Hintergrundpapier zum Vorschlag für eine Verordnung zur Verhinderung und zur Bekämpfung von Kindesmissbrauchsinhalten (CSAM-Verordnung)

Am 11. Mai 2022 hat die EU-Kommission den Vorschlag für eine Verordnung zur Verhinderung und zur Bekämpfung von Kindesmissbrauchsinhalten verabschiedet und veröffentlicht. Nach einer ersten Analyse möchte eco insbesondere auf folgende Punkte hinweisen.

I. Geplante Verpflichtungen für Anbieter von Online-Diensten

- **Risk-Assessment und Risk-Mitigation**

Vorgaben für Hosting-Anbieter und Anbieter interpersoneller Kommunikationsdienste

Hosting-Anbieter und Anbieter interpersoneller Kommunikationsdienste sollen anbieter- und dienstspezifisch für jedes „Produkt“ das potenzielle Risiko in Bezug auf „online child sexual abuse” (im Sinn der Verordnung die Verbreitung von Darstellungen des sexuellen Missbrauchs Minderjähriger sowie Grooming-Aktivitäten im digitalen Raum) bewerten. Wird ein potenzielles Risiko bejaht, sollen effektive, zielgerichtete und verhältnismäßige „Vorsorgemaßnahmen“ zur Minimierung des Risikos ergriffen werden. Zudem soll von den Providern bzw. Diensteanbietern ein Bericht zu Prozess und Ergebnis der Risikobewertung sowie zu den geplanten Vorsorgemaßnahmen an die sogenannte "Coordinating Authority“ (Koordinierungsbehörde) des jeweils zuständigen Mitgliedsstaates übermittelt werden.

Für die Risikobewertung soll unter anderem entscheidend sein, ob in der Vergangenheit in Bezug auf das zu bewertende Produkt bzw. den zu bewertenden Dienst „online child sexual abuse“ bekannt wurde, welche Regeln zum Umgang damit existieren, welche Prozesse etabliert sind, welche Nutzung durch die Anwender:innen vorgesehen oder möglich ist und inwieweit Minderjährige den Dienst nutzen. In Bezug auf Minderjährige ist die Altersgruppe und der entsprechende Gefährdungsgrad zu bewerten; vorgesehene Altersverifizierungen können ein Risiko abschwächen. Dabei sind auch Funktionen des Dienstes mit einem potenziellen Grooming-Risiko (z.B. Teilen von Bildern/Videos, Suche nach anderen Nutzer:innen, direkte Kontaktmöglichkeiten etc.) zu berücksichtigen.

Als „Vorsorgemaßnahmen“ werden beispielhaft aufgezählt: Content Moderation, strikte AGB-Regelungen, interne Prozesse zum Umgang mit „online child sexual abuse“ inklusive interner „Aufsicht“, Anpassen der „Produkte“ mit dem Ziel weniger risikobehafteter Nutzungsmöglichkeiten sowie Kooperationen mit Mitbewerbern und Stakeholdern (Behörden, Zivilgesellschaft, Trusted Flaggern). In Bezug auf Grooming werden Altersverifizierungs- und Alterseinschätzungsmaßnahmen vorgeschlagen, um Minderjährige identifizieren und schützen zu können.

Diese Vorgaben für Hosting-Anbieter und Anbieter von interpersonellen Kommunikationsdiensten werfen eine Vielzahl von Fragestellungen auf.

In Bezug auf Anbieter von Hosting-Diensten wird nicht nach den unterschiedlichen Arten und Angeboten von Hosting-Dienstleistungen differenziert. Neben den „klassischen Hosting-Anbietern“ unterfällt auch das Speichern von Inhalten in sozialen Netzwerken und auf anderen Plattformen (zum Beispiel Image-/File-Hoster) dem Anbieten von Hosting-Diensten. Die vielfältigen Hosting-Dienstleistungen haben jeweils unterschiedliche Handlungsoptionen. Hierdurch und durch die mangelnde Differenzierung im Verordnungsvorschlag ist unklar, wer im Einzelfall in Bezug auf die konkreten Hosting-Dienstleistungen die Verpflichtungen erfüllen soll, mithin Adressat der Vorgaben ist. In der Regel hat der klassische Hosting-Anbieter (im Gegensatz zu seinen Kund:innen/ Nutzer:innen) keine Kenntnis darüber, welche Anwendungen, Dienste und Inhalte die Nutzenden auf dem Server speichern oder zu welchem Zweck. Auch ist beispielsweise unklar, wie weit eine Unterteilung in bereitgestellte Hosting-Dienste für die Bewertung vorgenommen werden muss. Diese könnte nach virtuellen oder physischen Servern erfolgen oder nach Kunde/Kundin bzw. Produkt. Zudem liegt es vielfach in der Natur des Dienstes, keine Möglichkeit der Kenntnis von den genutzten Anwendungsmöglichkeiten bzw. den auf den Systemen gespeicherten Daten zu haben. Es ist daher zweifelhaft, ob insbesondere klassische Hoster in der Praxis die im Verordnungsentwurf vorgeschlagene Risikobewertung werden umsetzen können.

Bei international agierenden Anbietern stellt sich weiter die Frage, ob der Sitz oder der jeweilige Serverstandort für das Bestehen der Verpflichtung entscheidend ist.

Fraglich erscheint auch, inwieweit die Vorsorgemaßnahmen freiwillige Suchmaßnahmen ermöglichen sollen/können. Der Verordnungsvorschlag lässt dies offen. Vertreter der EU-Kommission haben zumindest in öffentlichen Veranstaltungen zu dem Thema mitgeteilt, dass nach der CSAM-Verordnung zukünftig eine freiwillige Suche nicht mehr möglich sei.

Der Einsatz von Maßnahmen zur Altersverifikation, zur Minimierung der Grooming-Risiken, scheint äußerst bedenklich. Diese Maßnahmen sind mit den Grundsätzen von Datenschutz, Datensparsamkeit und Privatsphäre nicht zu vereinbaren. Dies betrifft sowohl Erwachsene als auch Kinder.

App-Store-Anbieter

App-Store-Anbieter sollen im Rahmen einer Risikobewertung (gegebenenfalls zusammen mit den App-Anbietern) Anstrengungen unternehmen, um das Grooming-Risiko der verfügbaren Apps zu bewerten, und anschließend durch Vorsorgenmaßnahmen sogenannte “child users” (im Sinn der Verordnung Minderjährige bis 16 Jahre) vor entsprechend risikobehafteten Apps schützen. Als Vorsorgemaßnahmen werden insoweit Altersverifizierungs- und Alterseinschätzungsmaßnahmen, Hinweise auf die Risikobewertung sowie Zugriffsbeschränkungen auf entsprechende Apps benannt.

Die vorgeschlagenen Maßnahmen erscheinen in mehrfacher Hinsicht problematisch. Zum einen stellt sich die Frage der technischen Machbarkeit. Zum anderen stellen die Maßnahmen für die Praktikabilität jedenfalls eine große Hürde dar.

App-Store-Anbieter werden regelmäßig nicht in der Lage sein, alle bereitgestellten Apps den Vorgaben entsprechend zu prüfen und zu bewerten. Insbesondere KMUs, kostenlose Angebote oder Community-Projekte, die App-Stores anbieten oder betreiben, sind nicht in der Lage diese Vorgaben zu erfüllen. Eine Umsetzung der Pflicht könnte allenfalls durch eine Einschätzung und Kennzeichnung des Grooming-Risikos durch die jeweiligen Anbieter der App denkbar sein.

Darüber hinaus erscheint eine altersabhängige Kontrolle bzw. Beschränkung in der Praxis problematisch. Auf internationaler Ebene, ja sogar innerhalb Europas, gibt es keine einheitliche Definition von Grooming. Eine vorsorgliche grundsätzliche „Ausblendung“ jeglicher Applikationen und Dienste, die eine Möglichkeit zur Kommunikation im weiteren Sine beinhalten, für Minderjährige wäre schwer mit dem wichtigen Teilhabegedanken eines modernen Jugendmedienschutzes zu vereinbaren. Eine allgemeinverpflichtende Altersverifikation aller Nutzenden (Erwachsener und Minderjähriger) wäre datenschutzrechtlich bedenklich.

- **Proaktive Suche**

Die vorgeschlagene Verordnung sieht vor, dass auf befristete Anordnung (sogenannte „detection order“) hin, Hosting-Anbieter sowie Anbieter von interpersonellen Kommunikationsdiensten aktiv nach bekannten und/oder neuen Missbrauchsdarstellungen sowie Grooming-Fällen suchen müssen. Diese Verpflichtung ist an verschiedene weitergehende Vorgaben gekoppelt, insbesondere: Transparenz gegenüber den Nutzer:innen, Berichtspflicht zur Umsetzung gegenüber der in den Mitgliedstaaten einzurichtenden Behörde und Meldepflicht bei CSAM Funden.

Die „detection order“ soll auf Ebene der Mitgliedsstaaten, nach Durchlaufen eines mehrstufigen Verfahrens (u.a. unter Beteiligung der Datenschutzbehörden) und unter Abwägung aller betroffenen Grundrechte erteilt werden. Die materiellen Voraussetzungen für die Erteilung einer „detection order“ durch die zuständigen Behörden in den Mitgliedstaaten sind mangels klar definierter Vorgaben jedoch sehr niedrigschwellig. Es genügt grundsätzlich ein „signifikantes Risiko für online child sexual abuse“. Hierfür soll die „Wahrscheinlichkeit trotz Vorsorgemaßnahmen” bzw. die Verbreitung von „online child sexual abuse“ auf dem betroffenen Dienst in den letzten 12 Monaten ausreichen. Wenn der Dienst/ das Produkt neu ist, soll genügen, wenn vergleichbare Produkte anderer Anbieter betroffen waren. In Bezug auf die Verpflichtung zur Suche nach neuen Inhalten bzw. nach Grooming-Fällen werden die Voraussetzungen für eine Anordnung um ebenfalls niedrigschwellige Vorgaben ergänzt. Hervorzuheben ist insoweit die Vorgabe, dass eine Suchanordnung in Bezug auf Grooming nur interpersonelle Kommunikation mit Nutzer:innen bis 16 Jahren erfassen soll.

Für die Umsetzung ist zwar keine spezielle Technologie vorgegeben; sie muss allerdings effektiv, zuverlässig, „state of the art“ und so wenig eingreifend wie möglich sein. Hierzu können Unternehmen eigene technologische Lösungen einsetzen oder eine durch das EU-Zentrum noch bereitzustellende Technologie verwenden. Für die einzusetzenden Indikatoren für die Suche (Hashwerte, KI etc.) hingegen ist vorgegeben, dass diese zwingend durch das EU-Zentrum bereitgestellt sein müssen.

Es ist aufgrund des Auslaufens der temporären e-Privacy Derogation für Anbieter von interpersonellen Kommunikationsdiensten sowie des Zusammenspiels von CSAM Verordnung und Digital Services Act faktisch eine umfassende und allgemeine Suchpflicht, wohlmöglich mit einer „stay down“-Verpflichtung, zu erwarten.

eco sieht die vorgeschlagene Suchpflicht sehr kritisch.

Die EU-Kommission hat mehrfach – im Rahmen der Veröffentlichung des Verordnungsvorschlags sowie auf Rückfragen hin – betont, dass eine freiwillige Suche aufgrund mangelnder Beteiligung nicht ausreiche. In der Folge muss davon ausgegangen werden, dass seitens der EU-Kommission eine niedrigschwellige Einstiegshürde für die „detection order“ intendiert ist und damit die Möglichkeit für ein verpflichtendes proaktives dauerhaftes Monitoring eröffnet werden soll.

Bedenklich ist zudem die Unklarheit darüber, ob immer alle materiellen Voraussetzungen für die „detection order“ erfüllt sein müssen, oder ob es sich bei den Voraussetzungen um eine „oder-Aufzählung“ handelt. Die grundsätzlichen Bedenken hinsichtlich einer umfassenden Suchpflicht lassen sich jedenfalls nicht durch das vorgeschlagene Verfahren minimieren.

Erhebliche Bedenken hat eco auch in Bezug auf die Einbeziehung verschlüsselter Kommunikation in die Suchpflicht. Eine Schwächung von Verschlüsselungstechnologien birgt massive Sicherheitsrisiken. Damit verbunden sind erhebliche Auswirkungen auf die Vertraulichkeit und Integrität digitaler Kommunikation von Wirtschaft und Bürger:innen, die weit über die Problematik von CSAM hinaus gehen. Eine Schwächung von Verschlüsselungstechnologien wird daher von eco strikt abgelehnt.

Inwiefern eine freiwillige Suche durch Anbieter interpersoneller Kommunikation künftig noch erwünscht und möglich sein wird, ist unklar. So läuft die temporäre Derogation als rechtliche Grundlage für entsprechende Suchmaßnahmen zum Beispiel in Messengern aus. Freiwillige proaktive Suchmaßnahmen sind in dem Entwurf der CSAM Verordnung nicht explizit vorgesehen.

Der Ansatz, ausschließlich validierte Indikatoren für die Umsetzung der „detection order“ zu verwenden, ist nachvollziehbar, würde aber für international tätige Unternehmen bedeuten, dass für Europa gesonderte Hash-Datenbanken eingesetzt werden müssten. Hier stellt sich die Frage sowohl der Praktikabilität als auch der Umsetzbarkeit für die Unternehmen.

Auch die Einbeziehung von Grooming in die Suchpflicht stößt auf erhebliche rechtliche und technische Bedenken. Insbesondere besteht auf europäischer Ebene kein harmonisierter Rechtsrahmen. In den Mitgliedsstaaten existieren unterschiedliche Grooming-Definitionen und unterschiedliche Altersstufen. In technischer Hinsicht ist die unzuverlässige Erkennung von Grooming durch KI ein

maßgeblicher Faktor. Darüber hinaus darf nicht verkannt werden, dass die Einbeziehung von Grooming in die Suchpflicht eine massenhafte Überwachung privater sowie besonders geschützter Individual-Kommunikation zur Folge hätte. Eine Einschränkung auf Kommunikation mit Minderjährigen bis 16 Jahren erscheint in der Praxis fraglich und wäre mit erheblichen Auswirkungen auf den Datenschutz für alle Nutzenden verbunden (beispielsweise durch Identifikation bzw. Altersverifikation).

Grundsätzlich möchte eco darauf hinweisen, dass etwaige Suchpflichten für KMU eine besondere Herausforderung darstellen können. Die Berücksichtigung der Situation von KMU ist jedoch im europäischen Wirtschaftsraum essenziell. Es erscheint zweifelhaft, ob die besondere Situation der KMU ausreichend über die verfahrensrechtliche Frage nach „technological & financial capabilities“ berücksichtigt wird.

- **Meldung potenzieller online child sexual abuse Inhalte**

Die vorgeschlagene Verordnung sieht vor, dass Hosting-Anbieter und Anbieter interpersoneller Kommunikationsdienste bei Kenntnis von „potential online child sexual abuse“ die entsprechenden Inhalte an das EU Center über einen vorgegebenen Kommunikationsweg und unter Verwendung vorgegebener Formulare melden müssen. Über erfolgte Meldungen soll der betroffene Nutzer bzw. die betroffene Nutzerin informiert werden.

Flankierend müssen die Anbieter eine Funktion für Nutzer:innen bereithalten, mit der diese „potential online child sexual abuse“ an den Anbieter melden (flaggen) können.

eco sieht diesen Vorschlag sehr kritisch.

Der Verordnungsvorschlag zur Meldepflicht wird in der Praxis vielfach zu Doppelmeldungen und folglich zu deutlicher Mehrarbeit führen:

- Konstellation 1 - Meldung durch US-Anbieter:

  Amerikanische Anbieter sing gesetzlich verpflichtet, bei jeder Kenntnis von entsprechenden Inhalten NCMEC zu informieren. Stellt NCMEC einen Europabezug fest, erfolgt durch NCMEC eine Weiterleitung an europäische Strafverfolgungsbehörden (zum Beispiel bei einem deutschen Tatverdächtigen nach Deutschland an das BKA).
  Müssen die amerikanischen Anbieter künftig „online child sexual abuse“ auch an das EU Center melden, welches dann den Inhalt prüft und ggfs. an

die Strafverfolgungsbehörden in den jeweiligen Mitgliedsstaaten weiterleitet, kommt es sowohl zu einer Doppelmeldung seitens des Providers als auch in der Folge zu einer Doppelmeldung an die Strafverfolgungsbehörden.

- Konstellation 2 - Provider erhält durch eine Beschwerdestelle Kenntnis von „potential online child sexual abuse“:

  Beschwerdestellen arbeiten eng mit den Strafverfolgungsbehörden zusammen und informieren diese im Rahmen ihrer Beschwerdebearbeitung. Die deutschen Beschwerdestellen von eco, FSM und jugendschutz.net zum Beispiel informieren zuerst das Bundeskriminalamt (BKA) und erst nach einer vereinbarten Stillhaltefrist den Provider. Wenn der Provider zukünftig das EU Center informieren muss, welches dann das BKA informiert, kommt es zu einer Doppelmeldung an das BKA.

Darüber hinaus ist bei „geflaggten, unvalidierten Inhalten“ die unmittelbare Ausleitung von IP-Adressen und Nutzerdaten ohne vorhergehende staatliche Prüfung und Bewertung rechtsstaatlich bedenklich.

Nicht eindeutig scheint auch der Zeitpunkt der Information an die betroffenen/ gemeldeten Nutzenden. Das Verhältnis von Art. 12 Absatz 2 zu Absatz 3 kann gegebenenfalls eine doppelte Informationspflicht auslösen. Sofern dies gewollt ist, besteht das Risiko der Täterwarnung. Jedenfalls bedarf es einer entsprechenden Klarstellung.

Die allgemeine und undifferenzierte Pflicht zum Vorhalten einer Melde-/ Flaggingfunktion ist insbesondere im Hinblick auf klassische Hoster auf ihren tatsächlichen praktischen Nutzen zu hinterfragen. Denn im Regelfall ist es für Nutzer:innen nicht ersichtlich, bei welchem Hosting-Anbieter ein Inhalt gehostet ist und an wen man einen Hinweis richten sollte. Sofern klassische Hoster dennoch eine Meldeinfrastruktur vorhalten sollen, muss diese praxistauglich sein. Aus Sicht von eco muss beispielsweise in dieser Fallkonstellation ausreichend sein, wenn der Hoster zentral auf seiner eigenen Webpräsenz eine Meldeoption zur Verfügung stellt. Nicht umsetzbar und praktikabel ist eine durch den Hoster zu implementierende und zu verantwortende Flaggingfunktion auf jeder Webpräsenz seiner Kund:innen. Für Flaggingfunktionen auf einzelnen Webpräsenzen wäre sinnvoller Weise beim Anbieter des jeweiligen Dienstes als Verantwortlichen anzusetzen, da deren Handlungsmöglichkeiten mit denen von Plattformanbietern verglichen werden können.

Daneben wäre es sinnvoll, klassichen Hostern (insbesondere KMUs) zur Umsetzung der Verpflichtung die Möglichkeit einzuräumen, mit zentralen neutralen

Anlaufstellen (zum Beispiel die etablierten Beschwerdestellen) zur Entgegennahme von Hinweisen/Meldungen zu kooperieren. Beispielsweise wäre bei entsprechender Kooperation eine Verlinkung zu den Meldeformularen der Beschwerdestellen statt des Vorhaltens einer eigenen Meldeinfrastruktur denkbar.

- **Strikte Lösch-Vorgaben**

Die geplante Pflicht für Hosting-Anbieter, auf Anordnung CSAM innerhalb von 24 Stunden zu löschen oder innerhalb der EU den Zugang zu diesen Inhalten zu sperren, wird flankiert durch eine Pflicht zur Rückmeldung über die ergriffenen Maßnahmen gegenüber der Koordinierungsbehörde und dem EU-Zentrum. Zudem müssen grundsätzlich spätestens nach sechs Wochen (bzw. bei Verlängerung der Schweigepflicht spätestens nach 12 Wochen) betroffene Nutzer:innen über die Sperrung und das Beschwerderecht informiert werden.

Für die Anordnung muss ein Inhalt durch die Koordinierungsbehörde, ein Gericht oder eine andere vom Mitgliedstaat benannte “independent administrative authority“ als CSAM bewertet worden sein. Ist dies der Fall, kann die Koordinierungsbehörde die Order beantragen, die nach anschließender Prüfung von der Justiz- oder Verwaltungsbehörde erteilt wird.

Unabhängig von diesem mit dem vorliegenden Entwurf der Kommission zu etablierenden förmlichen Verfahren der Lösch-Order sollen zukünftig auch weiterhin informelle Notifizierungen der Hostprovider möglich sein, bei denen der Provider CSAM aufgrund von Hinweisen und Benachrichtigungen, z.B. durch Nutzende oder Beschwerdestellen, entfernt.

Im Hinblick auf die vorgegebene 24-Stunden-Frist zur Umsetzung der Lösch-Order gibt eco zu bedenken, dass diese strikte zeitliche Vorgabe in der Praxis in Einzelfällen nicht realisierbar sein kann. Dies betrifft insbesondere KMUs. Geringere personelle, technische wie finanzielle Ressourcen sollten hier berücksichtig werden. eco regt entsprechende Anpassungen des Verordnungsvorschlags an.

In Bezug auf die Information der betroffenen Nutzer:innen regt eco an, den Dialog mit den Strafverfolgungsbehörden zu suchen, um sicherzustellen, dass keine Beeinträchtigung der Ermittlungen und insbesondere tatsächlich keine unerwünschte Täterwarnung erfolgt.

Aufgrund der gut funktionierenden bestehenden Meldewege über Beschwerdestellen ist aus Sicht des eco die geplante Pflicht allenfalls als

Eskalationsstufe zu verstehen und in der Praxis nur in wenigen Fällen eine sinnhafte Ergänzung des bestehenden Regimes. Denn in den allermeisten Fällen werden die Hostprovider gemeldete/geflaggte Inhalte innerhalb kürzester Zeit ohne entsprechende Order, also freiwillig, entfernen. Sofern ein Hinweis zuerst bei einer Behörde eingeht, muss sichergestellt und gewährleistet werden, dass deren Verfahren im Interesse der Verhinderung weiterer Reviktimisierung zügig durchgeführt werden.

- **Access-Blocking/Netzsperren**

Die geplante Pflicht für Internetzugangsanbieter sieht auf (befristete) Anordnung hin Netzsperren für nicht in der EU gehostete CSAM-URLs vor, bei denen eine Löschung beim Hostprovider nicht erreicht werden kann. Die Sperrung geht mit einer Information der Nutzer:innen über die erteilten Blocking-Orders einher.

Für die Sperre ist verpflichtend eine URL-Liste zu verwenden, die vom EU-Zentrum erstellt und bereitgestellt wird. Im Rahmen des Erlasses einer Blocking-Order durch eine Justiz- bzw. Verwaltungsbehörde soll sichergestellt werden, dass die zu verwendende Liste aktuell ist und die Umsetzung der Netzsperre des Providers effektiv und zielgerichtet ist.

Die Koordinierungsbehörde muss die weitere Notwendigkeit der Blocking-Order zumindest jährlich überprüfen und die Order ggfs. anpassen bzw. zurücknehmen.

eco steht Netzsperren aus grundsätzlichen Erwägungen kritisch gegenüber. Netzsperren sind weder effektiv noch nachhaltig. Unabhängig davon weist das im Entwurf vorgeschlagene Verfahren eine Vielzahl an problematischen Aspekten und Fragestellungen auf.

Nach Ansicht des eco müssen die Ermittlung und die Strafverfolgung der Täter sowie die effektive und nachhaltige Löschung der Inhalte oberste Priorität haben. Entsprechend ist es essenziell, den Schwerpunkt der Bekämpfung von CSAM auf die internationale Zusammenarbeit und Kooperation bei der Strafverfolgung und Löschung zu legen. Bei funktionierenden Prozessen und Kooperationen lassen sich URLs mit CSAM auch international zuverlässig und schnell entfernen.

Dabei zeigt die Erfahrung der eco Beschwerdestelle mit grenzüberschreitenden CSAM Fällen, dass eine Löschung international schneller erreicht werden kann, wenn die Rechtslage im Hostingland in Bezug auf CSAM auch im Detail identisch ist mit der des meldenden Landes. eco erachtet es daher als unerlässlich, bei etwaigen Problemfällen die internationale Zusammenarbeit auszubauen bzw. zu stärken. Dabei ist es aus Sicht von eco unumgänglich, hier auch auf politischer Ebene aktiv zu werden und sich für eine weitere Rechtsangleichung bei CSAM einzusetzen. Dies gilt insbesondere vor dem Hintergrund, dass CSAM zwar prinzipiell international

geächtet und strafbar ist. Im Detail gibt es dennoch international unterschiedliche Maßstäbe bei der Definition von Missbrauchsdarstellungen von Kindern und Jugendlichen, sobald der Bereich der sogenannten „Baseline-Fälle“ (also Darstellungen von Missbrauchshandlungen an vorpubertären Minderjährigen) verlassen wird – selbst innerhalb der EU.

Prozedural erscheint aus Sicht des eco höchst fragwürdig, wie festgestellt werden kann, dass der Internetzugangsanbieter in den letzten 12 Monaten zum Aufruf von CSAM genutzt wurde. Dies würde voraussetzen, dass Zugangsanbieter das Nutzerverhalten und damit die aufgerufenen “Inhalte” überwachen. Das wiederum wäre unter Aspekten des Datenschutzes, des Verbots der allgemeinen Überwachungspflicht und des Fernmeldegeheimnisses höchst bedenklich.

Unabhängig davon, ist es aus Sicht des eco wichtig, über klare und einheitliche Vorgaben zu der Definition nicht löschbarer URLs sowie in Bezug auf die Aktualität der bereitgestellten URL-Blocking-Liste zu verfügen. Das Risiko eines Overblockings legaler und nicht zu beanstandender Inhalte muss weitestgehend ausgeschlossen/ bestmöglich begrenzt werden. Daher bedarf es einer regelmäßigen Aktualisierung und Überprüfung der in der Datenbank/Liste enthaltenen URLs auf CSAM durch das EU-Zentrum. Die regelmäßige Überprüfung dieser URLs muss aus Sicht von eco jeweils auch den Wechsel des Hostproviders umfassen. Wird im Rahmen der Überprüfung eine Veränderung des Hostings festgestellt, ist in Bezug auf die entsprechende URL umgehend ein neues „notice and takedown“-Verfahren zu initiieren, um den neuen Kontakt zu nutzen und dem Vorrang des Löschens von CSAM Rechnung zu tragen sowie durch die Löschung der weiteren Re-Viktimisierung der Opfer entgegenzuwirken.

Aktualisierungen der URL-Liste müssen den von Sperr-Anordnungen betroffenen Internetzugangsanbietern mindestens täglich bereitgestellt werden.

II. Umsetzung/Durchsetzung der Verordnung

- **Festlegung zuständiger bzw. koordinierender Behörden in den Mitgliedsstaaten**

Für die Umsetzung bzw. Durchsetzung der Verordnung sollen in den Mitgliedsstaaten „zuständige Behörden“ bzw. „Koordinierungsbehörden“ etabliert und damit eine neutrale Instanz in den Mitgliedsländern geschaffen werden. Hierzu sieht der Verordnungsvorschlag Kriterien vor, die in der Konsequenz neue Strukturen etablieren.

Der Vorschlag bedingt, dass nicht auf bereits bestehende Strukturen und etablierte Akteure zurückgegriffen werden kann und bereits vorhandene Kooperationen und Synergien nicht genutzt, ausgebaut und intensiviert werden. Diesbezüglich regt eco dringend an, die Vorgaben anzupassen und eine starke Einbeziehung der etablierten Strukturen sowie Kooperationen der verschiedenen Akteure und deren Expertise auf Ebene der Mitgliedsstaaten zu ermöglichen. Der Wunsch der EU-Kommission nach Neutralität wäre hierdurch nach Ansicht von eco nicht gefährdet.

- **Etablierung eines eigenen EU-Zentrums**

Ein EU-Zentrum soll als eigene, unabhängige Einrichtung (Behörde oder behördenähnlich) fungieren. Dessen Aufgabe soll es insbesondere sein, die unterschiedlichen Akteure bei der Umsetzung der Verordnung und die Erfüllung der neuen Verpflichtungen zu unterstützen (zum Beispiel im Bereich der Durchführung von Risikobewertungen, Suchverpflichtungen und Sperrverpflichtungen). Das EU-Zentrum soll sogenannte Indikatoren für die Umsetzung von Such- und Sperrverpflichtungen (Hash- und URL-Listen) bereitstellen und darüber hinaus Meldungen der Anbieter zu potenziellem „online child sexual abuse“ entgegennehmen und bewerten.

Durch die Etablierung eines eigenen EU-Centers kommt es zu einem Nebeneinander von EU-eigener Einrichtung und dem etablierten Beschwerdestellennetzwerk INHOPE (als Dachverband sowie die einzelnen Beschwerdestellen als jeweiliges INHOPE-Mitglied), wobei EU-Center und INHOPE-Netzwerk das gemeinsame Ziel der Bekämpfung von CSAM haben. Daher regt eco an, bestehende Strukturen und Kooperationen ausdrücklich einzubeziehen und auf deren Tätigkeiten und Erfahrungen aufzubauen.

Das INHOPE Netzwerk mit seinen Beschwerdestellen ist seit über 20 Jahren in vielen Bereichen tätig, die nach dem Verordnungsentwurf zukünftig auch dem einzurichtenden EU-Zentrum obliegen sollen (u.a. die Bewertung von gemeldeten Inhalten, die Zusammenarbeit mit Strafverfolgungsbehörden und Hostprovidern).

Aus Sicht von eco ist es wichtig sicherzustellen, dass bisherige effektive Maßnahmen zur CSAM-Bekämpfung weiterhin beibehalten werden und folglich das INHOPE-Netzwerk auch zukünftig als integraler Bestandteil der CSAM-Bekämpfung einbezogen wird. Hierfür erscheint eine entsprechende Klarstellung im vorgeschlagenen Verordnungstext dringend erforderlich.

- **Technologie für die Umsetzung von Suchverpflichtungen**

Der Verordnungsentwurf sieht vor, dass im Falle einer Suchverpflichtung das betroffene Unternehmen auf Technologien zurückgreifen kann, die durch das EU-Zentrum bereitgestellt werden sollen.

Diese, auf den ersten Blick unterstützend wirkende Möglichkeit, wird in der Praxis erhebliche Herausforderungen mit sich bringen. Letztlich hat jeder Provider sein eigenes technisches Setting. In der Praxis herrscht eine große Vielfalt der genutzten Technologien. Die Integration einer bereitgestellten Technologie hat immer die Herausforderung, dass sie mit der vorhandenen technischen Infrastruktur kompatibel sein muss. eco sieht das Risiko, dass dies bei der Bereitstellung von Technologie durch das EU-Zentrum nicht ausreichend berücksichtigt ist.

Kann der Provider aufgrund mangelnder Kompatibilität nicht auf Technologien des EU Centers zurückgreifen, muss er kurzfristig mit eigenen Mitteln und Aufwänden für das Vorhandensein von Suchtechnologien sorgen, die effektiv, zuverlässig, state of the art und so wenig eingreifend wie möglich sind. Diese Entwicklung dürfte einige Zeit in Anspruch nehmen und gegebenenfalls länger dauern als der Zeitraum, welcher den Unternehmen nach Erlass der „detection order“ für den Beginn der Suchmaßnahmen zugestanden wird (drei bis 12 Monate).

- **Sanktionen**

Der Vorschlag sieht vor, dass Mitgliedstaaten Sanktionen in Höhe von maximal sechs Prozent des weltweiten Jahresumsatzes festsetzen.

Der Bußgeldrahmen orientiert sich zwar an den Gesetzesvorhaben der letzten Zeit, ist aus Sicht des eco dennoch zu hoch bemessen. Gerade im Hinblick auf die große Diversität der betroffenen Unternehmen und die Einbeziehung von KMUs mit geringeren Ressourcen regt eco eine Herabsetzung des Bußgeldrahmens an.