



Bundesministerium
der Justiz

WIR FEIERN
75 JAHRE
GRUNDGESETZ

POSTANSCHRIFT Bundesministerium der Justiz, 11015 Berlin

Einschreiben International

Herrn

c/o Universität Zürich

HAUSANSCHRIFT Mohrenstraße 37, 10117 Berlin
POSTANSCHRIFT 11015 Berlin

BEARBEITET VON
REFERAT
TEL
FAX
E-MAIL
AKTENZEICHEN

DATUM Berlin, 1. Oktober 2024

BETREFF: Informationsfreiheitsgesetz (IFG)
HIER: Stellungnahmen zu 2022/0155 „Combating child sexual abuse online“ - Chatkontrolle
BEZUG: Ihr IFG-Antrag vom 13. September 2024
ANLAGE: - 7 Dokumente -

Sehr geehrter

auf Ihren Antrag nach dem Informationsfreiheitsgesetz (IFG) auf Zugang zu amtlichen Informationen des Bundesministeriums der Justiz (BMJ) vom 13. September 2024 ergeht folgender

B e s c h e i d :

1. Ich gebe Ihrem Antrag statt.
2. Eine Gebühr wird nicht erhoben.

Begründung:

I.

LIEFERANSCHRIFT Kronenstraße 41, 10117 Berlin
VERKEHRSANBINDUNG U-Bahnhof Hausvogteiplatz (U2)

Mit E-Mail vom 13. September 2024 beantragen Sie unter Bezugnahme auf das IFG Zugang zu Unterlagen „zum EU-Regulierungsvorhaben 2022/0155 ‚Combating child sexual abuse online‘, welches medial auch unter dem Titel ‚Chatkontrolle‘ diskutiert“ werde.

Konkret fragen Sie bzw. bitten Sie um Folgendes:

„(1) Haben sich externe Stakeholder (z.B. Unternehmen, Verbände, NGOs, andere) an Ihr Haus mit Positionen, einer Stellungnahme oder ähnlichem gewandt?

(2) Sofern (1) zutrifft, möchte ich Sie gerne auch um die Übersendung der betroffenen Dokumente bitten, wie auch möglicherweise betroffener Kommunikation zu den Dokumenten / Stellungnahmen / Positionierungen.“

Mit der Schwärzung personenbezogener Daten (die Hausleitung ausgenommen) haben Sie sich einverstanden erklärt.

II.

Nach § 1 Absatz 1 Satz 1 IFG hat jeder nach Maßgabe des IFG gegenüber den Behörden des Bundes einen Anspruch auf Zugang zu amtlichen Informationen. Nach § 2 Nummer 1 Satz 1 IFG ist amtliche Information jede amtlichen Zwecken dienende Aufzeichnung, unabhängig von der Art ihrer Speicherung.

Zu Frage (1) teile ich Folgendes mit:

Es haben sich externe Stakeholder mit einer Stellungnahme oder ähnlichem zum EU-Regulierungsvorhaben 2022/0155 ‚Combating child sexual abuse online“- „Chatkontrolle“ an BMJ gewandt.

Zu (2) übersende ich Ihnen in der Anlage die erbetenen Informationen. Es handelt sich dabei um sieben Dokumente. Ggf. doppelt erfasste Dokumente werden nur einmal übersandt.

Personenbezogene Daten wurden unkenntlich gemacht.

Mit freundlichen Grüßen

Im Auftrag



Hinweis:

Das BMJ verarbeitet im Zusammenhang mit Ihrem Antrag nach dem IFG ausschließlich solche Daten, die notwendig sind, um mit Ihnen zu kommunizieren und um das Verwaltungshandeln des BMJ ordnungsgemäß zu dokumentieren. Hierzu gehören insbesondere personenbezogene Informationen, die Sie unmittelbar übermittelt haben. Die Verarbeitung der Daten ist zur Wahrnehmung der Aufgaben des BMJ erforderlich (vgl. Artikel 6 Absatz 1 Buchstabe e und Absatz 3 Buchstabe b der Datenschutz-Grundverordnung in Verbindung mit § 3 des Bundesdatenschutzgesetzes und dem IFG).

Weitere Informationen zur Verarbeitung von personenbezogenen Daten durch das BMJ finden Sie auf der Internetseite unter www.bmj.de. Hier finden Sie u. a. auch nähere Erläuterungen zu Ihren Rechten sowie weiterführende Kontakt- bzw. Beschwerdemöglichkeiten.



Deutscher**Anwalt**Verein

Stellungnahme

des Deutschen Anwaltvereins durch
den Ausschuss Gefahrenabwehrrecht

zum Vorschlag für eine Verordnung des
Europäischen Parlaments und des Rates zur
Festlegung von Vorschriften zur Prävention und
Bekämpfung des sexuellen Missbrauchs von
Kindern (COM(2022) 209 final)

Stellungnahme Nr.: 32/2023

Berlin, im Mai 2023

Mitglieder des Ausschusses

[REDACTED]

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Zuständig in der DAV-Geschäftsstelle

- [REDACTED]

Ansprechpartnerin in Brüssel:

- [REDACTED]

Verteiler

Europa

- Europäische Kommission
 - o Generaldirektion Migration und Inneres (HOME)
- Europäisches Parlament
 - o Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE)
 - o Ausschuss für die Rechte der Frauen und die Gleichstellung der Geschlechter (FEMM)
 - o Ausschuss Binnenmarkt und Verbraucher (IMCO)
- Rat der Europäischen Union
- Ständige Vertretung der Bundesrepublik Deutschland bei der EU
- Justizreferent:innen der Landesvertretungen
- Rat der Europäischen Anwaltschaften (CCBE)
- Bundesverband der Freien Berufe (BFB) Büro Brüssel

Deutschland

- Bundesverfassungsgericht
- An die Mitglieder des Rechtsausschusses des Deutschen Bundestages
- Ausschuss für Inneres und Heimat des Deutschen Bundestages
- Arbeitsgruppe Recht und Verbraucherschutz der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppe Inneres der im Deutschen Bundestag vertretenen Parteien
- Rechts- und Innenausschüsse der Landtage
- Bundesministerium der Justiz
- Bundesministerium des Innern und für Heimat
- An die Justizministerien und Justizverwaltungen der Bundesländer
- Bundesrechtsanwaltskammer
- Landesministerien und Senatsverwaltungen des Innern
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Deutscher Richterbund
- Bundesverband der Freien Berufe
- Deutsches Institut für Menschenrechte
- Gesellschaft für Freiheitsrechte
- An die Mitglieder des Vorstandes des Deutschen Anwaltvereins
- An die Vorsitzenden der Landesverbände des Deutschen Anwaltvereins
- An die Vorsitzenden der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Forum Junge Anwaltschaft

Presse

- Redaktion NJW
- Frankfurter Allgemeine Zeitung
- Süddeutsche Zeitung
- Berliner Verlag GmbH
- Hamburger Abendblatt
- Der Tagesspiegel
- Der Spiegel
- Juris Newsletter
- JurPC
- Netzpolitik.org
- Heise
- LTO

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt ca. 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

1. Zusammenfassung

Der DAV unterstützt das Ziel des Verordnungsentwurfs; die Bekämpfung der Verbreitung von Kindesmissbrauchsmaterial im Internet ist ein wichtiges Anliegen. Es ist daher ein begrüßenswerter Schritt, dass innerhalb der EU die Zusammenarbeit und Koordinierung von Strafverfolgungsbehörden der Mitgliedstaaten verbessert werden sollen. Ebenfalls zuzustimmen ist dem Verordnungsentwurf insoweit, als dass die Löschung strafbarer Inhalte, die beispielsweise aufgrund von Hinweisen identifiziert worden sind, einheitlich geregelt wird. Dies schafft Rechtssicherheit für die Diensteanbieter über die Grenzen der Mitgliedstaaten hinweg.

Im Übrigen ist der Vorschlag indes in weiten Teilen unverhältnismäßig. Das im Verordnungsvorschlag vorgesehene Instrument der Aufdeckungsanordnung läuft auf eine automatisierte, massenhafte Analyse von Kommunikations(inhalts-)daten aller Nutzer hinaus. Dies würde letztlich zu einer vollständigen Aufhebung der Vertraulichkeit der Kommunikation im digitalen Raum – etwa bei Email-, Messenger- und Chatanbietern, sozialen Medien oder Clouddiensten – führen, die mit den Grundrechtsgarantien insbesondere der Art. 7, 8 und 11 GRCh nicht zu vereinbaren ist.

Derartige Auswertungen von Kommunikationsinhalten würden eine Durchbrechung bzw. Umgehung von Verschlüsselungstechnologien wie der – mittlerweile verbreitet eingesetzten – Ende-zu-Ende-Verschlüsselung erfordern und so zu einer Schwächung der Sicherheit der Daten sämtlicher Kommunikationsteilnehmer führen.

Die kürzlich vom Berichterstatter des LIBE-Ausschusses vorgeschlagenen Änderungen sind nicht geeignet, die gegen das Instrument der Aufdeckungsanordnung vorgebrachte Kritik zu entkräften. Die vorgeschlagene Ergänzung des Verordnungsentwurfs um eine Befugnis zur *freiwilligen* Auswertung von Kommunikationsinhalten durch Diensteanbieter, ohne dass es einer entsprechenden Anordnung bedürfte, begegnet im Kern denselben rechtlichen Bedenken wie das Instrument der Aufdeckungsanordnung.

Es ist darüber hinaus nicht zu erwarten, dass die geplante Verordnung die Verbreitung von Missbrauchsmaterial signifikant eindämmen wird. Bereits jetzt findet dessen Austausch überwiegend abseits des Clear Web statt. Die geplanten Maßnahmen würden voraussichtlich lediglich dazu führen, dass entsprechende illegale Aktivitäten in noch größerem Umfang in das einer Regulierung kaum zugängliche Dark Web verlagert werden.

2. Hintergrund/Aktueller Stand

Die EU-Kommission hatte am 24. Juli 2020 eine EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern¹ vorgelegt und am 11. Mai 2022 einen Verordnungsvorschlag zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (COM(2022) 209 final, im Folgenden „CSAM-VO-E“) veröffentlicht.

Vor der Veröffentlichung des CSAM-VO-E hat die EU-Kommission eine öffentliche Konsultation durchgeführt, an der sich der DAV mit Stellungnahme Nr. 29/2021 beteiligt hat. Der DAV hat seine Bedenken gegen die derzeit geltende Übergangs-VO bereits in Stellungnahme Nr. 25/2021 geäußert. Im Gegensatz zur Übergangs-VO sieht der CSAM-VO-E – neben weiteren regulatorischen Anforderungen – eine behördliche Befugnis zur *Verpflichtung* von Diensteanbietern zur Aufdeckung von Missbrauchsdarstellungen vor.

Gem. Art. 1 Abs. 1 dient der CSAM-VO-E dem Kampf „gegen den Missbrauch einschlägiger Dienste der Informationsgesellschaft für den sexuellen Kindesmissbrauch

¹ EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern, COM(2020) 607 final, 24. Juli 2020.

im Internet“. Um dieses Ziel zu erreichen, sieht der CSAM-VO-E ein gestuftes Pflichtenprogramm für Anbieter von Hosting- und Kommunikationsdiensten im Internet vor, in der Form von Risikobewertungen (Art. 3), Risikominderung (Art. 4), Risikoberichten (Art. 5), Aufdeckungspflichten (Arts. 7 – 11), Meldepflichten (Arts. 12 – 13), Entfernungspflichten (Arts. 14 – 15) sowie Sperrpflichten (Art. 16 – 18). Hierbei wird zwischen bekanntem und unbekanntem Missbrauchsmaterial, sowie dem sogenannten „Grooming“ (Kontaktaufnahme zu Kindern für sexuelle Zwecke im Sinne von Art. 2 lit. o) unterschieden. Als Kommunikationsdienste sind u.a. Telefonie, E-Mail, Messenger, Chats und Videokonferenzen betroffen, die verpflichtet werden können, Texte, Bilder, Videos und Sprachnachrichten zu durchsuchen. Als Hostingdienste sind u.a. Webhoster, soziale Medien, Video-Streamingdienste, Filehoster und Clouddienste betroffen. Insbesondere können auch persönliche Cloudspeicherdienste, die nicht mit anderen Menschen geteilt werden, durchsucht werden.

Am 19. April 2023 hat der Berichterstatter des LIBE-Ausschusses im EU-Parlament, [REDACTED] (EPP, Spanien) seinen Berichtsentwurf vorgelegt und eine Reihe von Änderungen und Ergänzungen am Verordnungsentwurf vorgeschlagen.²

3. Stellungnahme

3.1. Ablehnung von Aufdeckungsmaßnahmen

Abzulehnen ist der Verordnungsentwurf in Bezug auf das Instrument der Aufdeckungsanordnung („Detection Order“) und die dadurch begründete Pflicht von Diensteanbietern, Kommunikationsinhalte anlass- und unterschiedslos automatisiert auszuwerten. Die in Art. 7 Ziff. 4 ff. VO-E statuierten Voraussetzungen für den Erlass einer Aufdeckungsanordnung sind mit insbesondere dem Abstellen auf ein „erhebliches Risiko, dass der betreffende Dienst zur Verbreitung von Missbrauchsmaterial bzw. für „Grooming“ genutzt wird“, hochgradig unbestimmt und zudem so niedrigschwellig, dass sie im Regelfall in Bezug auf sämtliche Hosting- und Kommunikationsdienste, insbesondere soziale Netzwerke, erfüllt sein dürften, sofern es sich nicht ausschließlich um typischerweise beruflich genutzte Dienste (wie z.B. Karriereplattformen, berufliche

² Berichtsentwurf des Innenausschusses zum Verordnungsvorschlag der EU-Kommission zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (COM (2022) 209 final.

Netzwerke, berufliche Messengerdienste) handelt. Die dadurch begründete Pflicht zur massenhaften Auswertung von Kommunikationsinhalten ist mit den Freiheitsgrundrechten, insbesondere dem Recht auf Achtung des Privatlebens (Art. 7 EU-GRCh, Art. 8 EMRK), auf Schutz personenbezogener Daten (Art. 8 EU-GRCh) sowie dem Recht auf Meinungs- und Informationsfreiheit (Art. 11 EU-GRCh, Art. 10 EMRK), unvereinbar.

Eine solche faktisch anlass- und unterschiedslose Speicherung von Kommunikationsdaten würde besonders schwere Eingriffe in die Vertraulichkeit der Kommunikation darstellen und überdies sämtliche Nutzer von E-Mail-, Chat- und Hosting-Diensten unter Generalverdacht stellen. Es drohen erhebliche „chilling effects“, d.h. einschüchternde, abschreckende oder sonst hemmende Auswirkungen auf die Ausübung der Freiheitsrechte der Betroffenen (vgl. dazu etwa EGMR, Entsch. v. 2.11.2006, 13071/03, Rn. 49; EGMR, Entsch. v. 6.10.2009, 27209/03, Rn. 37; BVerfGE 7, 198, 209; BVerfGE 73, 118, 183). Diese beeinträchtigenden Wirkungen würden sämtliche Kommunikationsteilnehmer treffen; im Speziellen wären erhebliche Eingriffe in das Vertrauensverhältnis zu Berufsgeheimnisträgern wie Rechtsanwältinnen, Ärzten und Journalisten zu befürchten (vgl. dazu EGMR, Entscheidung v. 6.7.1978, 5029/71, Rn. 41; BVerfGE 125, 260, 319, 332, 335).

Die im Entwurf vorgesehene massenhafte Auswertung von Kommunikationsinhalten stünde auch im Widerspruch zur ständigen Rechtsprechung des EuGH bezüglich der Zulässigkeit und Grenzen einer Vorratsdatenspeicherung. Der EuGH lässt die anlass- und unterschiedslose Speicherung von kommunikationsbezogenen Daten, selbst wenn es sich „lediglich“ um Verkehrs-, Bestands- und Standortdaten und nicht, wie vorliegend, auch um Inhaltsdaten handelt, nur unter sehr engen Voraussetzungen zu und verlangt für eine automatisierte Datenauswertung das Vorliegen „einer als real und aktuell oder vorhersehbar einzustufenden ernststen Bedrohung für die nationale Sicherheit“ oder eines konkreten Verdachts terroristischer Aktivitäten der Betroffenen. In beiden Fällen ist eine hinreichend wirksame gerichtliche oder behördliche Kontrolle zu gewährleisten (EuGH, Urt. v. 6.10.2020 – C-511/18, C-512/18, C-520/18). Zur Bekämpfung schwerer Kriminalität verlangt der EuGH darüber hinaus eine Eingrenzung auf einen objektiven und diskriminierungsfrei bestimmten Personenkreis oder auf eine bestimmte geographische Region (EuGH, C-511/18, C-512/18, C-520/18). Es sind klare

Garantien dafür erforderlich, dass bei der Verarbeitung der Daten die datenschutzrechtlichen Regeln eingehalten werden.

Eine Befugnis zur anlasslosen und massenhaften Auswertung auch von Kommunikationsinhalten und deren Meldung an Behörden würde zu besonders schwerwiegenden Eingriffen in die Vertraulichkeit von Kommunikation führen, die erheblich über die bisher diskutierten Maßnahmen der Vorratsdatenspeicherung hinausgehen.

Diese Einwände gelten gleichermaßen soweit Diensteanbieter, wie im Berichtsentwurf des LIBE-Ausschusses des EU-Parlaments vorgeschlagen, die Befugnis erhalten sollen, unabhängig von einer Aufdeckungsanordnung freiwillige Maßnahmen zur Überwachung und Auswertung von Kommunikationsinhalten zu ergreifen (siehe Änderungsanträge (ÄA) 11 (ErwGr 17a) und ÄA 37 (Art. 3 Abs. 2 lit. a bzgl. der Auflistung freiwilliger Aufdeckungsmaßnahmen in Risikoabwägungsberichten), ÄA 19 (ErwGr 29 bzgl. freiwilliger Aufdeckungsmaßnahmen), ÄA 30 (ErwGr 49) und ÄA 99 (Art. 5 Abs. a bzgl. freiwilliger Aufdeckungsmaßnahmen)).³

Auch das in ÄA 106 (Art. 6 Abs. a (neu)) vorgesehene Scannen von Metadaten lehnt der DAV ab. Es würde in der vorgeschlagenen Form den Anforderungen widersprechen, die der EuGH zuletzt in seiner Entscheidung *La Quadrature du Net* (Urteil vom 6. Oktober 2020 in den verb. Rs. C-511/18, C-512/18 und C-520/18, dort Abs. 172 ff.) in Bezug auf die anlasslose Überwachung derartiger Kommunikationsdaten aufgestellt hat.

3.1.1 Aushöhlung der Ende-zu-Ende-Verschlüsselung

Sofern – wie mittlerweile häufig – Online-Kommunikation Ende-zu-Ende verschlüsselt ist, wären Diensteanbieter verpflichtet, eine bestehende Verschlüsselung entweder aufzuheben oder dadurch zu umgehen, dass bereits auf dem verwendeten Endgerät vor dem Beginn des Übertragungsvorgangs ein Zugriff ermöglicht wird (sog. „Client-Side-Scanning“). Dies wiederum würde erhebliche Risiken für die Integrität und

³ Vgl. bereits die DAV-Stellungnahme zur CSAM-Übergangs-VO Nr. 25/2021.

Sicherheit von Kommunikationsmitteln begründen, die auch von Dritten ausgenutzt werden können, um Endgeräte auszuwerten und/oder zu kompromittieren. Die vorgeschlagene Verordnung würde damit letztlich eine Pflicht zur Quellen-TKÜ begründen, freilich ohne dass dafür die Voraussetzungen erfüllt sein müssten, die an entsprechende strafprozessuale Maßnahmen nach § 100a Abs. 1 S. 2 u. 3 StPO (insb. das Bestehen eines Verdachts bestimmter schwerer Straftaten) gestellt werden. Jegliche Aushebelung oder Schwächung von Ende-zu-Ende-Verschlüsselung birgt zudem ein hohes Missbrauchsrisiko, etwa durch (teil-)autoritäre Staaten oder Hackerangriffe durch böswillige Dritte, die nicht zuletzt auch ein erhebliches Risiko für die Sicherheit von Geschäftsgeheimnissen darstellen können.

3.1.2 Falsch-positive Treffer

Der Verordnungsentwurf macht darüber hinaus unzureichende Vorgaben hinsichtlich der Leistungsfähigkeit und Zuverlässigkeit der von den Diensteanbietern zu verwendenden Analysesoftware. Anforderungen wie „dem neuesten Stand der Technik in der Branche“ und „hinreichend zuverlässig“ (Art. 10 Ziff. 4 lit. c VO-E) sind nicht geeignet, hinreichend sicher zu gewährleisten, dass insbesondere der Anteil falsch-positiver Treffer auf ein angemessenes Maß reduziert wird. Harmlose Inhalte, zum Beispiel im Rahmen von einvernehmlichem Sexting oder Aufnahmen zu medizinischen Zwecken, könnten zum Teil irrtümlicherweise als missbräuchlich identifiziert werden. Etwa die Hälfte der Verfahren in Deutschland richten sich nach Angaben von Kinderschutzverbänden gegen Kinder und Jugendliche selbst, die einvernehmlich intime Bilder über soziale Medien getauscht haben.

Konkrete Vorgaben hinsichtlich der Leistungsfähigkeit und Zuverlässigkeit der von den Diensteanbietern zu verwendenden Analysesoftware wären insofern ohne weiteres möglich; auch ohne Diensteanbieter auf die Verwendung einer bestimmten Technologie zu verpflichten. Nach dem derzeitigen Stand der Technik sind insbesondere im Bereich der Entdeckung von „Grooming“-Inhalten die Falsch-Positiv-Raten derart hoch (die EU-Kommission geht selbst von einem Anteil von 10 % aus), dass täglich milliardenfach Kommunikationsinhalte zu Unrecht als strafbar identifiziert und gemeldet würden.

3.1.3 „Grooming“

Um sogenanntes „Grooming“, also die schleichende Kontaktaufnahme von Erwachsenen zu Minderjährigen, aufzuspüren, wäre nicht nur bekanntes Bildmaterial etwa anhand von Hashwerten zu analysieren, sondern es wäre erforderlich, jegliche Kommunikation, auch solche in Textform, zu durchsuchen. Da es sich um Texte handelt, wäre es nicht möglich, diese mit Hashwerten zu versehen, sondern es müsste der Inhalt einer jeden Nachricht kontrolliert werden.

Es wäre eine gesteigerte Fehleranfälligkeit solcher Textanalysen zu erwarten, da die Identifizierung von „Grooming“ in besonderem Maße eine zutreffende Erfassung der Zusammenhänge und Hintergründe der ausgewerteten Kommunikation sowie die Identität der beteiligten Personen voraussetzt. Die Feststellung, dass ein erwachsener Nutzer mit einem minderjährigen Nutzer kommuniziert, würde es beispielsweise erfordern, dass das Alter der Nutzer hinreichend zuverlässig verifiziert wird. Dies würde letztlich zu einer Klarnamen- und Identifizierungspflicht im Bereich der Online-Kommunikation führen. Potenziell besonders betroffen wären in diesem Zusammenhang Kommunikationsvorgänge zwischen minderjährigen Nutzern.

3.2 Löschung

Der DAV begrüßt, dass Artikel 14 und 15 CSAM-VO-E das zeitnahe Entfernen von Darstellungen des sexuellen Kindesmissbrauchs aus dem Internet vorsehen. Dies ist nicht zuletzt zum Schutz der Opfer unabdingbar. Da es sich um eindeutig rechtswidrige Inhalte handelt, sollte für diese eine Löschpflicht für Hostingdienste innerhalb kurzer Frist bei gleichzeitiger Sicherung für Zwecke des Ermittlungs- und Strafverfahrens greifen. Sperranordnungen, wie in Art. 16 ff. VO-E vorgesehen, sollten nur dann in Erwägung gezogen werden, wenn die Löschung der Inhalte nicht möglich ist.

3.3 Verletzung des anwaltlichen Berufsgeheimnisses

Anwältinnen und Anwälte kommunizieren, wie andere Berufsgruppen auch, überwiegend digital; die Kommunikation mit Mandantinnen und Mandanten wäre somit

der inhaltlichen Auswertung aufgrund von Aufdeckungsanordnungen in gleicher Weise ausgesetzt wie die Online-Kommunikation anderer Nutzer. Das Berufsgeheimnis ist in einem Rechtsstaat unabdingbar und dient u.a. der Verwirklichung des Anspruchs auf ein faires Verfahren inklusive einer Verteidigung (Art. 6 EMRK) und des Rechts auf einen wirksamen Rechtsbehelf inklusive der Beratung, Verteidigung und Vertretung (Art. 47 GRCh). Die Nutzung und Verwertung von Informationen, die dem Berufsgeheimnis unterliegen, muss dementsprechend unterbunden werden (vgl. zum deutschen Recht §§ 100 d Abs. 5, 160a Abs. 2 u 3 StPO). Insbesondere Mandatsbeziehungen zu Rechtsanwältinnen und Rechtsanwälten, die Opfer von Kindesmissbrauch und/oder Beschuldigte in Strafverfahren in diesem Bereich beraten und vertreten, wären von der Verordnung betroffen. Hier dürften die Beteiligten nicht mehr davon ausgehen, dass Nachrichten und Bildmaterial, die zwischen Mandantin und Rechtsanwalt sei es per E-Mail oder über Cloud-Server ausgetauscht werden, vertraulich bleiben und nicht zu Unrecht als strafbare Inhalte identifiziert und gemeldet werden. Das Wohl des Kindes umfasst auch sein Recht auf Vertraulichkeit. Dies ist besonders wichtig in Situationen, in denen Rechtsanwälte Opfer von Kindesmissbrauch vertreten. Die Nutzung von Online-Diensten im Mandatsverhältnis würde damit nicht hinnehmbare berufs- und strafrechtliche Risiken für Rechtsanwältinnen und Rechtsanwälte bedeuten, die in der Konsequenz dazu führen würden, dass Anwältinnen und Anwälte jedenfalls im Bereich der Verteidigung und Opfervertretung im Zusammenhang mit Kindesmissbrauch und „Grooming“ von digitaler Kommunikation absehen und auf die analoge Welt ausweichen müssten.

Momentan ist es für Analysesoftware technisch nicht möglich, Kommunikationsinhalte, die aus Gründen des Berufsgeheimnisses geschützt werden müssen, zuverlässig auszusondern. Dies stellt nicht die besondere – grundrechtlich geschützte – Stellung des Berufsgeheimnisses in Frage. Vielmehr offenbart eine solche technische „Unmöglichkeit“, dass die Analysesoftware nicht in der Lage ist, eine rechtlich unbedenkliche Auswertung der identifizierten Inhalte zu gewährleisten. Solange diese technische „Unmöglichkeit“ besteht, darf schon deshalb keine Verpflichtung zur massenhaften Auswertung von Kommunikationsinhalten bestehen, die Kommunikationsinhalte, die aus Gründen des Berufsgeheimnisses geschützt werden müssen, nicht aussondern kann.

Von: [REDACTED] IIIB7 - <[REDACTED]@bmj.bund.de>
An: E-Post-RegIII <E-Post-RegIII@bmj.bund.de>
CC: [REDACTED]@bmj.bund.de>
Gesendet am: 23.05.2023 19:13:00
Betreff: WG: Stellungnahme der Bundesrechtsanwaltskammer - Verordnung zur Bekämpfung des Kindesmissbrauchs online („Chatkontrolle“)

Bitte verakten.

[REDACTED]
- III B 7 -
[REDACTED]

Von: [REDACTED] (BRAK) <[REDACTED]@brak.de>
Gesendet: Dienstag, 23. Mai 2023 13:13
An: [REDACTED] (BRAK) <[REDACTED]@brak.de>; [REDACTED] (BRAK) <[REDACTED]@brak.de>; [REDACTED] (BRAK Brüssel) <[REDACTED]@brak.eu>
Betreff: Stellungnahme der Bundesrechtsanwaltskammer - Verordnung zur Bekämpfung des Kindesmissbrauchs online („Chatkontrolle“)

Sehr geehrte Damen und Herren,

die Bundesrechtsanwaltskammer hat zum Vorschlag einer Verordnung zur Bekämpfung des Kindesmissbrauchs online („Chatkontrolle“) Stellung genommen (s. Anlage).

Die Bundesrechtsanwaltskammer sieht den vorgelegten Entwurf kritisch.

Die Europäische Kommission hat am 11. Mai 2022 eine Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern im Internet vorgeschlagen. Dieser Entwurf wird derzeit von den Co-Gesetzgebern Rat und Parlament beraten. In naher Zukunft sollen die Verhandlungen im Trilog beginnen.

Die Bundesrechtsanwaltskammer kritisiert, dass der Entwurf mit der Verpflichtung zur Erkennung von Missbrauchsinhalten sowie daran anschließenden Datenverarbeitungen in einem Rechtsstaat inakzeptabel weitreichende Grundrechtsbeeinträchtigungen vorsieht, die auch angesichts des Zieles des Missbrauchsschutzes nicht gerechtfertigt werden können. Der von der EU-Kommission betonte Ausgleich der Grundrechtspositionen ist nicht gelungen. Er kann ohne eine Beschränkung der Zielrichtung des Entwurfs, weitreichende Inhaltserkennungen

Besonders bedauerlich und rechtsstaatlichen Maßstäben nicht genügend ist, dass das Bedürfnis nach einem Schutz des Mandatsgeheimnisses im Entwurf keine Berücksichtigung findet. Über die im Entwurf angelegte Beeinträchtigung der Vertraulichkeitsgrundrechte können auch die – nur begrenzt – vorgesehenen Sicherungsmechanismen und Verpflichtungsbeschränkungen nicht hinweghelfen. Das Mandatsgeheimnis würde weitgehend ausgehebelt. Auch die durch den Berichtsentwurf vorgenommenen Änderungen sind nicht ausreichend. Auch eine Begrenzung auf unverschlüsselte Inhalte oder freiwillige Erklärungen würden keinen hinreichenden Schutz bieten.

Für weitere Einzelheiten darf ich Sie auf die beigefügte Stellungnahme verweisen.

████████████████████

11/11/2011

Bitte beachten Sie unsere Datenschutzhinweise unter <https://www.brak.de/datenschutz/allgemein>

<<https://www.brak.de/datenschutz/allgemein>> .

BRAK-Mitteilungen und BRAK-Magazin finden Sie unter <https://www.brak.de/zeitschriften>
<<https://www.brak.de/zeitschriften>> .



BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 22/2023

Mai 2023

Registernummer: 25412265365-88

Verordnung zur Bekämpfung des Kindesmissbrauchs online („Chatkontrolle“)

Mitglieder des Ausschusses Datenschutzrecht

[REDACTED]

Mitglieder des Ausschusses Europa

[REDACTED]

Bundesrechtsanwaltskammer

The German Federal Bar
Barreau Fédéral Allemand
www.brak.de

Büro Berlin – Hans Litten Haus

Littenstraße 9
10179 Berlin
Deutschland
Tel. +49.30.28 49 39-0
Fax +49.30.28 49 39-11
Mail zentrale@brak.de

Büro Brüssel

Avenue des Nerviens 85/9
1040 Brüssel
Belgien
Tel. +32.2.743 86 46
Fax +32.2.743 86 56
Mail brak.bxl@brak.eu

[REDACTED]

Verteiler: Bundesministerium des Innern und für Heimat
Bundesministerium der Justiz
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Rechtsausschuss des Deutschen Bundestages
Innenausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesnotarkammer
Bundessteuerberaterkammer
Bundesverband der Freien Berufe
Deutscher Anwaltverein
Deutscher Juristinnenbund
Deutscher Notarverein
Deutscher Richterbund
Neue Richtervereinigung e.V.
Patentanwaltskammer
Deutscher Steuerberaterverband e.V.
Wirtschaftsprüferkammer
Gesellschaft für Datenschutz und Datensicherheit e. V.
Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Deutsche Vereinigung für Datenschutz e. V.
Bitkom e. V.
davit – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.
eco – Verband der Internetwirtschaft e. V.
VAUNET – Verband Privater Medien e. V.
Stiftung Datenschutz
Datenschutzberater
Computer und Recht
Redaktionen der NJW, ZAP, AnwBl, DRiZ, FamRZ, FAZ, Süddeutsche Zeitung, Die Welt, taz, Handelsblatt, dpa, Spiegel, Focus, Deubner Verlag Online Recht, Beck aktuell, Jurion
Expertenbriefing, Juris Nachrichten, LexisNexis Rechtsnews, Otto Schmidt Verlag

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Die Bundesrechtsanwaltskammer bedankt sich für die Möglichkeit einer Stellungnahme und gibt Nachstehendes zu bedenken.

Inhalt

Zusammenfassung	4
Stellungnahme.....	5
1. Erkennung	5
1.1 Verpflichtende Erkennung	5
1.1.1 Auswirkungen auf die anwaltliche Verschwiegenheit.....	5
1.1.2 Inakzeptable Kommunikationszugriffe durch die Pflicht zur Erkennung in jedem Fall zu erwarten.....	6
1.1.3 Anlasslosigkeit und unzureichende Risiko- bzw. Verdachtskonkretisierung	6
1.1.4 Problematischer Einbezug Privater Akteure	7
1.1.5 Grundrechtsabwägung und unzureichende Sicherungsmechanismen.....	7
1.1.6 Insbesondere: Fehlender Schutz von Berufsgeheimnissen.....	8
1.1.7 Verschärfung durch zu weite Definitionen und fehlende Ausnahmen	12
1.1.7.1 Bekannte Missbrauchsdarstellungen	12
1.1.7.2 Unbekannte Missbrauchsdarstellungen	12
1.1.7.3 Grooming-Kommunikation.....	13
1.1.7.4 Ausschluss des elektronischen Rechtsverkehrs	14
1.1.8 Nachgelagerte Risiken durch Erhebung, Sammlung und Austausch von Informationen.....	14
1.1.8.1 Achtung von Verschwiegenheitspflichten bei nachfolgenden Verarbeitungsvorgängen.....	15
1.1.8.2 Keine Weiterverarbeitungsbefugnis beim Diensteanbieter.....	15
1.1.8.3 Kein Sammeln und Reporting von Mandatsinformationen	15
1.1.8.4 Beschränkung der Kooperationsbefugnisse.....	16
1.1.8.5 Vermeidung von Personenbezügen.....	16
1.1.9 Menschliche Aufsicht (human oversight)	16
1.2 Ausschluss von Erkennungsmaßnahmen auf freiwilliger Basis und Richtervorbehalt	17
2. Altersprüfung	18
3. Behördliche Aufsicht	18
3.1 Aufsichtsbefugnisse.....	19
3.2 Verschwiegenheit	19
4. Verschwiegenheit der Zentralstelle	20
5. Verhältnis zum übrigen Datenschutzrechtsregime und Datenschutz-Folgenabschätzung	20
6. Evaluation	20
7. Alternative Ansätze	21

Zusammenfassung

Der vorgelegte Entwurf sieht mit der Verpflichtung zur Erkennung von Missbrauchsinhalten sowie daran anschließenden Datenverarbeitungen in einem Rechtsstaat inakzeptabel weitreichende Grundrechtsbeeinträchtigungen vor, die auch angesichts des Zieles des Missbrauchsschutzes nicht gerechtfertigt werden können. Der von der EU-Kommission immer wieder betonte Ausgleich der Grundrechtspositionen ist nicht gelungen. Er kann ohne eine Beschränkung der Zielrichtung des Entwurfs, weitreichende Inhaltserkennungen zu ermöglichen, auch nicht erreicht werden. Über die in dieser Grundentscheidung angelegte grundsätzliche Beeinträchtigung der Vertraulichkeitsgrundrechte können auch die – nur begrenzt – vorgesehenen Sicherungsmechanismen und Verpflichtungsbeschränkungen nicht hinweghelfen. Auch die durch den Berichtsentwurf vorgenommenen Änderungen sind nicht ausreichend.

Verschlimmert wird diese Ausgangssituation durch zu weite Tatbestandsvoraussetzungen der Erkennungsverpflichtung, einen übermäßigen Umfang derselben und weit reichende Datensammlungs- und Austauschbefugnisse.

Besonders bedauerlich und rechtsstaatlichen Maßstäben nicht genügend ist, dass das auf der Hand liegende, von den Rechtsanwaltsorganisationen mehrfach vorgetragene und wenigstens in den Erwägungsgründen der derzeit übergangsweise geltenden Verordnung (EU) 2021/1232 noch anerkannte Bedürfnis nach einem Schutz des Mandatsgeheimnisses in diesem Gesetzesvorhaben noch nicht einmal erwähnt – geschweige denn gewährleistet wird. Dies kann nicht anders gedeutet werden, als dass die Autoren sich bewusst über dieses Erfordernis und die dadurch geschützten Grundrechte hinweggesetzt haben ohne der gesetzgeberischen Pflicht, eine gewissenhafte Grundrechtsabwägung vorzunehmen, auch nur im Ansatz zu genügen. Dies stellt die Beteuerungen der Kommission, einen angemessenen Grundrechtsausgleich angestrebt und erzielt zu haben, ad absurdum.

Die Bundesrechtsanwaltskammer fordert die EU-Institutionen vor diesem Hintergrund dazu auf, von der vorgesehenen Einführung der Erkennungspflicht abzusehen.

Soweit dies nicht geschieht, sind dringend weitere – indes naturgemäß nicht ausreichende – Sicherungsmechanismen vorzusehen und der Verpflichtungsbereich durch klarere und engere Definitionen einzugrenzen.

Entsprechende Vorschläge finden sich in dieser Stellungnahme unter 1.1.7 und 1.1.8. Insbesondere müssen Erkennungsmaßnahmen, durch welche die anwaltliche Verschwiegenheit beeinträchtigt würde, ausgeschlossen werden (s. dazu 1.1.6). Insoweit sollte auch klargestellt werden, dass jedenfalls Dienste des elektronischen Rechtsverkehrs von jeglicher Erkennungspflicht ausgenommen sind (1.1.7.3).

Auch sollten zur Vermeidung wiederholter Grundrechtsbeeinträchtigungen der ursprünglichen Erkennung nachgelagerte Datenverarbeitungen und -austausche reduziert werden. Entsprechende Vorschläge finden sich in dieser Stellungnahme unter 1.1.8.

Kritisch zu bewerten ist auch die vorgesehene Altersverifizierung, die regelmäßig nicht ohne identifizierende Maßnahmen erfolgen wird können. Um die rechtsstaatlich gebotene Möglichkeit der unerkannten Inanspruchnahme anwaltlicher Beratung zu gewährleisten, sollten Altersverifizierungen nur auf Plattformen vorgeschrieben werden, auf denen mit einer Inanspruchnahme anwaltlicher Beratung nicht gerechnet werden kann. Ein entsprechender Regelungsvorschlag findet sich unter 2. Altersprüfung.

Die vorgesehenen Aufsichtsbefugnisse müssen zum Schutz des Mandatsgeheimnisses in Bezug auf Berufsgeheimnisträger beschränkt werden. Ein entsprechender Regelungsvorschlag findet sich unter 3.1.

Aufgrund der Möglichkeit des Rückgriffs auf fremde Ausweisdokumente erscheint die Altersverifizierung ohnehin wenig erfolgsversprechend.

Es muss sichergestellt werden, dass eingebundene Private – und namentlich die Beschäftigten der verpflichteten Diensteanbieter – den einschlägigen mitgliedstaatlichen Verschwiegenheitsverpflichtungen sowie im Mindesten den der Art. 339 AEUV geregelten Verpflichtungen unterliegen (1.1.4). Die in dem Entwurf bereits vorgesehenen Verschwiegenheitssicherungen der Aufsichtsbehörden und der neu zu schaffenden Zentralstelle sollten geschärft werden (3.1 und 4.). Einer weitergehenden Flankierung zur Gewährleistung der Verschwiegenheit bedarf es auch bei der – im Grundsatz zu begrüßenden – menschlichen Aufsicht der Missbrauchserkennung (1.1.9).

Erforderlich ist ferner eine Klarstellung, dass Inhaltserkennungen allenfalls auf der Grundlage einer richterlichen Anordnung und keinesfalls auf freiwilliger Grundlage erfolgen dürfen (siehe dazu 1.2).

Das Erfordernis der Durchführung einer Datenschutz-Folgenabschätzung sollte dem Grundsatz der Unberührtheit des EU-Datenschutzregimes folgend von der Erkennung von Grooming-Kommunikation auch auf die Erkennung von Missbrauchsdarstellungen ausgeweitet werden (5.).

Diensteanbieter sollten verpflichtet werden, Nutzer auf etwaig bestehende alternative Möglichkeiten der vertraulichen Inanspruchnahme anwaltlicher Beratung hinzuweisen (1.1.6).

Stellungnahme

1. Erkennung

Die in dem Entwurf vorgesehene Erkennung von Missbrauchsinhalten stößt auf grundlegende Bedenken. Sie ist daher abzulehnen.

1.1 Verpflichtende Erkennung

Artt. 7 – 10 des Entwurfs sehen für Anbieter interpersoneller Kommunikationsdienste sowie von Hosting-Diensten eine Verpflichtung zur Erkennung von Missbrauchsdarstellungen sowie von Kontaktaufnahmen (sog. Grooming-Kommunikation) vor, wenn dies auf behördlichen Antrag hin gerichtlich oder durch eine andere unabhängige Behörde angeordnet wurde (sog. detection order).

1.1.1 Auswirkungen auf die anwaltliche Verschwiegenheit

Um einen effektiven Zugang zum Recht zu gewährleisten, ist es erforderlich, dass Mandantinnen und Mandanten anwaltliche Beratung vertrauensvoll über die von ihnen im Alltag eingesetzten Kommunikationswege in Anspruch nehmen können. Spiegelbildlich sind Anwältinnen und Anwälte zur Ausübung ihres Berufs darauf angewiesen, ihre Dienste auf diesem Wege anbieten zu können. Zudem muss Anwältinnen und Anwälten in der modernen arbeitsteiligen Welt die Möglichkeit bleiben, unter besonderen Sicherheitsvorkehrungen vertrauensvoll Hosting-Dienste in Anspruch zu nehmen. All dies wäre nicht mehr möglich, wenn die in dem Verordnungsvorschlag vorgesehene Pflicht zur Erkennung von Inhalten durch Kommunikations- und Hosting-Anbieter realisiert würde (dazu im Einzelnen sogleich ab 1.1.2).

Die Kommission scheint trotz mehrfacher Hinweise die Bedeutung des Mandatsgeheimnisses und die zu seinem Schutz zwingend erforderliche Möglichkeit der Inanspruchnahme vertraulicher Online-Kommunikation zu verkennen oder – schlimmer – schlicht zu ignorieren. Für letzteres spricht, dass sogar die in den Erwägungsgründen der Übergangsverordnung ((EU) 2021/1232) noch enthaltene Klausel zum Schutz des Mandatsgeheimnisses sich in dem nun vorgelegten Vorschlag nicht wiederfindet. Die BRAK sieht sich daher gezwungen, ihre mehrfach erfolgten Erläuterungen zur Bedeutung des Mandatsgeheimnisses zu wiederholen: Die anwaltliche Verschwiegenheit ist eine Voraussetzung für die Inanspruchnahme rechtsanwaltlicher Beratung und damit ein Grundpfeiler eines jeden Rechtsstaats. Sie unterfällt dem Schutz der europäischen wie nationalen Rechtsstaatsgarantien aus Art. 47 Abs. 1 Satz 2 GRCh, Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK sowie Art. 20 Abs. 2 GG, Art. 103 Abs. 1 GG. Zugleich ist sie im Kontext anwaltlicher Beratung Voraussetzung für die Verwirklichung europäischer wie nationaler Grundrechte aus Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK, Art. 47 Abs. 1, 2 Satz 2 GRCh, Art. 20 Abs. 3, Art. 103 Abs. 1 GG, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK, Art. 7 GRCh, Art. 12 Abs. 1 GG. Sie dient in erster Linie dem Schutz des Mandanten und seines Zugangs zum Recht. Das Mandatsgeheimnis schützt Opfer, Täter und sonstige Rechtsuchende gleichermaßen. Wird sein Schutz nicht gewährleistet und können Mandanten daher keinen Rechtsrat in Anspruch nehmen, wird dadurch zugleich die Anwaltschaft in ihrer Berufsausübungsfreiheit beeinträchtigt.

1.1.2 Inakzeptable Kommunikationszugriffe durch die Pflicht zur Erkennung in jedem Fall zu erwarten

Jede Art der Erkennung von Missbrauchsdarstellungen bzw. von Grooming-Kommunikation wird einen Zugriff auf die Kommunikations- bzw. Speicherinhalte erfordern. Dies gilt auch, wenn die Erkennung mittels – vergleichsweise – vertraulichkeitsschonender Technologien wie etwa durch einen Abgleich von Hashwerten erfolgt. Denn sobald die hierzu zwingend erforderliche Möglichkeit des Kommunikationszugriffs – etwa zum Zwecke der Erstellung bzw. des Abgleichs von Hashwerten – eröffnet ist, können die Kommunikationsteilnehmer nicht länger auf die Vertraulichkeit der Kommunikation vertrauen und der mit dem Mandatsgeheimnis verfolgte Zweck, Rechtsuchende nicht durch die Befürchtung von Vertraulichkeitsverlusten von der Inanspruchnahme anwaltlicher Beratung abzuhalten, könnte nicht länger erfüllt werden. Der in der Verordnung vorgesehene Einsatz schonender technischer Mittel ist aus dem genannten Grund nicht geeignet, diese Bedenken auszuräumen. Gleiches gilt für die organisatorischen und prozessualen Schutzvorkehrungen sowie die wiederholten Betonungen des – ohnehin zwingend zu beachtenden – Verhältnismäßigkeitsgrundsatzes. Bereits aus diesem Grund ist jede Erkennung von Kommunikationsinhalten abzulehnen.

1.1.3 Anlasslosigkeit und unzureichende Risiko- bzw. Verdachtskonkretisierung

Überdies können die primär- und verfassungsrechtlichen Anforderungen der Anlassbezogenheit bzw. der hinreichenden Risikokonkretisierung angesichts der in der Verordnung vorgesehenen, keinen konkreten Verdacht erfordernden und nicht auf einzelne Sachverhalte oder Korrespondenzen bezogene, Pflicht zu Erkennung nicht erfüllt werden. Vielmehr lässt Art. 7 Abs. 4 lit. a im Gegenteil bereits ein „signifikantes Risiko“ ausreichen. Auch die in den Folgeabsätzen 5 bis 7 vorgenommenen Konkretisierungen des Risikobegriffs begrenzen den Anwendungsbereich nicht auf konkrete Anlässe oder Verdachtsfälle. Besonders zu beanstanden ist in diesem Zusammenhang, dass die Konkretisierungen mit der Formulierung „gilt als“ („shall be deemed“) als bloße Regelbeispiele verstanden werden könnten, sodass zu befürchten steht, dass Behörden und Gerichte ein signifikantes Risiko auch in Fällen annehmen werden, in denen die dort genannten Voraussetzungen nicht erfüllt sind. Auch der Einbezug bloß vergleichbarer Dienste gemäß Art. 7 Abs. 5 lit. b, Abs. 6 lit. b und Abs. 7 lit. c läuft den Erfordernissen eines Anlassbezugs und einer Risikokonkretisierung zuwider.

1.1.4 Problematischer Einbezug Privater Akteure

Die vorgesehenen Verpflichtungen zur Erkennung, Sammlung und Weiterleitung von Inhaltsinformationen treffen zuvorderst die Diensteanbieter und damit überwiegend private Stellen, die weder einem Dienstgeheimnis noch einer demokratischen Kontrolle unterliegen. Überdies haben sich einige von ihnen durch Datenlecks und Skandale als geradezu untauglich zur Verarbeitung höchstsensibler Inhalte erwiesen. Die Beharrlichkeit, mit der sich große Plattformanbieter seit Jahren trotz aufsichtsbehördlicher Maßnahmen, hoher Bußgeldandrohungen und privater Initiativen über elementarste datenschutzrechtliche Anforderungen hinwegsetzen, zeigt, dass gesetzlich vorgegebene Sicherungsmechanismen in diesem Bereich keine hinreichende Gewähr für die Vertraulichkeit der Datenverarbeitungen bieten. Auch dieses Problem wird sich nur zufriedenstellend lösen lassen, indem auf die Pflicht zur Inhaltserkennung verzichtet wird. Sollte der europäische Gesetzgeber sich indes über alle rechtsstaatlichen und praktischen Bedenken hinwegsetzen und an der Erkennungspflicht festhalten, so wären zumindest erheblich weitergehende Flankierungen zum Schutz der Vertraulichkeit erforderlich, die über die bisher bereits datenschutzrechtlich vorgegebenen hinausgehen. Dies gilt insbesondere mit Blick auf Berufsgeheimnisse.

Ferner sollte in Art. 40 Abs. 2 des Entwurfs, nach welchem die EU-Zentralstelle in nicht näher spezifizierter Weise mit privaten Organisationen zusammenarbeiten soll, konkretisiert werden, welche Arten der Zusammenarbeit gemeint sind und welche Kooperationen ausgeschlossen sind. Auch in diesem Zusammenhang muss der Vertraulichkeitsschutz – insbesondere mit Blick auf Berufsgeheimnisse – gewährleistet werden.

Entsprechende Änderungsvorschläge werden sogleich unter 1.1.6 Insbesondere: fehlender Schutz von Berufsgeheimnissen im Zusammenhang mit den dort unterbreiteten Vorschlägen dargestellt.

1.1.5 Grundrechtsabwägung und unzureichende Sicherungsmechanismen

Art. 7 Abs. 4 lit. b stellt den Erlass einer Erkennungsanordnung unter den Vorbehalt einer umfassenden Grundrechts- und Interessensabwägung. Wenngleich dieses – selbstverständliche – Erfordernis grundsätzlich zu begrüßen ist, ist es in diesem Zusammenhang nicht geeignet, einen hinreichenden Grundrechtsschutz zu gewährleisten.

Zunächst ist zu beanstanden, dass die Grundrechtsabwägung bei derart einschneidenden Grundrechtseingriffen bereits weitest möglich auf Ebene des Gesetzgebers erfolgen muss und nicht den Gerichten überlassen bleiben darf. Abgesehen von den übrigen unzureichenden Einschränkungen des Art. 7 Abs. 4 – 8 sind jedoch keinerlei gesetzgeberische Wertungen vorgegeben. Als Wertentscheidung des Gesetzgebers erkennbar ist einzig, dass es bei signifikanten Risiken in einer kaum überschaubaren Vielzahl von Fällen möglich sein soll, (Kommunikations-)Inhalte zu erkennen. Damit wird in weiten Teilen die Möglichkeit der vertraulichen elektronischen Kommunikation und Datenverarbeitung abgeschafft und ohne hinreichende Rechtfertigung oder ausgleichende Sicherungsmechanismen in Vertraulichkeitsgrundrechte eingegriffen.

Soweit der Entwurf etwa in Art. 7 Abs. 8 und 9 sowie den Artt. 8 – 10 Sicherungsmechanismen vorsieht, sind diese angesichts der Grundentscheidung, dass Inhalte auf breiter Front und weitestgehend ohne Möglichkeiten der Differenzierung zwischen betroffenen Nutzern erkannt und zu diesem Zweck eingesehen werden sollen, ebenso untauglich, Grundrechtsverletzungen zu verhindern, wie die Erfordernisse einer Grundrechtsabwägung durch Behörden und Gerichte sowie eines signifikanten Risikos. Die strafrechtlich relevante Nutzung eines Dienstes durch Einzelne vermag massenhafte Eingriffe in die Vertraulichkeitsgrundrechte anderer Nutzer nicht zu rechtfertigen – auch nicht unter Opferschutzgesichts-

punkten. Dies gilt umso mehr als mittlerweile ein Großteil der vertraulichkeitsbedürftigen Grundrechtsausübungen im Onlinebereich erfolgt – sei es bei der Inanspruchnahme elektronischer Kommunikation oder der Nutzung von Cloud-Diensten. Würde in diesem Bereich die Möglichkeit vertraulicher Kommunikation eingeschränkt, verbliebe für die entsprechende Grundrechtsausübung kaum noch Raum. Die Grundrechte wären damit faktisch in weiten Teilen nicht länger gewährleistet. Ausweis dieser inakzeptablen Grundentscheidung der Entwurfsautoren zulasten der Vertraulichkeitsgrundrechte ist auch Erwägungsgrund 23 Satz 2, in welchem zwar die Verhältnismäßigkeit angemahnt wird, und zu deren Erreichung allerlei Sicherungsmechanismen aufgezählt werden, diese jedoch unter den Vorbehalt gestellt werden, dass die Effektivität der Inhaltserkennung dadurch nicht beeinträchtigt werde. Der von der Kommission angestrebte und beanspruchte Grundrechtsausgleich kann auf diese Weise nicht erreicht werden.

Der im EP-Berichtsentwurf enthaltene Änderungsantrag 99 zu Art. 5 a über freiwillige Aufdeckungsanordnungen ist deswegen ebenfalls nicht unterstützenswert. Auch der Zusatz des Berichtstatters zu Art. 7 (Änderungsantrag 111, Art. 7 (2) UAbs. 1 a), welche eine „fair balance between the fundamental rights“ vorsieht, verkennet die Bedeutung dieser Grundrechte.

An dieser Stelle wird auch auf die Ergebnisse der ergänzenden Folgenabschätzung des Wissenschaftlichen Dienstes des Europäischen Parlaments aus dem April 2023 und die gemeinsame Stellungnahme zum Kommissionsvorschlag des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten verwiesen.

Änderungsvorschlag:

- **Die in den Artt. 7 – 10 vorgesehene Verpflichtung zur Erkennung von Inhalten ist zu streichen**

1.1.6 Insbesondere: Fehlender Schutz von Berufsgeheimnissen

Insbesondere in Fällen, in denen ein Berufsgeheimnis betroffen ist, kann nach dem vorgelegten Entwurf ein hinreichender Grundrechtsschutz bzw. ein hinreichender Grundrechtsausgleich nicht geschaffen werden. Denn eine grundrechtskonforme Erkennung und Aussonderung anwaltlicher, ärztlicher oder sonstiger streng vertraulicher Kommunikation erscheint weder vorgesehen noch technisch möglich.

In rechtlicher Hinsicht ist mit Blick auf Berufsgeheimnisse und die diesen zugrundeliegenden Grundrechte zudem zu beachten, dass sie im Vergleich zu basalen Persönlichkeitsrechten regelmäßig deutlich höher zu gewichten und an entsprechende Eingriffe höhere Anforderungen zu stellen sind. Dies gilt wie bereits oben unter 1.1.1 dargestellt in besonderem Maß für das anwaltliche Mandatsgeheimnis. So sind Einblicke in der anwaltlichen Verschwiegenheit unterliegende Informationen nur ausnahmsweise zum Schutz gewichtigster Rechtsgüter und unter Beachtung strenger Anforderungen – beispielsweise zur Verhinderung einer mit hinreichender Gewissheit unmittelbar bevorstehenden schweren Straftat – zulässig. Eingriffe in das Mandatsgeheimnis müssen also im Regelfall und namentlich unter den im Entwurf vorgesehenen geringen Anforderungen und dem dort angelegten Umfang unterbleiben. Im Kontrast zu dieser rechtlichen Anforderung scheint dem vorgelegten Entwurf jedoch die Logik zugrunde zu liegen, dass Eingriffe in der Regel zulässig seien. Denn anderenfalls verbliebe für die vorgesehene Erkennungsanordnung kaum ein Anwendungsbereich. Es steht zu befürchten, dass Gerichte und Aufsichtsbehörden diese Logik fälschlicherweise übernehmen und das Mandatsgeheimnis im Rahmen der gemäß Art. 7 Abs. 4 Unterabsatz 1 lit. b vorgesehenen Grundrechtsabwägung missachten oder falsch gewichten. Es gilt dringend zu verhindern, dass das Mandatsgeheimnis auf diese Weise im Online-Bereich faktisch außer Kraft gesetzt wird.

Sofern nicht auf die Erkennungsverpflichtung verzichtet wird, muss eine solche daher zumindest die Gewährleistung des Berufs- bzw. Mandatsgeheimnisschutzes zur Voraussetzung haben und um technische und organisatorische Maßnahmen zur Erreichung dieses Zwecks ergänzt werden. Ferner sollten Anbieter in diesem Fall verpflichtet werden, Nutzer auf etwaig bestehende Möglichkeiten hinweisen, Rechtsrat vertraulich in Anspruch zu nehmen. Die oben unter 1.1.4 Problematischer Einbezug Privater Akteure dargestellten Aspekte müssen dabei beachtet werden.

Überdies sollte das Verhältnis zwischen den Verpflichtungen nach der Verordnung und solchen, die aus nationalen berufsrechtlichen Verpflichtungen erwachsen, analog zur datenschutzrechtlichen Kollisionsregel des Art. 1 Abs. 3 lit. d zugunsten der berufsrechtlichen (Verschwiegenheits-)Verpflichtungen geregelt werden.

Änderungsvorschläge:

Damit ergeben sich die nachstehenden Änderungsvorschläge.

- **Art. 1 Abs. 3** sollte wie folgt ergänzt werden:

„Diese Verordnung berührt nicht die in den folgenden Rechtsakten festgelegten Vorschriften:

(a) Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie, die den Rahmenbeschluss 2004/68/JI des Rates ersetzt;

(b) Richtlinie 2000/31/EG und Verordnung (EU) .../... [über einen Binnenmarkt für digitale Dienste (Digital Services Act) und zur Änderung der Richtlinie 2000/31/EG];

(c) Richtlinie 2010/13/EU;

(d) die Verordnung (EU) 2016/679, die Richtlinie 2016/680, die Verordnung (EU) 2018/1725 und, vorbehaltlich des Absatzes 4 des vorliegenden Artikels, die Richtlinie 2002/58/EG;

(e) Nationale sowie unions- und konventionsrechtliche Regelungen betreffend die Ausübung freier Berufe und namentlich solcher betreffend den Schutz von Berufsgeheimnissen.“

(Hinzufügungen hervorgehoben)

- Am **Ende des sechsten Abschnitts des zweiten Kapitels** sollte nach dem derzeitigen Art. 24 ein zusätzlicher Artikel mit folgendem Inhalt eingefügt werden:

„Artikel xx

Verschwiegenheit und Vertraulichkeit

1. *Diensteanbieter sind auch im Rahmen ihrer Tätigkeit nach dieser Verordnung zur Achtung der Vertraulichkeit verpflichtet. Inhalte und sonstige Informationen, die einem Berufsgeheimnis wie etwa der anwaltlichen Verschwiegenheitspflicht unterliegen, dürfen nicht erhoben, gespeichert oder weitergegeben werden. Berufsgeheimnissen unterliegende Informationen dürfen auch anderen Stellen gegenüber nicht offenbart werden, gegenüber denen nach dieser Verordnung eine Pflicht zur Zusammenarbeit oder zum Datenaustausch besteht.*

2. *Mitarbeiter von Diensteanbietern sowie von deren Auftragnehmern unterliegen mit Blick auf nach dieser Verordnung erhobene oder übermittelte Informationen den Verschwiegenheitsanforderungen des Art. 339 AEUV; dies gilt auch für Organe, freie Mitarbeiter oder sonstige Beschäftigte.*
3. *Diensteanbieter haben geeignete Vorkehrungen zu treffen, um Offenbarungen von Informationen, die einem Berufsgeheimnis und namentlich dem anwaltlichen Mandatsgeheimnis unterliegen, zu verhindern. Dies gilt auch für Offenbarungen gegenüber eigenen Mitarbeitern. Sofern dem Diensteanbieter oder einem Beschäftigten gleichwohl derart geschützte Informationen zur Kenntnis gelangen, sind diese unverzüglich zu löschen. Der Diensteanbieter und die Beschäftigten sind in diesem Fall in gleicher Weise zur Verschwiegenheit verpflichtet, wie die betroffenen Berufsgeheimnisträger. Bestehen Zweifel über das Bestehen oder die Reichweite einer mitgliedstaatlichen Verschwiegenheitspflicht nehmen sie den Rat der in dem Mitgliedstaat zur Beurteilung des Bestehens einer Verschwiegenheitspflicht zuständigen berufsständischen Vertretung – etwa der Anwalts- oder Ärztekammer – in Anspruch.*
4. *Personenbezogene Daten sind vor jeder Weiterverarbeitung zu anonymisieren, sofern der Zweck der Verarbeitung dies zulässt.*

- **Art. 26 Abs. 5** sollte wie folgt um einen dritten Satz ergänzt werden:

„Artikel xx [hier Verweis auf vorgenannten Artikel] Abs. 1 und 3 gelten entsprechend.“

- In **Art. 74** sollte ein neuer Absatz 5 eingefügt werden:

„Artikel xx [hier ebenfalls Verweis auf den nach Artikel 24 neu vorgeschlagenen Artikel zur Verschwiegenheit] Abs. 1 und 3 gelten entsprechend. Inhalte, die einem Berufsgeheimnis unterliegen, dürfen insbesondere Mitgliedern der Leitungsebene gegenüber nicht offenbart werden, die zugleich anderen Institutionen und namentlich Europol angehören.“

- **Art. 40 Abs. 2** sollte wie folgt geändert werden:

*„Die EU-Zentralstelle trägt zur Verwirklichung des Ziels dieser Verordnung bei, indem sie die Umsetzung ihrer Bestimmungen über die Aufdeckung, Meldung, Beseitigung oder Sperrung des Zugangs zu sexuellem Kindesmissbrauch im Internet und die Sperrung des Zugangs dazu unterstützt und erleichtert, Informationen und Fachwissen sammelt und austauscht und die Zusammenarbeit zwischen den einschlägigen öffentlichen und privaten Stellen im Zusammenhang mit der Verhütung und Bekämpfung des sexuellen Kindesmissbrauchs, insbesondere im Internet, erleichtert. **Diese Zusammenarbeit darf nicht die Weitergabe von persönlichen oder inhaltlichen Informationen beinhalten, es sei denn, dies ist ausdrücklich vorgesehen oder rechtlich erforderlich. Informationen, die einem Berufsgeheimnis wie insbesondere der anwaltlichen Verschwiegenheit unterliegen, dürfen nicht offenbart werden.**“*

(Änderungen hervorgehoben)

- **Art. 40** sollte um den folgenden dritten Absatz erweitert werden:

„Für private Stellen im Sinne des Absatzes 2 gilt Art. xx [hier Verweis auf die am Ende des sechsten Abschnitts des zweiten Kapitels nach dem derzeitigen Artikel 24 einzufügende Verschwiegenheitsvorschrift – s.o.] entsprechend.“

- Die in den **Artt. 7 – 10** vorgesehene Verpflichtung zur Erkennung von Inhalten muss auch aus Gründen des Berufsgeheimnisschutzes ersatzlos gestrichen werden.
- **Hilfsweise:** Sollte der EU-Gesetzgeber sich über alle rechtsstaatlichen und praktischen Bedenken hinwegsetzen und die Erkennungsverpflichtung beibehalten werden, bedürfte es im Mindesten der folgenden Änderungen:
 - In **Art. 7 Abs. 4 Unterabsatz 1 lit. b** bedürfte es zumindest eines Hinweises auf Berufsgeheimnisse sowie einer abstrakten gesetzgeberischen Abwägungsentscheidung zugunsten derselben. Art. 7 Abs. 4 Unterabsatz 1 lit. b sollte dann wie folgt ergänzt werden:

*„(b) die Gründe für den Erlass der Aufdeckungsanordnung überwiegen die nachteiligen Folgen für die Rechte und berechtigten Interessen aller Betroffenen, wobei insbesondere ein angemessener Ausgleich zwischen den Grundrechten dieser Betroffenen zu gewährleisten ist. **Einblicke in und Erkennungen von Informationen, die einem Berufsgeheimnis unterliegen, dürfen nicht erfolgen und müssen sicher ausgeschlossen sein.**“*

(Hinzufügungen hervorgehoben)

- **Art. 7 Abs. 8** sollte wie folgt ergänzt werden:

*„Wenn die Koordinierungsbehörde des Niederlassungsortes um den Erlass von Aufdeckungsanordnungen ersucht bzw. die zuständige Justiz- oder unabhängige Verwaltungsbehörde die Aufdeckungsanordnung erlässt, richten sie diese so aus und präzisieren sie so, dass die in Abs. 4 Unterabsatz 1 Buchstabe b genannten negativen Folgen auf das beschränkt bleiben, was unbedingt erforderlich ist, um dem unter Buchstabe a genannten erheblichen Risiko wirksam zu begegnen. **Der in lit. b vorgesehene Schutz von Berufsgeheimnissen ist in jedem Fall zu gewährleisten. Ist dies nicht möglich, darf keine Erkennungsanordnung ergehen.**“*

(Hinzufügungen hervorgehoben)

- **Art. 10 Abs. 3** müsste um die folgende, neu einzufügende litera d) ergänzt werden:

„Offenbarungen von Informationen, die einem Berufsgeheimnis unterliegen, wirksam verhindern.“

- **Art. 10 Abs. 4 lit. a-b** müsste wie folgt ergänzt werden:

„4. Der Anbieter muss:

(a) alle erforderlichen Maßnahmen treffen, um sicherzustellen, dass die Technologien und Indikatoren sowie die Verarbeitung personenbezogener Daten und anderer Daten im Zusammenhang damit ausschließlich zum Zweck der Aufdeckung der Verbreitung von bekanntem oder neuem Material des sexuellen Missbrauchs von Kindern bzw. der Anwerbung von Kindern verwendet werden, soweit dies zur Ausführung der an ihn gerichteten Aufdeckungsaufträge unbedingt erforderlich ist;

(b) wirksame Maßnahmen zum Schutz von Mandatsgeheimnissen etablieren

(b) (c) wirksame interne Verfahren zur Verhinderung und erforderlichenfalls zur Aufdeckung des Missbrauchs der Technologien, Indikatoren und personenbezogenen Daten sowie anderer unter Buchstabe a genannter Daten, einschließlich des unbefugten Zugriffs auf und der unbefugten Weitergabe solcher personenbezogenen Daten und anderer Daten;“

(Änderungen hervorgehoben)

- **Art. 10 Abs. 5 Satz 1** müsste um die folgende neu einzufügende litera d) ergänzt werden:

„etwaig bestehende alternative Kommunikationswege, um vertraulich Rechtsrat in Anspruch zu nehmen.“

1.1.7 Verschärfung durch zu weite Definitionen und fehlende Ausnahmen

Verschärft werden diese grundlegenden Probleme durch zu weite Anwendungsbereichs- und Tatbestandsdefinitionen.

So ist der Anwendungsbereich in Art. 1 äußerst weit definiert. Ausnahmen etwa für den elektronischen Rechtsverkehr fehlen. Ferner erscheinen angesichts der weiten Definitionen der zu erkennenden, zu meldenden und vorzuhaltenden Inhalte und Parameter vergleichsweise eingriffsarme Erhebungen und Prüfungen, die nähere Befassungen mit den Inhalten nicht erfordern würden, nicht ausreichend, um die vorgesehenen Erkennungsverpflichtungen zu erfüllen. Anordnungen in den Artt. 7 – 10, die eine möglichst schonende Vorgehensweise – eher scheinbar – vorsehen, laufen damit ins Leere.

Im Einzelnen:

1.1.7.1 Bekannte Missbrauchsdarstellungen

In besonderem Maße abzulehnen ist zunächst die in Art. 2 lit. m enthaltene Definition bekannter Missbrauchsdarstellungen als bloß „potentielle“ Missbrauchsdarstellungen, die anhand der Indikatoren des Art. 44 Abs. 1 lit. a erkannt wurde. Eine derart weite Tatbestandsfassung läuft den primär- und verfassungsrechtlichen Erfordernissen der Anlassbezogenheit und der hinreichenden Risikokonkretisierung deutlich zuwider.

Änderungsvorschlag:

- **Art. 2 lit. m** ist wie folgt zu ändern:

*„bekanntes Material über den sexuellen Missbrauch von Kindern“: **potenzielles** Material über den sexuellen Missbrauch von Kindern, das anhand der Indikatoren in der Datenbank der Indikatoren nach Art. 44 Abs. 1 Buchstabe a ermittelt wurde;“*

1.1.7.2 Unbekannte Missbrauchsdarstellungen

Gleiches gilt – in noch erheblicherem Umfang – für den Einbezug auch unbekannter Missbrauchsdarstellungen in den Artt. 7 – 9 und deren wiederum viel zu weitgehende Definition in Art. 2 lit. n als ebenfalls „potentielle“ Missbrauchsdarstellung. Hinzukommt in diesem Zusammenhang, dass die Ermittlung

unbekannter Darstellungen eine eingehendere Auseinandersetzung mit den zu prüfenden Kommunikationsinhalten anhand einer größeren Anzahl von – überdies im Vergleich etwa zu Hashwerten bekannter Darstellungen weniger treffsichereren – Kriterien erfordern würde. Dadurch würde die Menge der betroffenen Kommunikationsinhalte noch einmal erheblich vergrößert und die Gefahr falsch-positiver Treffer zugleich deutlich erhöht.

Änderungsvorschläge:

- Art. 2 lit. n ist zu streichen.
- In den Artt. 7 – 9 sind die Bezugnahmen auf neue Missbrauchsdarstellungen und die spezifischen Regelungen derselben zu streichen.
- Art. 44 Abs. 1 lit. b ist zu streichen
- Alle weiteren Bezugnahmen auf und spezifische Regelungen im Umgang mit neuen Missbrauchsdarstellungen sind zu streichen.

1.1.7.3 Grooming-Kommunikation

Die Erkennung von Kontaktaufnahmen im Sinne von Art. 2 lit. o (sog. Grooming-Kommunikation) wird aufgrund der individuellen Prägung einer jeden Kontaktaufnahme in besonderem Maße eine Auseinandersetzung mit Kommunikationsinhalten auch betreffend darin gewählter Formulierungen und Kontexte erfordern. Eine einigermaßen schonende, abstrakte Prüfung und Einordnung – etwa anhand von Hashwerten – erscheint daher kaum möglich. Insbesondere die in Art. 36 Abs. 1 lit. a vorgesehene Übermittlung von Konversationstranskripten wird eine inhaltliche Auseinandersetzung mit der Korrespondenz erfordern; Art. 44 Abs. 2 lit. c gibt dementsprechend bereits vor, dass „Sprachidentifikatoren“ („language identifiers“) vorzuhalten seien. Angesichts derartiger Vertraulichkeitsbeeinträchtigungen ist jegliche Pflicht zur Erkennung von Grooming-Kommunikationen abzulehnen.

Änderungsvorschlag:

- Art. 7 Abs. 1 sollte wie folgt geändert werden:

*„Die Koordinierungsbehörde ist befugt, das zuständige Gericht des Mitgliedstaats, in dem sie benannt wurde, ~~oder eine andere unabhängige Verwaltungsbehörde dieses Mitgliedstaats~~ zu ersuchen, eine Aufdeckungsanordnung zu erlassen, mit der ein Anbieter von Hosting-Diensten oder ein Anbieter von interpersonellen Kommunikationsdiensten, der der Rechtshoheit dieses Mitgliedstaats unterliegt, verpflichtet wird, die in Artikel 10 genannten Maßnahmen zu ergreifen, um den sexuellen Online-Missbrauch von Kindern in einem bestimmten Dienst aufzudecken. **Nicht öffentliche einsehbare Inhalte dürfen nicht auf Kontaktaufnahmen im Sinne von Art. 2 lit. o hin überprüft werden.**“*

(Hinzufügungen hervorgehoben)

- In den Artt. 7 – 8 sollten sämtliche Bezugnahmen auf Kontaktaufnahmen bzw. spezifische Regelungen derselben gestrichen werden.

1.1.7.4 Ausschluss des elektronischen Rechtsverkehrs

Nach dem Verständnis der Bundesrechtsanwaltskammer sind Systeme des elektronischen Rechtsverkehrs, das heißt solche, die einzig zum Zwecke der Kommunikation zwischen Rechtsanwälten, Gerichten, Behörden und Mandanten bzw. Verfahrensparteien eingerichtet sind, weder von der Definition eines Hosting-Dienstes gemäß Art. 2 lit. a noch von der eines öffentlichen interpersonellen Kommunikationsdienstes gemäß Art. 2 lit. b umfasst. Zur Vermeidung von Missverständnissen und unnötigen Belastungen sollte gleichwohl klargestellt werden, dass die Verordnung auf Anbieter solcher Dienste nicht anwendbar ist. Denn es ist bereits absehbar, dass die in dem Entwurf vorgesehenen Verpflichtungen in Bezug auf Anbieter solcher Dienste unter keinem rechtlichen Gesichtspunkt zu rechtfertigen wären. Solche Dienste werden nicht zur Verbreitung von Missbrauchsdarstellungen oder zur Anwerbung von Kindern genutzt. Zudem verbieten der Grundsatz des Zugangs zum Recht sowie die im Bereich des elektronischen Rechtsverkehrs geltenden besonderen Vertraulichkeitsverpflichtungen wie namentlich das Mandatsgeheimnis sowie nicht zuletzt die anwaltliche und justizielle Unabhängigkeit eine Verpflichtung zur Erkennung von Inhalten ebenso wie die diesbezüglich vorgesehene Beaufsichtigung durch die Koordinierungsbehörden.

Änderungsvorschlag:

- **Art. 1 Abs. 2** der sollte daher wie folgt ergänzt werden:

*„Diese Verordnung gilt für Anbieter einschlägiger Dienste der Informationsgesellschaft, die diese Dienste in der Union anbieten, unabhängig vom Ort ihrer Hauptniederlassung. **Sie gilt nicht für Anbieter von Systemen des elektronischen Rechtsverkehrs, das heißt solcher Systeme, die spezifisch zum Zwecke der Kommunikation zwischen Rechtsanwälten, Gerichten, Behörden und Mandanten bzw. Verfahrensparteien eingerichtet wurden.**“*

(Hinzufügungen hervorgehoben)

1.1.8 Nachgelagerte Risiken durch Erhebung, Sammlung und Austausch von Informationen

Im Interesse der Missbrauchsbekämpfung werden im Verordnungsentwurf bezüglich der zu erkennenden Inhalte zahlreiche sich anschließende Erhebungen, Sammlungen und Austausche von Informationen vorgesehen (so in Art. 37, Art. 38, Art. 39 Abs. 1, Art. 40 Abs. 2, Art. 43 Abs. 1 lit. a, Abs. 2 lit. b und c, Abs. 3 lit. a und b, Abs. 5 lit. c, d und f, Abs. 6 lit. a, Art. 46 Abs. 2, Abs. 3, Abs. 4, Abs. 5, Abs. 7, Art. 48 Abs. 3, Art. 50 Abs. 2 lit. a, Art. 53 Abs. 2, Art. 54 Abs. 1, Art. 83). Neben der vorgelagerten Erkennung durch die Anbieter sind diese Vorgänge ihrerseits mit weiteren Vertraulichkeitsbeeinträchtigungen verbunden, bezüglich derer ebenfalls auf eine Wahrung von Grund- und Verfassungsrechten sowie des Verhältnismäßigkeitsgrundsatzes zu achten ist. Insbesondere muss auch und gerade bei diesen Vorgängen der Schutz von Berufsgeheimnissen gewährleistet werden. Dabei ist zu berücksichtigen, dass die Rechte der Betroffenen umso stärker beeinträchtigt werden, je länger die Inhalte aufbewahrt, je umfangreicher sie mit anderen Akteuren geteilt und je leichter sie mit anderen Daten verknüpft werden können. Insbesondere für Opfer und Täter sexuellen Missbrauchs, die sich anwaltlich über die der Verordnung unterfallende Dienste beraten lassen, können rechtsstaatlich und persönlichkeitsrechtlich unter keinen Umständen zu rechtfertigende Beeinträchtigungen entstehen, wenn Daten an andere Akteure und insbesondere Strafverfolgungsbehörden, Europol oder Gerichte weitergegeben werden. Dies gilt aber auch für Mandanten, die keiner dieser Gruppen angehören, deren Mandatskommunikation aber als falsch-positiver Treffer erfasst und ggf. weitergeleitet wird. Vor diesem Hintergrund sind die entsprechenden Informationserhebungs-, Sammlungs-, und Austauschpflichten auf ein absolut erforderliches Minimum zu beschränken und vor jeder Weitergabe eine gewissenhafte Prüfung des Materials

vorzusehen. Insoweit besteht jedoch der Zielkonflikt, dass eine gewissenhafte Prüfung regelmäßig auch nähere Beschäftigung mit dem Material sowie einen menschlichen Einblick erfordern dürfte, wodurch seinerseits Beeinträchtigungen von Grund- und Verfassungsrechten sowie des Mandatsgeheimnisses begründet wären. Um der so programmierten Wiederholung von Beeinträchtigungen von Grund- und Verfassungsrechten entgegenzuwirken, müssen daher bereits auf der vorgelagerten Ebene der Erkennung durch die Diensteanbieter größtmögliche Begrenzungen der zu erfassenden Inhalte vorgenommen bzw. auf diese verzichtet werden. Wo dies nicht möglich ist, sollten Folgebeeinträchtigungen durch die nachstehenden Maßnahmen begrenzt werden.

1.1.8.1 Achtung von Verschwiegenheitspflichten bei nachfolgenden Verarbeitungsvorgängen

Es bedarf zunächst der bereits in den Änderungsvorschlägen zu 1.1.6 zu einem hinter Art. 24 neu einzufügenden Artikel enthaltenen Klarstellung, dass die Erhebung oder Sammlung von Inhalten und Informationen, die einem Berufsgeheimnis und insbesondere dem anwaltlichen Mandatsgeheimnis unterliegen, ausgeschlossen ist, und dass diese anderen Akteuren gegenüber auch dann nicht offenbart werden dürfen, wenn ein Datenaustausch nach dieser Verordnung vorgesehen ist.

1.1.8.2 Keine Weiterverarbeitungsbefugnis beim Diensteanbieter

Ferner muss die nach dem derzeitigen Wortlaut von Art. 22 Abs. 1 Unterabsatz 2 Satz 2 mögliche Nutzung mandatsbezogener Informationen zur Produktverwendung klarstellend auch dort ausgeschlossen werden.

Änderungsvorschlag:

- **Art. 22 Abs. 1 Unterabsatz 2 Satz 2** sollte wie folgt ergänzt werden

*„Er darf jedoch keine personenbezogenen Daten **oder solche, die einem Berufsgeheimnis unterliegen, zu diesem Zweck speichern.**“*

(Änderungen hervorgehoben)

1.1.8.3 Kein Sammeln und Reporting von Mandatsinformationen

Es muss klargestellt werden, dass die derzeit in Art. 83 bzw. 84 für Diensteanbieter vorgesehenen Datenspeicherungs- bzw. Reporting-Verpflichtungen keine Mandatsinformationen umfasst.

Änderungsvorschläge:

- **Art. 83 Abs. 4 Satz 2** sollte wie folgt ergänzt werden:

*„Die gespeicherten Daten dürfen keine personenbezogenen Daten **oder solche, die einem Berufsgeheimnis unterliegen, enthalten.**“*

(Änderungen hervorgehoben)

- **Art. 84 Abs. 5 Satz 2** sollte wie folgt ergänzt werden:

*„Sie dürfen auch keine personenbezogenen Daten **oder solche, die einem Berufsgeheimnis unterliegen, enthalten.**“*

(Änderungen hervorgehoben)

1.1.8.4 Beschränkung der Kooperationsbefugnisse

Es bedarf einer Klarstellung, dass die teils vage formulierten Kooperationsbefugnisse bzw. -gebote nach der Verordnung (vgl. Art. 38 Abs. 1, 39 Abs. 1, 40 Abs. 2, 43 Abs. 1 a) keine über die explizit darin vorgesehenen Befugnisse hinausgehende Befugnis zur Erhebung, Sammlung oder Weitergabe von erkannten Inhalten beinhalten.

Änderungsvorschläge:

- **Am Ende des vierten Abschnitts des dritten Kapitels nach dem derzeitigen Art. 39** sollte daher der folgende zusätzliche Artikel eingefügt werden:

„Artikel xx

Beschränkungen

„Den Kooperationsbefugnissen bzw. -geboten nach dieser Verordnung und insbesondere den Artikeln 38 Abs. und 39 Abs. 1 ist keine, über die explizit in der Verordnung vorgesehenen Befugnisse hinausgehende Befugnis zur Erhebung, Sammlung oder Weitergabe von erkannten Inhalten zu entnehmen.“

- **Am Ende des vierten Abschnitts des vierten Kapitels nach dem derzeitigen Art. 54** sollte ferner der folgende Artikel aufgenommen werden:

„Artikel xx

Beschränkungen

„Artikel xx [hier Verweisung auf den vorgenannten Artikel am Ende des vierten Abschnitts des dritten Kapitels nach dem derzeitigen Artikel 39] gilt auch für Kooperationen nach diesem Abschnitt.“

1.1.8.5 Vermeidung von Personenbezügen

Schließlich bedarf es zur Vermeidung nachgelagerter Risiken der ebenfalls bereits in den Änderungsvorschlägen unter 1.1.6 zu einem hinter Art. 24 neu einzufügenden Artikel vorgeschlagenen Klarstellung, dass jegliche Erhebung, Sammlung oder Weitergabe von Inhalten oder Informationen, soweit möglich und mit dem Zweck vereinbar, ohne Bezug zu natürlichen Personen erfolgen muss und dass hierzu im Rahmen des Möglichen auch Anonymisierungen erfolgen müssen.

1.1.9 Menschliche Aufsicht (human oversight)

Der Entwurf sieht in Art. 10 Abs. 4 lit. c) die Implementierung einer menschlichen Aufsicht (human oversight) für automatisierte Erkennungsprozesse vor. Angesichts der potenziell einschneidenden Auswirkungen, die falsch-positive Treffer auf die Rechte und Interessen der Betroffenen haben können und angesichts der Fehleranfälligkeit und Voreingenommenheit vieler automatisierter Erkennungsprozesse ist dieses Erfordernis – als lediglich zweitbeste Lösung zum eigentlich gebotenen Verzicht auf Erkennungsmaßnahmen – im Grundsatz zu begrüßen. Zu beachten ist allerdings, dass hierdurch zugleich Offenbarungen von Inhalten gegenüber Mitarbeitern der jeweiligen Diensteanbieter bzw. Institutionen

befördert werden. Zudem steht dieses Erfordernis einer, zumindest auf der ersten Erhebungsebene, vergleichsweise eingriffsarmen Erkennung – etwa anhand von Hashwerten – entgegen. Ein hinreichender Vertraulichkeitsschutz kann angesichts dieses Dilemmas nur durch ein Absehen von der Erkennung insgesamt erzielt werden. Wo indes in Ermangelung eines Erhebungsverbots auf erster Ebene zur Vermeidung schlimmerer Folgen eine menschliche Aufsicht sinnvollerweise zum Einsatz kommt, muss die Vertraulichkeit der Inhalte durch weitreichende Verschwiegenheitsverpflichtungen geschützt werden. Dies gilt insbesondere mit Blick auf die Einbindung privater Akteure (s. dazu oben unter 1.1.4).

Änderungsvorschlag:

- **Art. 10 Abs. 4 lit. c)** sollte daher wie folgt ergänzt werden:

„eine regelmäßige menschliche Aufsicht gewährleisten, um sicherzustellen, dass die Technologien hinreichend zuverlässig funktionieren und erforderlichenfalls, insbesondere wenn potenzielle Fehler und eine mögliche Anwerbung von Kindern festgestellt werden, menschlich eingegriffen wird; es gelten die Verschwiegenheitsverpflichtungen des Art. xx [Verweis auf den am Ende des sechsten Abschnitts des zweiten Kapitels nach dem derzeitigen Art. 24 einzufügenden Artikel zur Vertraulichkeit – siehe Änderungsvorschläge unter 1.1.6 Insbesondere: fehlender Schutz von Berufsgeheimnissen]“;

(Änderungen hervorgehoben)

1.2 Ausschluss von Erkennungsmaßnahmen auf freiwilliger Basis und Richtervorbehalt

Art. 4 des Entwurfs verpflichtet Anbieter interpersoneller Kommunikationsdienste sowie von Hosting-Diensten zur Risikominimierung. In diesem Zusammenhang bedarf es einer Klarstellung, dass Maßnahmen zur Inhaltserkennung nicht ergriffen werden dürfen. Sofern der EU-Gesetzgeber trotz aller rechtsstaatlichen und sachlichen Bedenken an der Erkennungsverpflichtung gemäß Artt. 7 – 10 festhalten sollte, bedürfte es zumindest einer Klarstellung, dass Erkennungsmaßnahmen keinesfalls auf freiwilliger Basis erfolgen dürfen. Angesichts der mit dieser Maßnahme verbundenen einschneidenden Grundrechtsbeeinträchtigung bedarf es darüber hinaus eines unbedingten Richtervorbehaltes; die alternative Anordnung durch eine sonstige Verwaltungsbehörde, wie derzeit vorgesehen, ist nicht ausreichend.

Änderungsvorschläge:

- In **Art. 4 Abs. 1** sollte daher ein dritter Satz mit folgendem Inhalt eingefügt werden.

„Maßnahmen zur Inhaltserkennung dürfen nicht ergriffen werden.“

- Sofern an der Erkennungsverpflichtung gemäß Artt. 7 – 10 festgehalten werden sollte, sollte es an gleicher Stelle alternativ heißen:

„Maßnahmen zur Inhaltserkennung dürfen nur auf richterliche Anordnung und ausschließlich unter den Voraussetzungen der Artt. 7 – 10 ergriffen werden.“

- In **Art. 7 Abs. 1** sollten die Worte „oder eine andere unabhängige Verwaltungsbehörde dieses Mitgliedstaats“ gestrichen werden.

2. Altersprüfung

Die in Erwägungsgrund 28, Art. 3 Abs. 2 lit. b) Spiegelstrich 3, Art. 4 Abs. 3, und Art. 6 Abs. 1 lit. c) des Entwurfs vorgesehenen Verpflichtungen zur Durchführung einer Altersverifikation bergen Risiken für den Zugang zum Recht. So steht zum einen – insbesondere mit Blick auf Art. 4 Abs. 3 – zu befürchten, dass Rechtsuchende aufgrund der mit den meisten Altersverifikationsmethoden einhergehenden Identifizierungsmöglichkeiten fürchten, bei der Inanspruchnahme von Rechtsrat erkannt zu werden, und daher von dieser Abstand nehmen. Zum anderen könnten Minderjährige durch Altersverifikationserfordernisse von der Nutzung von Kommunikationsdiensten – und damit von der Inanspruchnahme von Rechtsrat über dieselben – ausgeschlossen werden. Beides gilt es durch konkretisierende Beschränkungen der Anspruchsvoraussetzungen zu verhindern. Hierfür streiten neben der Möglichkeit der Inanspruchnahme von Rechtsrat auch allgemeinere Teilhabegesichtspunkte. Zweckmäßiger Weise sollte die Verpflichtung zur Altersverifikation daher auf solche Dienste beschränkt werden, die ihrer Natur gemäß erhöhte Risiken bergen – wie etwa Dating-Plattformen. Demgegenüber sollten allgemeine Kommunikationsdienste und unspezifisch ausgerichtete Social-Media-Plattformen explizit vom Erfordernis der Altersverifikation ausgenommen werden.

Änderungsvorschläge:

- **Art. 4 Abs. 3** sollte wie folgt geändert werden:

*„Anbieter interpersoneller Kommunikationsdienste, die gemäß der nach Artikel 3 durchgeführten oder aktualisierten Risikobewertung ein Risiko der Nutzung ihrer Dienste zum Zwecke der Anwerbung von Kindern festgestellt haben, **das in der Art ihres Dienstes angelegt ist**, ergreifen die erforderlichen Maßnahmen zur Altersüberprüfung und -bewertung, um die Nutzer im Kindesalter zuverlässig zu identifizieren, wie dies bei Dating-Diensten in ihren Diensten der Fall sein könnte, und so in die Lage zu versetzen, die erforderlichen Abhilfemaßnahmen zu treffen. **Dies gilt nicht für Kommunikationsdienste mit allgemeinem Zuschnitt und insbesondere nicht für solche, von denen vernünftigerweise angenommen werden kann, dass Nutzer sich darüber von einem Rechtsanwalt beraten lassen oder anderweitig besonders gewichtige Grundrechte darüber ausüben.**“*

(Änderungen hervorgehoben)

- **Art. 6 Abs. 1 lit. c)** sollte wie folgt geändert werden:

*„die erforderlichen Maßnahmen zur Altersüberprüfung und -bewertung ergreifen, um die Nutzer ihrer Dienste im Kindesalter zuverlässig zu identifizieren, damit sie die unter Buchstabe b genannten Maßnahmen ergreifen können. **Aufgrund von Risiken, die nicht in der Natur des jeweiligen Dienstes liegen, und für den Zugang zu Kommunikationsdiensten mit allgemeinem Zuschnitt und insbesondere zu solchen, von denen vernünftigerweise angenommen werden kann, dass Nutzer sich darüber von einem Rechtsanwalt beraten lassen oder anderweitig besonders gewichtige Grundrechte darüber ausüben, dürfen Maßnahmen zur Altersüberprüfung nicht angewendet werden.**“*

3. Behördliche Aufsicht

Der Entwurf sieht eine unabhängige Aufsicht mit Parallelen zum EU-Datenschutz-Regime vor.

3.1 Aufsichtsbefugnisse

Die in Art. 27 Abs. 1 lit. a und b vorgesehenen Aufsichtsbefugnisse bergen das Risiko, dass Aufsichtsmaßnahmen gegenüber Rechtsanwältinnen und Rechtsanwälten ergehen und so Mandatsgeheimnisse offenbart werden.

So soll die Aufsichtsbehörde gemäß Art. 27 Abs. 1 lit. a) neben den eigentlich verpflichteten Diensteanbietern Auskünfte auch von allen anderen Personen verlangen können, „die im Rahmen ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handeln und nach vernünftigem Ermessen Kenntnis von Informationen über einen mutmaßlichen Verstoß gegen diese Verordnung haben können“. Demnach könnten auch Rechtsanwältinnen oder Rechtsanwälte, die Diensteanbieter beraten zur Auskunft über Mandatsinhalte herangezogen werden, was mit dem Mandatsgeheimnis nicht zu vereinbaren wäre.

Darüber hinaus sind in Art. 27 Abs. 1 lit. b) Vorort-Untersuchungen mit einer Befugnis zur Kopie und Beschlagnahme von Informationen – ungeachtet von der Natur des Datenträgers – vorgesehen. Dies birgt die Gefahr, dass etwa gehostete Akteninhalte oder anwaltliche Korrespondenzen beschlagnahmt und den Aufsichtsbehörden offenbart werden. Auch dies ist weder mit dem Mandatsgeheimnis noch der anwaltlichen Unabhängigkeit vereinbar.

Entsprechende Beeinträchtigungen des Mandatsgeheimnisses und der anwaltlichen Unabhängigkeit müssen dringend durch entsprechende Beschränkungen der Aufsichtsbefugnis verhindert werden. Bei deren Ausgestaltung bietet sich angesichts der gesetzgeberischen Kompetenzverteilung in systematischer Hinsicht eine Orientierung an den datenschutzrechtlichen Normen des Art. 90 Abs. 1 DS-GVO bzw. des § 29 BDSG an. Dabei gilt es inhaltlich jedoch zu beachten, dass diese Normen sich in der Praxis als unzureichend erwiesen haben. So musste festgestellt werden, dass Aufsichtsbehörden ihre durch diese Vorschriften nicht ausgeschlossene Befugnis, gemäß Art. 58 Abs. 1 lit. a DS-GVO Auskunft zu verlangen, zu Befragungen zu Mandatshinhalten nutzten. Die Befugnisbeschränkung muss daher insoweit umfassender erfolgen und der Tatsache Rechnung tragen, dass ein Bruch der anwaltlichen Verschwiegenheit regelmäßig nicht zu rechtfertigen ist.

Änderungsvorschlag:

- **Art. 27** sollte daher wie folgt um einen dritten Absatz ergänzt werden:

„Aufsichtsmaßnahmen gegenüber Berufsgeheimnisträgern sind unzulässig. Die Mitgliedstaaten können die Befugnisse der Aufsichtsbehörden im Übrigen abweichend regeln und weiter einschränken, soweit dies notwendig ist, um den Schutz von Berufsgeheimnissen und gleichwertigen Verschwiegenheitspflichten zu gewährleisten. Jeder Mitgliedstaat teilt der Kommission bis zum xx.xx.20xx die Vorschriften mit, die er aufgrund von Satz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.“

3.2 Verschwiegenheit

Die in Art. 26 des Entwurfs vorgesehene Verschwiegenheit der Aufsicht muss beibehalten werden und wie oben unter 1.1.6 Insbesondere: fehlender Schutz von Berufsgeheimnissen vorgeschlagen ergänzt werden.

4. Verschwiegenheit der Zentralstelle

Die in Art. 74 des Entwurfs vorgesehene Verschwiegenheit der Aufsicht muss beibehalten werden und wie oben unter 1.1.6 Insbesondere: fehlender Schutz von Berufsgeheimnissen vorgeschlagen insbesondere um eine Verschwiegenheitspflicht gegenüber doppelunktionalen Führungspersonen im Sinne der Art. 56 und 61 ergänzt werden, um zu vermeiden, dass vertrauliche Informationen durch Personenidentität faktisch einer anderen Stelle und insbesondere Europol gegenüber offenbart werden.

5. Verhältnis zum übrigen Datenschutzrechtsregime und Datenschutz-Folgenabschätzung

Art. 1 Abs. 3 lit. d erklärt die Geltung des bestehenden Datenschutzrechtsregimes zustimmungswürdiger Weise für unberührt. Indes sieht Art. 7 Abs. 3 Unterabsatz 2 Satz 2 lit. b eine Datenschutz-Folgenabschätzung nur für Fälle der Erkennung einer Kontaktaufnahme vor, obwohl eine Risikoabschätzung im Rahmen des – ohnehin anwendbaren – Art. 35 auch hinsichtlich der Erkennung von Missbrauchsinhalten zu dem Ergebnis regelmäßig führen wird, dass eine Datenschutz-Folgenabschätzung durchgeführt werden muss. Die Klarstellung des Art. 7 Abs. 3 Unterabsatz 2 Satz 2 lit. b sollte daher auch auf Fälle der Erkennung von Missbrauchsinhalten ausgeweitet werden. Anderenfalls könnte bei Rechtsanwenden der falsche und unbedingt zu vermeidende Eindruck entstehen, dass eine Datenschutz-Folgenabschätzung in diesen Fällen entbehrlich sei.

Änderungsvorschlag:

- **Art. 7 Abs. 3 Unterabsatz 2 Satz 2 lit. b** sollte daher wie folgt geändert werden:

„(b) wenn der Entwurf des Durchführungsplans eine beabsichtigte Aufdeckungsanordnung ~~in Bezug auf die Anwerbung von Kindern~~ betrifft, bei der es sich nicht um die Verlängerung einer zuvor ergangenen Aufdeckungsanordnung ohne wesentliche Änderungen handelt, eine Datenschutz-Folgenabschätzung und ein vorheriges Konsultationsverfahren gemäß Artikel 35 bzw. Artikel 36 der Verordnung (EU) 2016/679 in Bezug auf die im Durchführungsplan dargelegten Maßnahmen durchführen;“

6. Evaluation

Art. 85 sieht eine Evaluation der Verordnung alle 5 Jahre vor. Gemäß Erwägungsgrund 77 sollen dabei insbesondere die Auswirkungen auf Vertraulichkeitsgrundrechte beleuchtet werden. Der vorliegende Entwurf verdeutlicht, wie erforderlich es ist, Entscheidungsträgern die Bedeutung des Mandatsgeheimnisses in diesem Regelungszusammenhang vor Augen zu führen. Aus diesem Grund sollte das Mandatsgeheimnis in einer etwaigen Verordnung explizit als Evaluationskriterium aufgeführt werden.

Änderungsvorschlag:

- Erwägungsgrund 77 sollte daher wie folgt ergänzt werden:

„Die Bewertung soll anhand der Kriterien der Effizienz, Notwendigkeit, Wirksamkeit, Verhältnismäßigkeit, Relevanz, Kohärenz und des Mehrwerts für die Union vorgenommen werden. Sie sollte das Funktionieren der verschiedenen in dieser Verordnung vorgesehenen operativen und technischen Maßnahmen bewerten, einschließlich der Wirksamkeit der Maßnahmen zur Verbesserung der Aufdeckung, Meldung und Beseitigung von sexuellem Missbrauch von Kindern im Internet, der Wirksamkeit der Schutzmechanismen sowie der Auswirkungen auf potenziell betroffene Grundrechte, die unternehmerische Freiheit, das Recht auf Privatleben,

*~~und~~ den Schutz personenbezogener Daten **und Berufsgeheimnisse**. Die Kommission sollte auch die Auswirkungen auf potenziell betroffene Interessen Dritter bewerten.“*

7. Alternative Ansätze

Die Bundesrechtsanwaltskammer spricht sich für den Rückgriff auf andere Methoden zur Bekämpfung des online-Kindesmissbrauchs aus. In erster Linie muss eine verstärkte Aufklärungsarbeit unter Einbeziehung von Akteuren wie Sozialarbeitern, Betroffenenhilfe, Schulen sowie Ärztinnen und Ärzten stattfinden.

Begrüßenswert ist der Vorschlag im EP-Berichtsentwurf für ein Victims' Consultative Forum (ÄA 273 für einen neuen Art. 66 a), das in diesem Zusammenhang eine Rolle spielen könnte.

Angeregt werden ferner Meldekanäle bzw. Beschwerdesysteme gerade auch für jugendliche Nutzer, so dass diese Inhalte vertraulich melden und dagegen vorgehen können.

Grundsätzlich ist eine Beschränkung auf gezielte Einzelfallmaßnahmen infolge entsprechender Ermittlungen und auf richterliche Anordnung der vorzugswürdige Ansatz.

* * *

Von: [REDACTED] - IIIB7 - <[REDACTED]@bmj.bund.de>
An: E-Post-RegIII <E-Post-RegIII@bmj.bund.de>
Gesendet am: 23.05.2023 09:36:18
Betreff: WG: DAV-Stellungnahme Nr. 32/2023 zum Vorschlag einer EU-Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSAM)

Bitte verakten.

[REDACTED]
- III B 7 -
[REDACTED]

-----Ursprüngliche Nachricht-----

Von: [REDACTED]@bmj.bund.de> Im Auftrag von Referat IIA7
Gesendet: Dienstag, 16. Mai 2023 12:31
An: [REDACTED] - IIIB7 - <[REDACTED]@bmj.bund.de>; Referat IIIB7 <IIIB7@bmj.bund.de>
Cc: [REDACTED] <[REDACTED]@bmj.bund.de>; [REDACTED]@bmj.bund.de>
Betreff: WG: DAV-Stellungnahme Nr. 32/2023 zum Vorschlag einer EU- Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSAM)

IIA7

[REDACTED]
liebe Kolleginnen und Kollegen,

der beiliegende Vorgang dürfte in Ihre Zuständigkeit fallen. Für eine Übernahme wäre ich daher dankbar.

Beste Grüße
[REDACTED]

[REDACTED]
[REDACTED]
II A 7 - Sexualstrafrecht; Kriminologie; Strafrechtliche Bekämpfung von Doping; Statistiken der Strafrechtspflege
[REDACTED]

-----Ursprüngliche Nachricht-----

Von: Poststelle BMJ <Poststelle@bmj.bund.de>
Gesendet: Dienstag, 16. Mai 2023 11:02
An: Referat IIA7 <IIA7@bmj.bund.de>
Betreff: WG: DAV-Stellungnahme Nr. 32/2023 zum Vorschlag einer EU- Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSAM)

Von: [REDACTED] (DAV) <[REDACTED]@anwaltverein.de> Im Auftrag von [REDACTED] (DAV)
Gesendet: Dienstag, 16. Mai 2023 09:50
Betreff: DAV-Stellungnahme Nr. 32/2023 zum Vorschlag einer EU- Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSAM)

Sehr geehrte Damen und Herren,

anbei übermittele ich Ihnen die Stellungnahme des Deutschen Anwaltvereins (DAV) durch den Ausschuss Gefahrenabwehrrecht zum Vorschlag einer EU- Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSAM) und zum Berichtsentwurf im Europäischen Parlament.

Der DAV unterstützt das Ziel des Verordnungsentwurfs; die Bekämpfung der Verbreitung von Kindesmissbrauchsmaterial im Internet ist ein wichtiges Anliegen. Es ist daher ein begrüßenswerter Schritt, dass innerhalb der EU die Zusammenarbeit und Koordinierung von Strafverfolgungsbehörden der Mitgliedstaaten verbessert werden sollen. Ebenfalls zuzustimmen ist dem Verordnungsentwurf insoweit, als dass die Löschung strafbarer Inhalte, die beispielsweise aufgrund von Hinweisen identifiziert worden sind, einheitlich geregelt wird. Dies schafft Rechtssicherheit für die Diensteanbieter über die Grenzen der Mitgliedstaaten hinweg.

Im Übrigen begegnet der Entwurf jedoch trotz seines wichtigen Anliegens erheblichen rechtsstaatlichen Bedenken. Er läuft auf eine Abschaffung der Ende-zu-Ende-Verschlüsselung und eine automatisierte, massenhafte Analyse von Kommunikations(inhalts-)daten aller Nutzer von bspw. Email-, Messenger- und Chat-Anwendungen, sozialen Medien oder auch Cloud-Speicherdiensten hinaus.

Dabei ist nicht nur mit einer hohen Zahl an falschen Treffern zu rechnen, die eine nähere Betrachtung höchstprivater Kommunikationsinhalte nach sich ziehen würden. Zwangsläufig wäre auch das anwaltliche Berufsgeheimnis beeinträchtigt. Der tatsächliche Nutzen für die Bekämpfung der Verbreitung von Kindesmissbrauchsmaterial wäre indes angesichts von Ausweichmöglichkeiten ins sog. Dark-Net fraglich.

Die kürzlich vom Berichterstatter des LIBE-Ausschusses im Europäischen Parlament vorgeschlagenen Änderungen sind nicht geeignet, die gegen das Instrument der Aufdeckungsanordnung vorgebrachte Kritik zu entkräften. Die vorgeschlagene Ergänzung des Verordnungsentwurfs um eine Befugnis zur freiwilligen Auswertung von Kommunikationsinhalten durch Diensteanbieter, ohne dass es einer entsprechenden Anordnung bedürfte, begegnet zudem im Kern denselben rechtlichen Bedenken wie das Instrument der Aufdeckungsanordnung.

Weitere Einzelheiten entnehmen Sie bitte der beigegeführten, ausführlich begründeten DAV-Stellungnahme Nr. 32/2023.

Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der

Bundesregierung zur Registernummer R000952

<https://www.lobbyregister.bundestag.de/suche/R000952/3812?backUrl=%2Fsuche%3Fq%3DDeutscher%2BAnwaltverein%26page%3D1%26pageSize%3D10%26sort%3DREGISTRATION_DESC> eingetragen.

Mit freundlichen Grüßen

██████████
Syndikusrechtsanwalt
Geschäftsführer

Deutscher Anwaltverein
Rechtsanwalt ██████████

Geschäftsführer

Littenstraße 11, 10179 Berlin

Tel. ██████████ ██████████
██████████@anwaltverein.de <mailto:██████████@anwaltverein.de>

Assistenz: ██████████

Tel. ██████████ ██████████

Fax ██████████ ██████████

www.anwaltverein.de <<http://www.anwaltverein.de>> [facebook.com/deutscheranwaltverein](https://www.facebook.com/deutscheranwaltverein)
<[http://www.facebook.com/deutscheranwaltverein](https://www.facebook.com/deutscheranwaltverein)>
twitter.com/anwaltverein <[http://www.twitter.com/anwaltverein](https://twitter.com/anwaltverein)>

Deutscher Diversity Tag 2023. Wir sind dabei!

+++

Denken Sie bitte an die Umwelt, bevor Sie diese E-Mail ausdrucken.

+++

Von: [REDACTED]@google.com>
An: [REDACTED] - IIIB7 - <[REDACTED]@bmj.bund.de>;
[REDACTED] <[REDACTED]@bmj.bund.de>
CC: [REDACTED] <[REDACTED]@google.com>
Gesendet am: 31.08.2023 15:03:13
Betreff: [CSA-VO] Feedback zu Entwicklungen im Rat der EU

[REDACTED]

ich hoffe, Sie hatten einen angenehmen Sommer. Angesichts der fortschreitenden Diskussionen im Rat der EU möchte ich Googles Feedback zu den jüngsten Vorschlägen der spanischen Ratspräsidentschaft zur CSA-Verordnung teilen.

Ich möchte außerdem die Gelegenheit nutzen, um [REDACTED] mit Ihnen zu verbinden, [REDACTED] dieses Thema von mir übernehmen wird. Vielen Dank für die gute Zusammenarbeit zu diesem komplexen und wichtigen Thema!

Unsere Kommentare erstrecken sich auf den Anwendungsbereich, Risikobewertungen, Maßnahmen zur Risikominderung und Aufdeckungsanordnungen. Im Anhang finden Sie einige Änderungsvorschläge zu diesen Schlüsselbereichen.

Risikobewertungen

- Die Anforderung, Risikobewertungen durchzuführen, sollte nur für jene Dienste gelten, die ein hohes Risiko des sexuellen Missbrauchs von Kindern im Internet darstellen. Es sollte vermieden werden, wertvolle Ressourcen von Behörden und Anbietern in Produkte fließen zu lassen, die, wenn überhaupt, nur ein geringes Risiko für die Verbreitung von Material über sexuellen Kindesmissbrauch bergen (z. B. Flugbuchungen, Zahlungsseiten, Kartendienste usw.).
- Um sicherzustellen, dass die Ressourcen der Aufsichtsbehörden und der Unternehmen so effizient wie möglich eingesetzt werden, schlagen wir daher vor, sich auf Dienste zu konzentrieren, die für den sexuellen Missbrauch von Kindern und die Verbreitung von Missbrauchsdarstellungen genutzt werden können. Wir schlagen außerdem vor, klarzustellen, dass die jährliche DSA-Risikobewertung für illegale Inhalte, die von VLOPs/VLOSEs verlangt wird, als Basis verwendet werden kann, ergänzt durch zusätzliche Maßnahmen im Rahmen des Entwurfs der CSA-Verordnung.

Aufdeckung

- Nach der vorgeschlagenen CSA-Verordnung könnten interpersonelle Kommunikationsdienste (ICS) CSAM nur mit einer Aufdeckungsanordnung aufdecken. Es könnte demnach bis zu 18 Monate dauern, bis eine Aufdeckungsanordnung ausgestellt wird – 18 Monate, in denen keine Aufdeckung von CSAM innerhalb von interpersonellen Kommunikationsdiensten möglich wäre.
- Es ist daher wichtig, die freiwillige Aufdeckung von sexuellem Online-Kindesmissbrauch in interpersonellen Kommunikationsdiensten zu ermöglichen. Wir schlagen vor, eine harmonisierte rechtliche Regelung einzuführen, die sowohl freiwillige Aufdeckungsmaßnahmen von ICS-Anbietern (gekoppelt mit strengen Datenschutzgarantien) als auch - für den Fall, dass ein ICS-Anbieter das Risiko nicht angemessen mindert - verbindliche Anordnungen einer Koordinierungsbehörde umfasst, die die Anbieter zu angepassten oder zusätzlichen Maßnahmen zur Risikominderung verpflichtet. Kurz gefasst:
 - Die CSA-Verordnung sollte Anbieter dazu verpflichten, Risikobewertungen vorzunehmen, von sich aus angemessene Maßnahmen zur Risikominderung zu ergreifen und den Behörden darüber Bericht zu erstatten;
 - Die CSA-Verordnung sollte auch ein System verbindlicher Anordnungen einführen, denen Hosting- und ICS-Anbieter reaktiv nachkommen müssen, wenn sie keine ausreichenden Abhilfemaßnahmen ergriffen haben.

Schriftstück bearbeiten

Risikobewertungen

- Es ist positiv, dass der Rat mit dem neuen Artikel 5a "angepasste oder zusätzliche Risikobewertung oder Risikominderungsmaßnahmen" vorschlägt. Es ist der richtige Weg, der Koordinierungsbehörde die Befugnis zu erteilen, Anbieter zu verpflichten, zusätzliche Maßnahmen zur Risikominderung zu ergreifen, wenn der Anbieter es versäumt hat, angesichts seiner Risikobewertung ausreichende Maßnahmen zur Risikominderung einzuführen.
- Der Anbieter sollte die Art der erforderlichen Maßnahmen je nach Art des Dienstes flexibel wählen können. Weit gefasste Aufdeckungsanordnungen verstoßen gegen das in den europäischen Gesetzen verankerte Verbot der allgemeinen Überwachung und sollten daher insgesamt abgelehnt werden.

Cloud-Dienste

- Cloud-Computing-Dienste sollten vom Anwendungsbereich der Definition des Hosting-Dienstes und den damit verbundenen Verpflichtungen ausgenommen werden.
- Stattdessen könnten sie in den Anwendungsbereich von "last resort removal orders" fallen. Als solches schlagen wir einen kaskadierende Ansatz vor (nach dem Vorbild von Artikel 5 Absatz 6 der e-Evidence-Verordnung), der vorsieht, dass Entfernungsanordnungen im Normalfall gegenüber dem nachgelagerten Kunden und nur ausnahmsweise gegenüber Cloud-Infrastrukturanbietern (d. h. als "letztes Mittel") erlassen werden.

App-Store Anbieter

- Die Anbieter von App-Stores sind nicht in der Lage, das Risiko des Groomings von Kindern durch einzelnen Apps zu beurteilen, da sie nicht in das Innenleben der einzelnen Apps eingeweiht sind. Die Pflicht, Risikobewertungen durchzuführen und Maßnahmen zur Risikominderung zu ergreifen, liegt daher bei den App-Entwicklern.
- Je nach den von den App-Entwicklern zur Verfügung gestellten Informationen (z. B. ob ein Risiko des sexuellen Missbrauchs von Kindern besteht, ob ihre App überhaupt nicht für Kinder geeignet ist, ob sie eine Alterseinstufung vorgenommen haben) sollten App-Store Anbieter jedoch angemessene Maßnahmen ergreifen, um den Zugriff von Kindern auf solche Apps zu verhindern.

Melden Sie sich gerne mit Feedback oder Fragen, wir würden uns freuen, diese Anmerkungen in deinem Gespräch vertiefen zu können.

Beste Grüße

_____ und _____

--

Government Affairs & Public Policy Manager

_____@google.com | _____ | Twitter: @_____

Google Germany | Tucholskystr. 2 | 10117 Berlin

Geschäftsführer: Paul Manide, Liana Sebastian

Registergericht und -nummer: Hamburg, HRB 86891. Sitz der Gesellschaft: Hamburg

Diese Email ist vertraulich. Falls Sie diese fälschlicherweise erhalten haben sollten, teilen Sie diese bitte nicht an jemand anderes weiter, löschen Sie alle Kopien und Anhänge davon und lassen Sie mich bitte wissen, dass die Email an die falsche Person gesendet wurde.

This email is confidential. If you received this communication by mistake, please don't forward it to anyone else, please erase all copies and attachments, and please let me know that it has gone to the wrong person.

Schriftstück bearbeiten

**Proposal for a Regulation of the European Parliament and of the Council
laying down rules to prevent and combat child sexual abuse**

The following key points should be taken into account in the upcoming discussions on scope, risk assessments, mitigation measures and detection orders of the draft EU CSAM Regulation to ensure effective prevention and removal of CSAM, while addressing privacy concerns.

- **The requirement to carry out risk assessments should apply to those services that poses a high risk of online child sexual abuse.** We should avoid situations where valuable resources by authorities and providers go into products that have only low risk, if any, in the distribution of child sexual abuse material (e.g. flight bookings, payment sites, geo imagery services, etc.). It is important to ensure that regulator's and company's resources are most efficiently used, thus we propose to concentrate on services that can be used for these purposes. We also suggest a clarification that the yearly DSA risk assessment for illegal content required by VLOPs/ VLOSEs can be used as a baseline, complemented by additional measures under the draft CSAM Regulation.
- **With the proposed EU CSAM regulation, interpersonal communication services could detect CSAM only with a detection order.** It could take up to 18 months until a detection order gets issued – 18 months during which no detection of CSAM within ICS would be possible. It is therefore important to allow for voluntary detection of online child sexual abuse within interpersonal communication service. We propose to introduce a harmonized legal regime that consists of both voluntary detection measures deployed by ICS providers (paired with strict privacy safeguards) and, in case an ICS provider fails to appropriately mitigate the risk, mandatory orders from a Coordinating Authority obliging providers to take adjusted or additional risk mitigation measures. Briefly put:
 - the CSAM proposal should oblige providers to carry out risk assessments, take reasonable mitigation measures at their own initiative and report about them to the authorities;
 - the CSAM proposal should also introduce a system of mandatory orders, with which hosting and ICS providers must comply reactively, if they failed to take sufficient mitigation measures.
- **There are less severe legal mandates than detection orders. We welcome the fact that the Council proposes, with its new Article 5a, 'adjusted or additional risk assessment or risk mitigation measures'.** It is the right path forward to give the Coordinating Authority of Establishment the power to require the provider to take additional necessary mitigation measures, if the provider failed to roll out sufficient mitigation measures in light of its risk assessment. We think it should be on the provider to choose the type of necessary measures to deploy, depending on the nature of the service. Detection orders with a broad scope do violate the prohibition on general monitoring enshrined in

European laws and as such should be rejected as a whole.

- **Cloud computing services should be excluded from the scope of the hosting service definition and related obligations. Instead, they could be in scope of ‘last resort removal orders’.** As such, we suggest a “cascade approach” (modeled on Article 5(6) of the e-Evidence Regulation) which provides that removal orders would be issued towards the downstream customer in the normal course, and only as an exception to cloud infrastructure providers (i.e. as a “last resort”).
- **App store providers are not best placed when it comes to assessing the risk for solicitation of children by each app as they are not privy to the inner workings of each app.** The obligations to run risk assessments and deploy mitigation measures therefore must be on the app developers. Depending on the information provided by app developers (e.g. whether there is a risk for child sexual abuse, whether their app is not suitable for children at all, whether they applied an age rating) app store providers shall take reasonable measure to prevent children from accessing such apps.

Against this background, the following **amendments are proposed for Articles 3, 4, 6 and 7 of the EU CSAM Regulation.**

Tabled amendments by the Council	Proposed amendments
Risk assessment	
Article 3 Risk assessment 1. Providers of hosting services and providers of interpersonal communications services shall diligently identify, analyse and assess, for each such service that they offer, the risk of use of the service for the purpose of online child sexual abuse. 2. When carrying out a risk assessment, the provider shall take into account, in particular:	Article 3 Risk assessment 1. Providers of hosting services and providers of interpersonal communications services shall diligently identify, analyse and assess, for each such service that poses a high risk of online child sexual abuse, they offer, the risk of use of the service for the purpose of online child sexual abuse. 2. When carrying out a risk assessment, the provider shall take into account, in particular:

(a) any previously identified instances of use of its services for the purpose of online child sexual abuse; (b) the existence and implementation by the provider of a policy and the availability of functionalities to address the risk referred to in paragraph 1, including through the following: – prohibitions and restrictions laid down in the terms and conditions; – measures taken to enforce such prohibitions and restrictions; – functionalities enabling age verification; – functionalities enabling parental control or parental consent mechanisms; – functionalities enabling users to flag notify online child sexual abuse to the provider through tools that are easily accessible and age-appropriate; – measures taken to ensure a robust and swift process to handle notified potential child sexual abuse; – functionalities enabling the providers the compilation and generation of relevant statistical information for assessment purposes. (c) the manner in which users use the service and the impact thereof on that risk; (ca) age appropriate measures taken by the provider to promote users' media-digital literacy and safe use of the service; (...)	(a) any previously identified instances of use of its services for the purpose of online child sexual abuse; (b) the existence and implementation by the provider of a policy and the availability of functionalities to address the risk referred to in paragraph 1, including through the following: – prohibitions and restrictions laid down in the terms and conditions; – measures, including voluntary detection efforts, taken to enforce such prohibitions and restrictions; – functionalities enabling age verification or age assurance; – functionalities enabling parental control or parental consent mechanisms; – functionalities enabling users to flag notify online child sexual abuse to the provider through tools that are easily accessible and user friendly¹ age-appropriate; – measures taken to ensure a timely² robust and swift process to handle notified potential child sexual abuse; – functionalities enabling the providers the compilation and generation of to gather relevant statistical information for assessment transparency purposes according to Article 84 of this Regulation. (c) the manner in which users use the service and the impact thereof on that risk; (ca) age appropriate measures taken by the provider to promote users' media-digital literacy and safe use of the service;
--	---

¹ We suggest alignment with Art. 16 DSA

² We suggest alignment with Art. 16 DSA

4.a The risk assessment shall gather information on the limitation of the risk to an identifiable part or component of the service where possible, such as specific types of channels of an interpersonal communications service, or to specific users or specific groups of users where possible, to the extent that such part, component, specific users or specific groups of users can be assessed in isolation for the purpose of mitigating the risk of online child sexual abuse.	4.a The risk assessment shall gather information on the limitation of the risk to an identifiable part or component of the service where possible, such as specific types of channels of an interpersonal communications service, or to specific users or specific groups of users where possible³, to the extent that such part, component, specific users or specific groups of users can be assessed in isolation for the purpose of mitigating the risk of online child sexual abuse. 7. Providers that are subject to an obligation to conduct a risk assessment under Regulation (EU) 2022/2065 may draw on such a risk assessment and complement it with a more specific assessment of the risks of use of their services for the purpose of online child sexual abuse, as required by this Regulation.
Risk mitigation	
Article 4 Risk mitigation If providers of hosting services and providers of interpersonal communications services have identified a risk of the service being used for the purpose of online child sexual abuse pursuant to Article 3, they shall take all reasonable mitigation measures, tailored to the that risk identified pursuant to Article 3, to minimise that risk. The risk mitigation measures shall be limited to an	Article 4 Risk mitigation If providers of hosting services and providers of interpersonal communications services have identified a risk of the service being used for the purpose of online child sexual abuse pursuant to Article 3, they shall take all reasonable mitigation measures, tailored to the that risk identified pursuant to Article 3, to minimise that risk. The risk mitigation measures shall can be limited

³ We have strong privacy concerns by identifying specific users or user groups in the risk assessments.

identifiable part or component of the service, or to specific users or specific groups of users, where possible, without prejudice to the effectiveness of the measure.

(...)

(d) initiating or adjusting functionalities that enable users to notify online child sexual abuse to the provider through tools that are easily accessible and age-appropriate;

3. Providers of interpersonal communications services that have identified, pursuant to the risk assessment conducted or updated in accordance with Article 3, a risk of use of their services for the purpose of the solicitation of children, shall take the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the mitigation measures.

~~3a. Any~~ Those age verification and age assessment measures shall be privacy preserving, proportionate, transparent, effective, accurate, non-discriminatory, accessible and take as a primary consideration the best interest of the child into account not involve any profiling or biometric identification of users.

to an identifiable part or component of the service, ~~or to specific users or specific groups of users,~~ where possible, without prejudice to the effectiveness of the measure.

(...)

(d) initiating or adjusting functionalities that enable users to notify online child sexual abuse to the provider through tools that are easily accessible and ~~user-friendly age-appropriate;~~

(...)

(h) the use of specific technologies on a voluntary basis for the sole purpose of preventing online child sexual abuse.

3. Providers of interpersonal communications services that have identified, pursuant to the risk assessment conducted or updated in accordance with Article 3, a risk of use of their services for the purpose of the solicitation of children, shall take the necessary age verification ~~and or~~ age assessment measures to reliably identify child users on their services, enabling them to take the mitigation measures.

~~3a. Any~~ Those age verification ~~and or~~ age assessment assurance measures shall be privacy preserving, proportionate, transparent, effective, accurate, non-discriminatory, accessible and take as a primary consideration the best interest of the child into account not involve any profiling or biometric identification of users.

Processing of personal data in ICS	
	New Article 4a⁴ Processing of personal data interpersonal communication services 1. Providers of number-independent interpersonal communications services shall be permitted to process electronic communication data for the sole purpose of preventing online child sexual abuse by detecting, removing and reporting material as defined in Article 2(p) provided that: (a) the processing is: (i) strictly necessary for the use of specific technology for the sole purpose of detecting and removing online child sexual abuse material and of detecting solicitation of children and reporting it to organisations acting in the public interest against child sexual abuse; (ii) proportionate and limited to technologies used by providers for the purpose set out in point (i); (iii) limited to content data and related traffic data that are strictly necessary for the purpose set out in point (i); (iv) limited to what is strictly necessary for the purpose set out in point (i);

⁴ This is taken from Art. 3 of the current Interim regulation that allows ICS to detect CSAM within private communication under strict safeguards. Please note that we made minor modifications to Article 3 to remedy some current deficiencies and to prevent duplication of obligations (e.g. transparency reporting obligations).

(b) the technologies used for the purpose set out in point (a)(i) of this paragraph are in accordance with the state of the art in the industry and are the least privacy-intrusive, including with regard to the principle of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679 and, to the extent that they are used to scan text in communications, they are not able to deduce the substance of the content of the communications until relevant key indicators described in (e) are met ~~but are solely able to detect patterns which point to possible online child sexual abuse;~~

(c) with regard to new technology, meaning technology used for the purpose of detecting online child sexual abuse material that has not been used by any provider in relation to services provided to users of number-independent interpersonal communications services ('users') in the Union before 2 August 2021, and with regard to technology used for the purpose of identifying possible solicitation of children, likely to result in a high risk to the rights and freedoms of natural persons, the provider reports back to the competent authority on the measures taken to demonstrate compliance with written advice issued in accordance with Article 36(2) of Regulation (EU) 2016/679 by the competent supervisory authority designated pursuant to Chapter VI, Section 1, of that Regulation ('supervisory authority') in the course of the prior consultation procedure;

(d) the technologies used are sufficiently reliable in that they limit to the maximum extent possible the rate of errors regarding the detection of content representing online child sexual abuse and, where such occasional errors occur, their consequences are rectified without delay;

(e) the technologies used to detect patterns of possible solicitation of children are limited to the use of relevant key indicators and objectively identified risk factors such as age difference and the likely involvement of a child in the scanned communication, without

	prejudice to the right to human review of content to confirm online child sexual abuse. (f) the providers: (i) have established internal procedures to prevent abuse of, unauthorised access to, and unauthorised transfers of, personal and other data; (ii) ensure human oversight of and, where necessary, human intervention in the processing of personal and other data using technologies falling under this Regulation; (iii) ensure that material not previously identified as online child sexual abuse material, or solicitation of children, is not reported to organisations acting in the public interest against child sexual abuse without prior human confirmation; (iv) have established appropriate procedures and redress mechanisms to ensure that users can lodge complaints with them within a reasonable timeframe for the purpose of presenting their views; (v) inform users in a clear, prominent and comprehensible way of the fact that they have invoked, in accordance with this Regulation, the derogation from Articles 5(1), 5(3) and 6(1) of Directive 2002/58/EC concerning the confidentiality of users' communications for the sole purpose set out in point (a)(i) of this paragraph, the logic behind the measures they have taken under the derogation and the impact on the confidentiality of users' communications, including the possibility that personal data are shared with law enforcement authorities and organisations acting in the public interest against child sexual abuse;
--	---

	(vi) inform users of the following, where their content has been removed or their account has been blocked or a service offered to them has been suspended: (1) the avenues for seeking redress from them; (2) the possibility of lodging a complaint with a supervisory authority; and (3) the right to a judicial remedy; (g) where suspected online child sexual abuse has been identified, the content data and related traffic data processed for the purpose set out in point (a)(i), and personal data generated through such processing are stored in a secure manner, solely for the purposes of: (h) reporting, without delay, the suspected online child sexual abuse to the competent law enforcement and judicial authorities or organisations acting in the public interest against child sexual abuse; (ii) blocking the account of, or suspending or terminating the provision of the service to, the user concerned; (iii) creating a unique, non-reconvertible digital signature ('hash') of data reliably identified as online child sexual abuse material (iv) enabling the user concerned to seek redress from the provider or pursue administrative review or judicial remedies on matters related to the suspected online child sexual abuse; or (v) responding to requests issued by competent law enforcement and judicial authorities in accordance with the applicable law to provide them with the necessary data for the prevention, detection,
--	--

	investigation or prosecution of criminal offences as set out in Directive 2011/93/EU; (vi) the training or development of technologies used for the purpose set out in point (a)(i). (i) the data are stored no longer than strictly necessary for the relevant purpose set out in point (h) (j) every case of a reasoned and verified suspicion of online child sexual abuse is reported without delay to organisations acting in the public interest against child sexual abuse.
Additional risk mitigation measures	
Article 7 Issuance of detection orders (...)	Article 7⁵ Issuance of detection orders (...) Adjusted or additional risk assessment or risk mitigation measures 1. Without prejudice to Articles 27 to 29, where on the basis of its assessment referred to in Article 5(2), the Coordinating Authority of establishment determines that the requirements of Articles 3 and or 4 have not been met, it shall require the provider of hosting services or the provider of interpersonal communications services to carry out one or several of the following actions, as appropriate: (a) to re-conduct or update the risk assessment in accordance with

⁵ We suggest to move the wording of the Presidency compromise text on additional risk mitigation measures from Art. 5a to Article 7 -- instead of detection orders. We made some minor tweaks to text of the Presidency to address the prohibition on general monitoring.

	<u>Article 3, including where appropriate by modifying the methodology used to conduct the risk assessment;</u> (b) to implement, review, modify, discontinue or expand some or all of the risk mitigation measures taken in accordance with Article 4; (c) to introduce additional risk mitigation measures in accordance with Article 4, <u>although the provider may choose the type of specific measures to take.</u> <u>The Coordinating Authority of establishment may request the EU Centre for an opinion on technical aspects of the possible actions that it intends to require pursuant to the first subparagraph.</u> 2. The provider shall inform the Coordinating Authority of the actions steps taken to ensure compliance with the measures required pursuant to paragraph 1, within a time period set by the Coordinating Authority. That time period shall be reasonable, taking into account the complexity of the required <u>actions measures.</u> 3. <u>Any requirement to take specific measures shall be without prejudice to Article 8 of Regulation (EU) 2022/2065 and shall entail neither a general obligation for providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.</u> <u>Any requirement to take specific measures shall not include an obligation to use automated tools by the provider.</u>
Cloud computing services	
	Insert new definition for Article 2

	“Cloud customer entity” means an entity that has a contractual agreement with a provider of a cloud computing service for the storage of data, by which it [performs or provides] a hosting service on behalf of its own end-users. ‘cloud computing service’ means a service as defined in Article 6, point 30, of Directive (EU) 2022/2555 of the European Parliament and of the Council. Amend definition for Article 2 ‘hosting service’ means an information society service as defined in Article 2, point (f), third indent, of Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC], excluding software application stores, interpersonal communication services and cloud computing services, Article 15a new Removal orders under Article 14 shall not be addressed to providers of cloud computing services. As an exception, where the cloud computing service stores data as part of an infrastructure provided to a cloud customer entity, the removal order may be directly addressed to the provider of the cloud computing service requiring it to remove or disable access at the lowest level possible where the cloud customer entity cannot be identified despite reasonable efforts on the part of the Coordinating Authority.
	App stores

Article 6

Obligations for software application stores

Providers of software application stores shall:

- (a) make reasonable efforts to assess, where possible together with the providers of software applications, whether each service offered through the software applications that they intermediate presents a risk of being used for the purpose of the solicitation of children;
- (b) take reasonable measures to prevent child users from accessing the software applications in relation to which they have identified a significant risk of use of the service concerned for the purpose of the solicitation of children;
- (c) take the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the measures referred to in point (b). **Those age verification and age assessment measures shall be privacy preserving, proportionate, transparent, effective, accurate, non-discriminatory, accessible and take as a primary consideration the best interest of the child.**

2. In assessing the risk referred to in paragraph 1, the provider shall take into account all the available information, including the results of the risk assessment conducted or updated pursuant to Article 3.

3. Providers of software application stores shall make publicly available information describing the process and criteria used to assess the risk and describing the measures referred to in paragraph 1. That description shall not include information that may reduce the effectiveness of the assessment of those measures.

4. The Commission, in cooperation with Coordinating Authorities and the EU Centre and after having conducted a public consultation, may

Article 6

Obligations for software application stores

Providers of software application stores shall:

- ~~(a) make reasonable efforts to assess, where possible together with the providers of software applications, whether each service offered through the software applications that they intermediate presents a risk of being used for the purpose of the solicitation of children;~~
- (b) **based on information provided by the application developers,** take reasonable measures to prevent **known** child users from **downloading or installing** accessing the software applications in relation to which they have identified a significant risk of use of the service concerned for the purpose of the solicitation of children **from its platform where**
 - i.) the developer of the software application has informed the software application store that children are not permitted to use its software applications or
 - ii.) the software application has a content rating that indicates it is only appropriate for use by adults.

~~(c) take the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the measures referred to in point (b). Those age verification and age assessment measures shall be privacy preserving, proportionate, transparent, effective, accurate, non-discriminatory, accessible and take as a primary consideration the best interest of the child.~~

~~2. In assessing the risk referred to in paragraph 1, the provider shall take into account all the available information, including the results of the risk assessment conducted or updated pursuant to Article 3.~~

issue guidelines on the application of paragraphs 1, 2 and 3, having due regard in particular to relevant technological developments and to the manners in which the services covered by those provisions are offered and used.

3. Providers of software application stores shall make publicly available information describing the process and criteria used to assess the risk and describing the measures referred to in paragraph 1. That description shall not include information that may reduce the effectiveness of the assessment of those measures.

4. The Commission, in cooperation with Coordinating Authorities and the EU Centre and after having conducted a public consultation, may issue guidelines on the application of paragraphs 1, 2 and 3, having due regard in particular to relevant technological developments and to the manners in which the services covered by those provisions are offered and used.

Von: [REDACTED]@bmj.bund.de>
An: GG-ALIII <GG-ALIII@bmj.bund.de>; GG-UALIIIB <GG-UALIIIB@bmj.bund.de>; E-Post-RegIII <E-Post-RegIII@bmj.bund.de>
CC: Referat IIIB7 <IIIB7@bmj.bund.de>
Gesendet am: 16.05.2023 17:06:05
Betreff: WG: Stellungnahme des Deutschen Anwaltvereins zur EU-Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSAM)

IIIB7

1. eGG
2. zVg

Viele Grüße

[REDACTED]
Referat IIIB7
[REDACTED]

Von: [REDACTED]@bmj.bund.de>
Gesendet: Dienstag, 16. Mai 2023 16:02
An: Referat IIIB7 <IIIB7@bmj.bund.de>
Cc: [REDACTED] <[REDACTED]@bmj.bund.de>; [REDACTED] - IIIB7 - <[REDACTED]@bmj.bund.de>
Betreff: WG: Stellungnahme des Deutschen Anwaltvereins zur EU-Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSAM)

Liebe KuK,

die DAV-Stellungnahme zur CSA-VO leite ich nur vorsorglich weiter, falls noch nicht bekannt.

BG
[REDACTED]

Von: .BRUEEU POL-JU-1-EU [REDACTED] <pol-ju-1-eu@brue.auswaertiges-amt.de>
Gesendet: Dienstag, 16. Mai 2023 15:48
An: [REDACTED] <[REDACTED]@bmj.bund.de>
Cc: [REDACTED] <[REDACTED]@bmj.bund.de>; [REDACTED] <[REDACTED]@bmj.bund.de>
Betreff: WG: Stellungnahme des Deutschen Anwaltvereins zur EU-Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSAM)

[REDACTED]
kennt Ihr wahrscheinlich schon...

Viele Grüße
[REDACTED]

Von: Brüssel - Öffentlich (DAV) <bruessel@eu.anwaltverein.de>

Gesendet: Dienstag, 16. Mai 2023 12:28.

An: [REDACTED] ([REDACTED]@diplo.de) <[REDACTED]@diplo.de>

Betreff: Stellungnahme des Deutschen Anwaltvereins zur EU-Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSAM)

Sehr [REDACTED]

anbei übermittele ich Ihnen die Stellungnahme 32/2023 des Deutschen Anwaltvereins (DAV) durch den Ausschuss Gefahrenabwehrrecht zum **Vorschlag einer EU-Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSAM) und zum Berichtsentwurf im Europäischen Parlament**.

Der DAV unterstützt das Ziel des Verordnungsentwurfs; die Bekämpfung der Verbreitung von Kindesmissbrauchsmaterial im Internet ist ein wichtiges Anliegen. Es ist daher ein begrüßenswerter Schritt, dass innerhalb der EU die Zusammenarbeit und Koordinierung von Strafverfolgungsbehörden der Mitgliedstaaten verbessert werden sollen. Ebenfalls zuzustimmen ist dem Verordnungsentwurf insoweit, als dass die Löschung strafbarer Inhalte, die beispielsweise aufgrund von Hinweisen identifiziert worden sind, einheitlich geregelt wird. Dies schafft Rechtssicherheit für die Diensteanbieter über die Grenzen der Mitgliedstaaten hinweg.

Im Übrigen begegnet der Entwurf jedoch trotz seines wichtigen Anliegens erheblichen rechtsstaatlichen Bedenken. Er läuft auf eine Abschaffung der Ende-zu-Ende-Verschlüsselung und eine automatisierte, massenhafte Analyse von Kommunikations(inhalts-)daten aller Nutzer von bspw. Email-, Messenger- und Chat-Anwendungen, sozialen Medien oder auch Cloud-Speicherdiensten hinaus.

Dabei ist nicht nur mit einer hohen Zahl an falschen Treffern zu rechnen, die eine nähere Betrachtung höchstprivater Kommunikationsinhalte nach sich ziehen würden. Zwangsläufig wäre auch das anwaltliche Berufsgeheimnis beeinträchtigt. Der tatsächliche Nutzen für die Bekämpfung der Verbreitung von Kindesmissbrauchsmaterial wäre indes angesichts von Ausweichmöglichkeiten ins sog. Dark-Net fraglich.

Die kürzlich vom Berichterstatter des LIBE-Ausschusses im Europäischen Parlament vorgeschlagenen Änderungen sind nicht geeignet, die gegen das Instrument der Aufdeckungsanordnung vorgebrachte Kritik zu entkräften. Die vorgeschlagene Ergänzung des Verordnungsentwurfs um eine Befugnis zur *freiwilligen* Auswertung von Kommunikationsinhalten durch Diensteanbieter, ohne dass es einer entsprechenden Anordnung bedürfte, begegnet zudem im Kern denselben rechtlichen Bedenken wie das Instrument der Aufdeckungsanordnung.

Weitere Einzelheiten entnehmen Sie bitte der beigefügten, ausführlich begründeten DAV-Stellungnahme Nr. 32/2023.

Mit freundlichen Grüßen

[REDACTED]
[REDACTED] für EU-Angelegenheiten/ Legal Adviser for EU-Affairs

Deutscher Anwaltverein
German Bar Association
Internationales, Europa und Menschenrechte
International and EU Affairs, Human Rights

[REDACTED]
Referentin für EU-Angelegenheiten/ Legal Adviser for EU-Affairs
[REDACTED]

Rue Joseph II 40, Boîte 7B
1000 Brüssel – Brussels

Tel. : [REDACTED]

Fax [REDACTED]

[REDACTED]@eu.anwaltverein.de

www.anwaltverein.de

facebook.com/deutscheranwaltverein

twitter.com/anwaltverein

twitter.com/DAVbxl