch von Ende-zu-Ende-verschlüsselter Kommunikation über sogenanntes Client-Side-Scanning, das die Verschlüsselung technisch vor der Übertragung umgeht.

Die drei EU-Institutionen vertreten seit Jahren diametral entgegengesetzte Positionen (siehe Tabelle in Abschnitt 4). Nach dem 5. Trilog am 11. Mai 2026 besteht weiterhin keine Einigung, insbesondere bei der Frage verpflichtender Aufdeckungsanordnungen. Die Verhandlungen sind aktuell für die Sommerpause ausgesetzt.

3. Chronologie der wichtigsten Ereignisse 2026

Datum	Ereignis
17.03.2026	Trilog-Verhandlungen zur 2. Verlängerung der freiwilligen Chatkontrolle (1.0) scheitern.
26.03.2026	EP lehnt Verlängerung der Übergangsregelung mit 228:311 Stimmen ab.
03.04.2026	Rechtsgrundlage für freiwilliges Scannen läuft aus – Regelungslücke entsteht.
11.05.2026	5. Trilog zur dauerhaften CSA-Verordnung ("2.0") – keine Einigung, insb. bei Aufdeckungspflichten.
05.06.2026	Datenschutzkonferenz fordert EU-Gesetzgeber zur endgültigen Absage an die Chatkontrolle auf.
17.06.2026	Rat bringt neue vorübergehende Ausnahme von der ePrivacy-Richtlinie auf den Weg ("Zombie"-Wiederbelebung).
01.07.2026	AStV-2: Vorbereitung der Ratsposition zur Wiedereinführung der Interims-VO; EU-Ratspräsidentschaft wechselt von Zypern zu Irland.
07.07.2026	EP stimmt mit 331:304 für Eilverfahren zur Neuabstimmung über die freiwillige Chatkontrolle.
09.07.2026	EP verfehlt mit 314 Gegenstimmen die nötige absolute Mehrheit (360) – Verlängerung kommt indirekt durch.
29.09.2026	Nächster politischer Trilog zur dauerhaften CSA-Verordnung angesetzt (nach Sommerpause).

Hinweis: Die Verhandlungen sind im laufenden Trilog-Prozess dynamisch; kurzfristige Änderungen sind jederzeit möglich.

4. Positionen der zentralen Akteure

Akteur	Position
EU-Kommission	Verpflichtendes Scannen aller Nutzerinhalte durch Hoster/Kommunikationsdienste (ursprünglicher Entwurf 2022).
Rat der EU-Mitgliedstaaten	Keine Verpflichtung; nur freiwilliges Scannen. Ratsposition v. 26.11.2025 ohne verpflichtende Aufdeckungsanordnungen.
Europäisches Parlament	Gegen anlasslose Massenüberwachung; falls überhaupt, nur verpflichtendes Scannen verdächtiger Nutzer als letztes Mittel.
Bundesregierung (BMJ / SPD)	Anlasslose Chatkontrolle "muss in einem Rechtsstaat tabu sein" (Justizministerin Hubig).
Bundesregierung (BMI)	Drängte auf schnellstmögliche Wiederherstellung der freiwilligen Regelung (1.0); bei 2.0 keine grundsätzliche Ablehnung, sofern "ergänzend" zu freiwilligen Maßnahmen.
Deutsche Delegation im Rat	Laut Verhandlungsdokumenten nicht gegen verpflichtende Chatkontrolle, sofern ergänzend zu freiwilligem Scannen.
Italien, Polen, Österreich	Ablehnend gegenüber jeder Form der Chatkontrolle durch Internetanbieter.
Juristischer Dienst des Rates	Anlasslose Chatkontrolle wird als rechtswidrig eingestuft; Verstoß gegen EuGH-Rechtsprechung zu genereller Überwachung.

Akteur	Position
Datenschutzkonferenz (DSK)	Fordert vollständigen Verzicht auf anlasslose Massenüberwachung und endgültige Absage.
Anbieter (Signal u.a.)	Ankündigung, EU-Markt eher zu verlassen als Verschlüsselung zu schwächen.

5. Auswirkungen auf nationale Gesetzgebung

- **Unmittelbare Geltung:** Als EU-Verordnung (nicht Richtlinie) würde die CSA-VO ohne nationales Umsetzungsgesetz unmittelbar in allen Mitgliedstaaten gelten – der nationale Gesetzgeber hätte keinen eigenen Ausgestaltungsspielraum wie bei einer Richtlinie.
- **Verfassungsrechtliche Kollisionsgefahr:** Mehrere Stimmen halten den Vorschlag für unvereinbar mit EuGH-Rechtsprechung zu genereller und unterschiedsloser Überwachung sowie mit nationalen Grundrechten – in Deutschland konkret dem Fernmeldegeheimnis (Art. 10 GG) und dem „IT-Grundrecht“ des Bundesverfassungsgerichts (Vertraulichkeit und Integrität informationstechnischer Systeme).
- **Verdrängung bestehender Datenschutzregeln:** Die Ausnahmeregelung wirkt als Durchbrechung der ePrivacy-Richtlinie bzw. ihrer nationalen Umsetzung; eine dauerhafte CSA-VO würde diese Durchbrechung dauerhaft im EU-Recht verankern.
- **Blockademacht im Rat:** Die deutsche Stimme ist im Rat entscheidend für das Erreichen bzw. Verhindern einer qualifizierten Mehrheit bzw. Sperrminderheit – eine Zustimmung Deutschlands hätte unmittelbare Hebelwirkung auf den gesamten Trilog-Ausgang.
- **Institutioneller Widerstand:** Die Datenschutzkonferenz (Zusammenschluss der deutschen Datenschutzaufsichtsbehörden) sowie der juristische Dienst des Rates selbst positionieren sich gegen anlasslose Massenüberwachung – ein Novum, das Rechtsunsicherheit für eine spätere gerichtliche Überprüfung (EuGH, BVerfG) begründet.
- **Standort- und Wettbewerbsfolgen:** Eine Verpflichtung, die andere Demokratien (UK, USA) so nicht durchsetzen, würde den digitalen Binnenmarkt der EU im Bereich vertraulicher Kommunikation benachteiligen; datenschutzfreundliche Anbieter könnten ihren Sitz verlagern.

6. Auswirkungen auf die Bürger

6.1 Bei Fortbestand der freiwilligen Regelung (1.0)

- Unverschlüsselte Inhalte (Cloud-Fotos, unverschlüsselte E-Mails/Chats) können weiterhin automatisiert durchsucht werden.
- Ende-zu-Ende-verschlüsselte Messenger (Signal, Threema, WhatsApp-Inhalte) bleiben ausdrücklich ausgenommen.
- Praxis zeigt bereits heute Kontrollverlust: Große US-Plattformen scannen laut eigenen Angaben teils unabhängig von der EU-Rechtsgrundlage weiter; Microsoft kann Nutzer über Geräte-IDs verfolgen, ohne dass Betroffene dies bemerken.

6.2 Bei Durchsetzung der verpflichtenden Variante (2.0 mit Client-Side-Scanning)

- Grundsatzfrage für Millionen Nutzer verschlüsselter Messenger in Deutschland/DACH: Dürfen private Nachrichten künftig direkt auf dem Endgerät durchsucht werden, bevor sie verschlüsselt werden?

- IT-Sicherheitsexperten warnen vor einem strukturellen Sicherheitsrisiko: Jeder eingebaute Scan-Mechanismus schafft einen Kanal, der technisch erweiterbar und missbrauchbar ist („Function Creep“) – was heute nach Missbrauchsmaterial sucht, kann morgen auf andere Inhalte ausgeweitet werden.
- Anbieterreaktion: Signal hat angekündigt, den EU-Markt eher zu verlassen als seine Verschlüsselung zu schwächen – mit der Folge, dass Bürger Zugang zu etablierten, sicheren Diensten verlieren könnten.
- Fehlalarm-Problematik: BKA-Daten deuten darauf hin, dass automatisierte Filtersysteme eine hohe Zahl an Falschmeldungen produzieren, was Ermittlungsbehörden zusätzlich belastet, statt sie zu entlasten – ein Zielkonflikt zwischen behauptetem Kinderschutz-Nutzen und tatsächlicher Wirksamkeit.
- Gesellschaftlich: Kritiker sprechen von einem Einstieg in eine Überwachungsinfrastruktur, die die gesamte Bevölkerung anlasslos unter Generalverdacht stellt, während technisch versierte Täter ohnehin auf dezentrale Plattformen oder das Darknet ausweichen.

7. Bewertung und mögliche Positionierung der WerteUnion

Aus wertkonservativer, marktliberaler und rechtsstaatlicher Perspektive ergeben sich folgende Anknüpfungspunkte für eine Positionierung:

- **Rechtsstaatliche Grundlinie:** Anlasslose, flächendeckende Überwachung privater Kommunikation ist mit dem Prinzip der Verhältnismäßigkeit und dem Schutz der Privatsphäre schwer vereinbar – unabhängig vom legitimen Ziel des Kinderschutzes, das nicht in Frage steht.
- **Kinderschutz und Grundrechte sind kein Widerspruch:** Wirksamer Opferschutz sollte über gezielte, anlassbezogene Ermittlungsbefugnisse bei konkretem Tatverdacht erfolgen, nicht über pauschale Techniküberwachung aller Bürger.
- **Wirtschafts- und Standortargument:** Eine Schwächung von Verschlüsselung schadet dem digitalen Wirtschaftsstandort Deutschland/EU – auch für Unternehmen, die auf vertrauliche Kommunikation angewiesen sind (z. B. im industriellen, sicherheitsrelevanten oder Prüfwesen-Kontext).
- **Kritik an Verfahren, nicht nur am Inhalt:** Die Reaktivierung ausgelaufener Regelungen über Eilverfahren gegen den erklärten Mehrheitswillen des Parlaments ist demokratietheoretisch angreifbar und bietet Anknüpfungspunkte für eine Kritik an der Verfahrenskultur der EU-Institutionen.
- **Beobachtungsbedarf:** Die uneinheitliche Position der Bundesregierung (BMJ vs. BMI) sowie der Kurs der deutschen Ratsdelegation sollten politisch beobachtet und ggf. öffentlich adressiert werden.

8. Handlungsempfehlungen

- Beobachtung der Trilog-Verhandlungen bis zum nächsten politischen Trilog (29. September 2026) und frühzeitige Positionierung vor diesem Termin.
- Parlamentarische Initiativen (Anträge, Kleine Anfragen) zur Klärung der tatsächlichen Position der Bundesregierung im Rat prüfen.
- Vernetzung mit IT-Sicherheits- und Datenschutzexperten sowie Anbietern (z. B. Signal, Threema) für sachlich fundierte Stellungnahmen.
- Kommunikationslinie: Klare Trennung zwischen „Kinderschutz stärken“ (Zustimmung) und „anlasslose Massenüberwachung“ (Ablehnung), um Vereinnahmungsversuchen der Gegenseite vorzubeugen.
- Laufendes Monitoring der Position von BMJ, BMI und der deutschen Ständigen Vertretung (AStV) in Brüssel.

9. Quellenlage

Dieses Briefing basiert auf Berichterstattung von netzpolitik.org (inkl. veröffentlichter interner Verhandlungsdokumente), ZDFheute, heise online, Table.Briefings, wbs.legal, Bundestag.de sowie Presseerklärungen der Datenschutzkonferenz und der Berliner Beauftragten für Datenschutz und Informationsfreiheit. Da sich die Trilog-Verhandlungen im laufenden Prozess befinden, kann sich der Sachstand kurzfristig ändern; eine Aktualisierung vor dem 29. September 2026 wird empfohlen.