- **Geheimhaltungsgrad:** Verschlusssache – Nur für den Dienstgebrauch
- **Von:** Ständige Vertretung EU Brüssel
- **An:** Auswärtiges Amt
- **Kopie:** BMI, BMJ, BMWK, BMDV, BMFSFJ, BKAMT, BMF
- **Betreff:** Sitzung der RAG Strafverfolgung (LEWP-P) am 19./20.01.2023
- **Hier:** Entwurf der CSA-Verordnung
- **Zweck:** Zur Unterrichtung
- **Geschäftszeichen:** 350.80/4

1. Zusammenfassung und Wertung

In der ersten LEWP-Sitzung unter SWE-Vors. zur CSA-VO stellte zunächst der Europäische Datenschutzbeauftragte (EDPS) kurz seine gemeinsame Stellungnahme mit dem Europäischen Datenschutzausschuss vom 28. Juli 2022 vor. Er kritisierte den VO-Entwurf deutlich. Auf Nachfragen von MS reagierte EDPS oft ausweichend. Er machte keine Vorschläge, wie die VO aus seiner Sicht rechtskonform ausgestaltet werden könne. Verschiedene MS und insbesondere KOM zeigten über die Ausführungen des EDPS enttäuscht. Sie hätten konstruktive Lösungsansätze seitens EDPS erwartet, nicht nur pauschale Kritik.

Eine vom Vors. initiierte Tischumfrage zu Regelungen zur Verschlüsselung in der CSA-VO ergab kein einheitliches Meinungsbild. Während einige MS eine klare Aussage zum Umgang mit verschlüsselten Inhalten im verfügenden Text der VO bevorzugten, hatten die meisten MS noch keine abschließende Position. Vors. schlussfolgerte, dass die Thematik weiter diskutiert werden müsse. Bezüglich der Frage, ob und ggf. unter welchen Voraussetzungen man neben verpflichtenden Aufdeckungsanordnungen auch zukünftig freiwillige Detektion durch die Dienstanbieter zulassen solle, ergab sich noch keine abschließende Position. Vors. kündigte an, auch diesen Bereich weiter zu erörtern.

Ferner wurden die grundsätzlichen Positionen der MS zu Audiokommunikation im Anwendungsbereich der CSA-VO sowie zu Maßnahmen in öffentlich zugänglichen Diensten und interpersoneller Kommunikation thematisiert. Abgeschlossen wurde die Sitzung mit der Erörterung der Artikel 12 bis 16 des VO-Entwurfs.

II. Im Einzelnen

TOP 1: Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse

(1) Joint Opinion 4/2022 of EDPS and EDPB

Der Europäische Datenschutzbeauftragte (EDPS) stellte kurz seine gemeinsame Stellungnahme mit dem Europäischen Datenschutzausschuss (EDPB) vom 28. Juli 2022 vor. Es stelle sich die Frage, wie frei die Europäer künftig bei der Nutzung des Internets sein würden. Er bezweifle, dass die gewählte Strategie die richtige sei. Der VO-Vorschlag der KOM sei aus seiner Sicht „nicht voll und ganz“ mit den europäischen Grundrechten vereinbar. Die im Entwurf vorgesehenen Aufdeckungsanordnungen seien nicht zielgerichtet genug und führten zu einem „noch nie dagewesenen Maß an Rechtsunsicherheit“. Das EU-Zentrum müsse organisatorisch und technisch von Europol getrennt werden.

FRA sprach sich dagegen aus, Grooming – wie vom EDPS gefordert – aus dem Anwendungsbereich der VO auszuschließen. AUT fragte zu Rz. 47 f. der EDPS/EDPB-Stellungnahme, welche „weniger einschneidende Maßnahmen“ EDPS vorschlage. EDPS erklärte, derartige „weniger einschneidende Maßnahmen“ nicht konkretisieren zu können. Auf Frage von FIN erklärte EDPS, dass es keinen Unterschied mache, ob eine Maschine oder ein Mensch die Kommunikation überwache, es sei immer ein unglaublicher Eingriff in die Privatsphäre“. CZE warnte davor, „sich immer nur im Kreis zu drehen“ und dabei den Schutz vor Kindern vor sexuellem Missbrauch aus dem Auge zu verlieren. Gerade bei unbekannten Darstellungen und Grooming müsse man sich des Risikos von Fehlern bewusst sein, dies dürfe aber nicht dazu führen, dass man nichts unternehme. EDPS machte geltend, dass er dem VO-Vorschlag auch bei geringeren Fehlerquoten bei der Detektion von CSAM nicht „zustimmen“ könne. SVN kritisierte, dass sich der EDPS in „geradezu gefährlicher Weise“ ausschließlich auf den Schutz der Privatsphäre fokussiere und forderte, dass der Schutz der Kinder Vorrang haben müsse, da diese lebenslang unter den Auswirkungen sexuellen Missbrauchs zu leiden hätten. Ohne gesetzliche Verpflichtungen der Diensteanbieter könne man das Phänomen nicht wirksam bekämpfen, daher solle der VO-Entwurf zügig angenommen werden.

Auf unsere Fragen zur Altersverifikation gab EDPS die Einschätzung ab, dass es derzeit keine verlässlichen Anbieter für Altersfeststellungen gebe. Es bestehe das „Risiko der Ausgrenzung“ oder „zu intrusiver Altersverifikation“. Ggf. könne man einen – nicht genauer definierten – „Elternkontrollmechanismus“ anwenden. Ansonsten habe der EDPS „keine weiteren Vorschläge“. KOM zeigte sich über die Ausführungen des EDPS verwundert und verwies auf den unter CZE-Ratspräsidentschaft durchgeführten Expertenworkshop zur Altersverifikation. Es gebe bereits mehrere gewerblich erhältliche Tools, die einen Altersverifikation zufriedenstellend ermöglichten.

EDPS machte geltend, „evtl. noch nacharbeiten zu müssen, weil die Stellungnahme sehr kurzfristig angefordert worden sei“. Er habe keine Vorschläge, wie man den VO-Entwurf rechtskonform ausgestalten könne. Verschiedene MS und insbesondere KOM zeigten sich enttäuscht, dass EDPS viele Fragen nicht beantwortet bzw. keine Lösungsvorschläge unterbreitet habe.

KOM wies darauf hin, dass die Aufdeckungsanordnung ein letztes Mittel sei, wenn „mitigation measures“ nicht erfolgreich seien. Außerdem gebe es immer noch einen Austausch zwischen dem Provider und der Behörde. Es gehe darum, die Maßnahmen zielgerichtet einzusetzen. Gerade dies werde vom EDPS gefordert. JD KOM machte geltend, dass es derzeit noch keine einschlägigen Urteile zu der konkreten Thematik gebe. Die Vorratsdatenspeicherung sei ein wichtiger Referenzrahmen, es gebe aber noch andere EuGH-Rechtsprechung, die bei der rechtlichen Analyse zu berücksichtigen sei. Illegale Inhalte seien etwas Anderes als Metadaten bei der Vorratsdatenspeicherung. Der KOM-Vorschlag sehe mehrere „Schichten“ an safeguards vor. KOM räumte ein, dass es keine Lösungsansätze ohne rechtliches Risiko gebe, warf aber umgekehrt die Frage auf, wie hoch ist das Risiko sei, wenn man gar nichts unternehme, um Kinder wirksamer vor sexuellem Missbrauch zu schützen.

ESP, PRT und FRA baten KOM, ihre rechtlichen Ausführungen auch schriftlich zu übermitteln. KOM erhob keine grundsätzlichen Einwände, wies aber darauf hin, hierfür noch eine interne Genehmigung zu benötigen. Auf Nachfrage von IRL und AUT erklärte JD Rat, dass sich seine angekündigte schriftliche Stellungnahme noch verzögere, weil man derzeit keinen Generaldirektor habe. Es gebe einen Entwurf, der aber noch gebilligt werden müsse. Wann die Stellungnahme übermittelt werde, ließe sich noch nicht sagen. AUT regte, dass der Vors. auch eine Stellungnahme der Grundrechteagentur FRA einholen solle. Vors. wies darauf hin, dass dies nicht üblich sei. Es bleibe der FRA aber selbstverständlich unbenommen, sich eigenständig zu äußern.

(2) Verschlüsselung

Vors. führte eine ad hoc-Tischumfrage zur Frage der Verschlüsselung durch. Einige MS hätten dafür plädiert, in den VO-Text aufzunehmen, dass Verschlüsselung nicht beeinträchtigt werden dürfe. Es herrsche auch Unsicherheit bei den Diensteanbietern, wie sich Verschlüsselung auf Aufdeckungsanordnungen auswirken würde.

CZE und IRL sprachen sich dagegen aus, ein explizites Verbot in die VO aufzunehmen, weil man sich sonst zukünftigen technologischen Entwicklungen komplett verschließen würde und den Rechtsakt bei jeder neuen Entwicklung wieder „aufmachen“ müsse.

FRA forderte, nichts in den Text aufzunehmen, was als Schwächung oder Verbot der Verschlüsselung angesehen werden könne. Auch SVN betonte die Bedeutung der Verschlüsselung.

Wir trugen weisungsgemäß vor. Dabei betonten wir, dass ein hohes Datenschutzniveau und ein hohes Maß an Cybersicherheit, einschließlich einer durchgängigen und sicheren Ende-zu-Ende-Verschlüsselung in der elektronischen Kommunikation, für die Bundesregierung unerlässlich seien. Vor diesem Hintergrund sei es aus unserer Sicht unter anderem erforderlich, in dem Entwurfstext festzuhalten, dass der Einsatz von Technologien, die zu einem Bruch, einer Schwächung, einer Umgehung oder einer Modifikation von Verschlüsselung führen würden, ausgeschlossen sei.

PRT warnte davor, dass Verschlüsselung zu einem safe harbour für Pädophile führen könne, man müsse daher sehr vorsichtig sein. HRV wies darauf hin, dass Verschlüsselung negative Auswirkungen auf die Aufdeckung von CSA haben könne und plädierte dafür, in der VO Regelungen zur Verschlüsselung aufzunehmen.

FIN legte einen PV ein, sprach sich aber dafür aus, Verschlüsselung nicht nur in einem Erwägungsgrund zu erwähnen, sondern im verfügenden Text zu regeln.

ROU machte geltend, kein „Patentrezept“ zu haben, wies aber auf Probleme der Strafverfolgungsbehörden mit verschlüsselter Kommunikation hin.

AUT nahm Bezug auf die Stellungnahme seines nationalen Parlaments, welche die Vorgabe der Wahrung der vertraulichen Kommunikation im Internet (insbesondere end-to-end encryption) enthalte.

BGR und MLT legten einen PV ein und kündigte schriftliche Stellungnahmen an.

EST ebenfalls mit PV, aber mit Hinweis auf die immensen Auswirkungen auf die Arbeit der Strafverfolgungsbehörden (Gefahr der Behinderung von Strafverfolgung) und evtl. Präzedenzwirkung für andere Bereiche.

NLD nahmen auf ihren schriftlichen Textvorschlag zu Artikel 10 Abs. 3 VO-Entwurf (keine Technologie, die end-to-end encryption unmöglich mache) Bezug.

LUX gab keine Stellungnahme ab.

LVA forderte, eine Regelung zur Integrität der Verschlüsselung in die VO aufzunehmen, es komme aber auf die konkrete Formulierung an.

ITA legte einen PV ein, plädierte aber für eine technologieneutrale Lösung. Die Güterabwägung sei wichtig, Verschlüsselung und Schutz der Privatsphäre dürften aber nicht zu einer Verletzung der Rechte der Opfer führen.

GRC betonte, dass der Polizei ohne Zugang zu Verschlüsselung „die Hände gebunden seien". Auch LTU betonte, dass es wichtig sei, Zugang zu verschlüsselten Daten zu haben (auch über CSA hinaus).

DNK wies darauf hin, keine Weisung zur Frage der Verschlüsselung zu haben und beschränkte sich auf die allgemeine Anmerkung, dass sowohl Rechtsgarantien als auch „flexible Verfahren" wichtig seien. In DNK habe man ein nationales System für Blockierungsanordnungen, das man auch nach Inkrafttreten der CSA-VO weiter nutzen wolle.

CYP machte geltend, dass das Aufbrechen der Verschlüsselung unabdingbar für die Bekämpfung von CSA, aber auch anderer krimineller Aktivitäten, sei. Man brauche eine Regelung im verfügenden Teil der VO. Die Lösung müsse ausgewogen und mit der EuGH Rechtsprechung vereinbar sein.

POL sprach sich dafür aus, dass das Wesen der Verschlüsselung nicht in Frage gestellt werden dürfe. Der Schutz der Privatsphäre sei aber kein uneingeschränktes Recht. Die Wahrung der Rechte der Kinder sei außergewöhnlich hoch zu bewerten, allerdings müssten Maßnahmen stets verhältnismäßig sein. Hierzu seien weitere Diskussionen notwendig. POL kündigte eine schriftliche Stellungnahme an.

HUN legte einen PV ein. Der Schutz des Kindes habe aber „absolute Priorität", daher müsse man mit den Diensteanbietern zusammenarbeiten.

BEL ebenfalls mit PV. Vorläufig könne man sagen, dass Behörden Daten schnell, wirksam und sicher bearbeiten müssten bzw. Zugang darauf haben sollten.

ESP machte geltend, dass der Zugang zu verschlüsseltem Material grundlegend für die Verbrechungsbekämpfung sei. Wie CZE und IRL plädierte ESP dafür, dass die VO auch zukünftige technologische Entwicklungen berücksichtigen müsse; es wäre gut, wenn die VO nur allgemein auf das Thema eingehen könnte.

SVK wies darauf hin, dass die dortigen internen Diskussionen noch andauerten. Verschlüsselung sei ein wichtiger Aspekt zum Schutz von Grund- und Menschenrechten. Es sei aber auch klar, dass dies kein Hindernis für die Verfolgung von CSA bilden dürfe.

KOM betonte, dass die Technologieneutralität ein Hauptbaustein ihres VO-Vorschlags sei. Eine Ausnahme von end-to-end encryption aus dem Anwendungsbereich der VO würde zu erheblichen Lücken führen und es müsse ausgeschlossen werden, dass sich Diensteanbieter ihren Verpflichtungen durch die CSA-VO entzögen, indem sie Verschlüsselung einführten. Eine „Freistellung" bestimmter Dienste sei gefährlich und eine Ausnahme von Aufdeckungsverpflichtungen würde die Verhältnismäßigkeit und Wirksamkeit des Vorschlags aufheben. Man habe ansonsten auch kein „level playing field" mehr für die Diensteanbieter.

Vors. schlussfolgerte, dass die Frage der Verschlüsselung für die Delegationen hohe Bedeutung habe und hob die Präzedenzwirkung einer Regelung in der CSA-VO hervor. Während einige MS eine klare Aussage im verfügenden Text der VO bevorzugten, hätten die meisten MS noch keine abschließende Position. Vors. wies darauf hin, dass EG 25 des VO-Entwurfs bereits Ausführungen zur Verschlüsselung enthalte. „Straffreiheit im verschlüsselten Umfeld" müsse man verhindern. Vors. werde über den Zugriff von Strafverfolgungsbehörden auf vertrauliche Kommunikation auch in anderen Gremien diskutieren und die Thematik beim informellen JI-Rat, im COSI und in der RAG COPEN erörtern.

(3) Freiwillige Detektionsmaßnahmen auch nach Inkrafttreten der CSA-VO?

Vors. wies darauf hin, dass es Wünsche einiger MS gebe, auch nach Inkrafttreten der CSA-VO weiterhin freiwillige Detektion durch die Diensteanbieter zu ermöglichen. Hierzu könne entweder die Bereichsausnahme zu E-Privacy verlängert bzw. perpetuiert werden oder eine separate Regelung in die CSA-VO aufgenommen werden. Vors. warf die Frage auf, ob die entsprechenden Möglichkeiten weiter geprüft werden sollten.

IRL, CZE, FIN und FRA plädierten dafür, weiterhin freiwillige Aufdeckungsmaßnahmen durch die Diensteanbieter zu ermöglichen. FRA hob dabei hervor, dass die hosting service provider aber eine klare Rechtsgrundlage bräuchten.

AUT, POL, NLD, ITA, ROU und wir plädierten dafür, zumindest zu prüfen, ob und ggf. unter welchen Voraussetzungen man auch zukünftig freiwillige Detektion durch die Diensteanbieter zulassen solle. Unter dem Aspekt der Verhältnismäßigkeit könne dies möglicherweise eine mildere Maßnahme als eine Aufdeckungsanordnung sein („Stufenverhältnis"). Allerdings müsse dann eine klare Rechtsgrundlage für die freiwillige Detektion geschaffen werden, da die temporäre Bereichsausnahme zur E-Privacy-RL auslaufe. Rechtstechnisch sei dabei einer eigenständigen Regelung in der CSA-VO der Vorzug zu geben. Die zugrundeliegenden Juristischen Fragen bedürften allerdings noch eingehender Diskussionen.

KOM äußerte sich dagegen skeptisch, auch nach Auslaufen der temporären Bereichsausnahme zu E-Privacy weiterhin freiwillige Detektion zuzulassen. Der Entwurf der CSA-VO sehe ausschließlich das Instrument der Aufdeckungsanordnung vor. Für freiwillige Aufdeckungsmaßnahmen durch die Diensteanbieter sei aus Sicht der KOM in der CSA-VO

kein Raum mehr. Eine parallele Existenz beider Instrumente sei nur „rein hypothetisch“ möglich.

Vors. schlussfolgerte, dass es seitens der MS hinreichende Unterstützung für eine Prüfung gebe, ob und ggf. unter welchen Voraussetzungen (Rechtsgrundlage) man auch zukünftig freiwillige Detektion durch die Dienstanbieter zulassen solle. Er werde daher auf die Thematik zurückkommen.

(4) Audiokommunikation im Anwendungsbereich der CSA-VO, Maßnahmen in öffentlich zugänglichen Diensten und interpersoneller Kommunikation

Vors. fragte nach Positionen der MS zu Audiokommunikation im Anwendungsbereich der CSA-VO sowie nach Maßnahmen in öffentlich zugänglichen Diensten und interpersoneller Kommunikation.

FRA und CZE trugen einen PV zu Audiokommunikation vor. Aus CZE-Sicht seien weitere safeguards erforderlich. Wir – unterstützt von NLD – trugen weisungsgemäß vor, dass Audiokommunikation aus dem Anwendungsbereich des Art. 7 VO-E auszunehmen sei. Aus PRT-Sicht sollte Audiokommunikation vom Anwendungsbereich umfasst bleiben, da PRT Definition sämtliche Inhalte unabhängig von der medialen Form umfasse. KOM betonte, dass Audiokommunikation an Bedeutung – auch im Bereich CSAM – gewinne.

Vors. führte aus, dass ein Unterschied zwischen TCO-VO und CSA-VO sei, dass terroristische Inhalte i.d.R. öffentlich verbreitet werden sollen, während CSAM i.d.R. im Privaten geteilt werden. Wir trugen weisungsgemäß vor, dass der PV insbesondere interpersonelle Kommunikationsdienste und persönliche Cloudspeicher umfasse. ITA führte aus, dass eine Abwägung zwischen dem Schutz minderjähriger Nutzerinnen und Nutzer und Datenschutz stattfinden müsse. NLD sprach sich für verhältnismäßige Aufdeckungsmaßnahmen nach bekanntem CSAM in interpersonellen Kommunikationsdiensten aus; bei unbekanntem CSAM und Grooming bestünden Zweifel an der Verhältnismäßigkeit. HRV – unterstützt von ESP, POL, CZE, PRT, HUN – sprach sich für Aufdeckungsanordnungen in interpersonellen Kommunikationsdiensten aus; das Recht auf Privatsphäre gelte nicht absolut, CSAM werde häufig über interpersonelle Kommunikationsdienste geteilt. ESP betonte die Pflicht zum Schutz von Kindern und Jugendlichen, die in verschiedenen europa- und völkerrechtlichen Dokumente festgehalten worden seien; die CSA-VO dürfe nicht hinter diesen Standards zurückfallen.

JD Rat führte aus, dass bei der Prüfung der Rechtmäßigkeit von Aufdeckungsanordnungen zwischen öffentlich zugänglichen Bereichen und interpersoneller Kommunikation zu unterscheiden sei. Bzgl. öffentlich zugänglicher Bereiche gebe Fallrecht zu ähnlich gelagerten Sachverhalten Anhaltspunkte (EuGH, Urteil vom 3. Oktober 2019 – C-18/18 sowie EuGH, Urteil vom 26. April 2022 – C-401/19). Hinsichtlich Aufdeckung in öffentlichen Diensten bestünde danach ein sehr geringes rechtliches Risiko. Bzgl. interpersonelle Kommunikation gebe es weniger Fallrecht; Entscheidungen in diesen Bereichen bezögen sich sehr spezifisch auf die jeweiligen Daten, sie eigneten sich daher weniger für Rückschlüsse auf die CSA-VO. Soweit möglich ließe sich ableiten, dass die Zweckbestimmung (Bekämpfung schwerer Straftaten) von großer Bedeutung sei. Außerdem habe der Gerichtshof in der Vergangenheit bzgl. Inhaltsdaten deutlich restriktiver als bzgl. Metadaten geurteilt. JD Rat kündigte ein schriftliches Gutachten an (Zeitpunkt der

Veröffentlichung blieb unklar). Vorläufig ließe sich festhalten, dass bzgl. interpersoneller Kommunikationsdienste mit Blick auf bisheriges Fallrecht rechtliche Risiken bestünden.

KOM betonte, dass 2/3 der derzeitigen CSAM-Meldungen ihren Ursprung in interpersonellen Kommunikationsdiensten fänden. KOM habe sich für eine Differenzierung zwischen den unterschiedlichen Inhaltstypen entschieden, da dies ein abgestuftes Vorgehen ermögliche. Für Maßnahmen, die allgemein und unterschiedslos gelten, hab der EuGH zwischen dem Zweck der Bekämpfung schwerer Straftaten und dem Schutz der öffentlichen Sicherheit differenziert. Allerdings sehe die CSA-VO spezifische, zeitlich begrenzte, zielgerichtete Maßnahmen vor. Anders als bei „Offlinedelikten“, würden Daten nicht (nur) zur Ermittlung des Täters benötigt, vielmehr stellten im Fall von CSAM die Inhaltsdaten selber bereits die Straftat dar. Angesichts der Pflicht zum Schutz von Kindern und Jugendlichen stelle es ebenfalls ein hohes rechtliches Risiko dar, keine geeigneten Maßnahmen zur Bekämpfung von CSAM zu ergreifen. FRA, HUN und IRL baten um schriftliche Übermittlung der juristischen Positionen.

(5) Artikel 12 ff. VO-Entwurf

Zu Artikel 12: Vors. erwog, die Informationspflicht des Nutzers auf die empfangende Behörde zu übertragen. DNK legte zu diesem Vorschlag einen PV ein; setzte sich für eine Verlängerung der Fristen in Artikel 12 Abs. 2 und für eine direkte Meldung an nationale Behörden ein. Wir legten ebenfalls PV ein; LEAs sollten nicht überlastet, Doppelung von Melde- und Informationswegen verhindert werden. Aus KOM Sicht liege die Zuständigkeit für den Empfang von Meldungen bereits zu großen Teilen bei den nationalen Behörden, diese legten auch die Aussetzung der Informationspflicht fest. Es sei allerdings naheliegend die Information des Nutzers durch den Diensteanbieter vorzunehmen. POL begrüßte Änderungen in Art. 12 – insbesondere auch die Verlängerung der Aussetzung der Informationspflicht in Abs. 2. Eine Verlagerung der Informationspflicht auf Strafverfolgungsbehörden sei insbesondere mit Blick auf die hohe Zahl erwarteter Meldungen zu prüfen.

KOM führte aus, dass mit der Gründung eines unabhängigen EU-Zentrums, der bisherigen Abhängigkeit von privaten Akteuren, die im außereuropäischen Ausland ansässig sein, ein starker europäischer Partner, der hohen EU-rechtlichen Standards unterliege, gegenübergestellt werde. Damit werde auch EP-Forderung aus den Verhandlungen der „Interims-VO“ aufgegriffen. Soweit doppelte Meldungen der Anbieter (an NCMEC und das geplante EU-Zentrum) nicht verhindert werden können, müsse sichergestellt werden, dass LEAs keine doppelten Meldungen empfangen. Dazu müsste das EU-Zentrum nach Prüfung von false-positives Meldungen ggf. zusammenführen. FRA fragte, wie Doppelungen in solchen MS zu verhindern seien, die Meldungen direkt von NCMEC empfangen. KOM führte aus, dass NCMEC die Meldungen derzeit nicht an die MS übersende, sondern online zur Verfügung stelle, sodass MS darauf zugreifen können. Diese Praxis sei auch nach der CSA-VO zulässig.

Zu Artikel 13: BEL setzte sich für eine stärkere Einbeziehung von Hotlines bei Meldungen (bspw. als trusted flaggers), insbesondere zur Beurteilung der Dringlichkeit von Meldungen ein. ITA und PRT begrüßten Änderung in lit f. NDL fragte ob Art. 13 lit. c auch Audioaufnahmen erfasse. HRV, POL, ITA, ROM und HUN unterstützten bisherige Formulierung in Art. 13 lit c. Anbieter könnten nicht beurteilen, welche Daten „relevant“ seien, dies sei nur den Strafverfolgungsbehörden möglich. KOM führte aus, dass mit Artikel 13 (i.V.m. Annex III) sichergestellt werde, dass alle Meldungen „actionable“ seien. Dies sei

derzeit nicht bei allen NCMEC-Meldungen gewährleistet. Artikel 13 lit h weise auf parallele Meldungen an NCMEC hin. Artikel 13 lit j und Artikel 48 sähen bereits den Hinweis auf die Dringlichkeit von Meldung vor. Annex III Punkt 8 sehe vor, den Ursprung der Meldung anzuzeigen. Annex III Punkt 3 spezifiziere den Umfang von Artikel 13 lit c. Danach sei im Falle einer Meldung von Audiokommunikation ggf. auch dazugehöriges Bild-, Ton- oder Videomaterial zu übermitteln.

Zu Artikel 14: FRA, IRL, CYP, POL und BEL sprachen sich für die Streichung von „under the jurisdiction of that Member State" in Artikel 14 Abs. 1 aus. Der Passus sei mit Blick auf Art. 14a obsolet. PRT wies daraufhin, dass es den MS überlassen bleiben müsse, die zuständige nationale Behörde zu benennen. FRA forderte eine Verkürzung der Frist in Abs. 2 auf eine Stunde in Angleichung zur TCO-VO: Annex IV sei für die Praxis nicht praktikabel.

Vors. schlug vor Abs. 3a deutlich zu kürzen. BEL und HRV sprachen sich für eine vollständige Streichung des Absatzes aus. Wir trugen weisungsgemäß vor, dass sich die Regelung in Abs. 3a für innerstaatliche Sachverhalte als wenig praktikabel darstelle, Abhilfe könne ggf. über Artikel 15 Abs. 1 gefunden werden, Position wurde von IRL unterstützt. Mehrere MS wiesen auf Schwierigkeiten im Verhältnis der nationalen Behörden zueinander hin, die eine Umsetzung des Abs. 3a in Jetziger Fassung erschwere. Wir trugen weisungsgemäß zu Abs. 5 vor, dass die Information über die Nichtausführung direkt an die Koordinierungsbehörde übermittelt werden sollte. Vors. führte aus, dass sich in diesem Zusammenhang ggf. auch Änderungsbedarf in Abs. 7 ergebe. Vors. werde dazu einen Kompromisstext übermitteln, der die Prozesse verschlanke. ITA fragte, ob in Abs. 6 nicht auch das EU-Zentrum zu berücksichtigen sei. KOM führte aus, dass die Verwaltungsbehörden über jeden Verfahrensschritt informiert werden müssten, das EU Zentrum sei gem. Abs. 7 abschließend zu informieren.

Zu Artikel 14a: IRL begrüßte Art. 14a insgesamt, Bedenken bestünden allerdings bzgl. Abs. 4, Adressat sollte hier die zuständige Behörde in dem anfragenden MS sein; IRL daher für eine Streichung von Abs. 4, Anbieter erhielten dadurch weitergehende Rechte als bei nationalen Anordnungen. DNK und EST äußerten Bedenken bzgl. Art. 14a mit Blick auf jeweilige nationalen Verfassungen. Wir trugen weisungsgemäß zu Artikel 14a vor. KOM äußerte Zweifel an der Einführung des Art. 14a, sofern die MS eine Übernahme der Regelung aus der TCO-VO in die CSA VO anstrebten, sei Art. 14a anzupassen. Vors. kündigte Überarbeitung des Art. 14a an.

Zu Artikel 15: Aus DNK und PRT Sicht sei die Frist in Art. 15 Abs. 4 zu kurz bemessen: „necessary" in Abs. 4 Satz 1 sei zu spezifizieren.

Zu Artikel 16 führte Vors. aus, dass Sperranordnungen bei URLs ansetzten. Dabei sei es regelmäßig nur möglich, ganze Websites zu sperren. Hier gelte es, die grundrechtliche Balance zu wahren, Artikel 16 werfe noch eine Reihe von Fragen auf. Gleichzeitig stelle die Sperrung von Inhalten eine sehr wichtige Maßnahme dar, um gegen Inhalte vorzugehen, die in Drittstaaten gehostet werden. Etablierte und effektive Systeme zum Sperren von Inhalten gebe es in DNK und FRA. Die Diskussion zu diesem Artikel werde in der nächsten Sitzung fortgeführt.

TOP 2: AOB

KOM kündigte eine Infografik zu Kindesmissbrauch an. Dazu werde sie die MS bitten, die zuständigen nationalen Stellen zu benennen.