Förmliche Stellungnahme des EDSB zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte

1. Einleitung und Hintergrund

- Diese förmliche Stellungnahme zu dem von der Europäischen Kommission am 12. September 2018 angenommenen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte (im Weiteren „der Vorschlag“)[1] erging durch den EDSB gemäß Artikel 57 Absatz 1 Buchstabe g und Artikel 58 Absatz 3 Buchstabe c der Verordnung (EU) Nr. 2018/1725[2].

- Ziel des Vorschlags ist die Schaffung von abgestimmten Regeln für Hostingdiensteanbieter, die ihre Dienste – unabhängig von ihrem Niederlassungsort – in der Union anbieten, um die Verbreitung terroristischer Inhalte durch ihre Dienste zu verhindern und ihre rasche Entfernung sicherzustellen.

- Durch den Vorschlag werden eine Reihe von Sorgfaltspflichten für Hostingdiensteanbieter definiert und verschiedene Pflichten für zuständige Behörden der Mitgliedstaaten in Bezug auf die Durchsetzung des Vorschlags festgelegt. Insbesondere werden durch den Vorschlag folgende Maßnahmen eingeführt:

  - Hostingdiensteanbieter müssten angemessene, sinnvolle und verhältnismäßige Maßnahmen gegen die Verbreitung von terroristischen Inhalten ergreifen und insbesondere Nutzer vor terroristischen Inhalten schützen (Artikel 3);
  - Hostingdiensteanbieter wären verpflichtet, die terroristischen Inhalte innerhalb einer Stunde nach Eingang der durch eine zuständige Behörde eines Mitgliedstaats erlassenen Entfernungsanordnung zu entfernen oder den Zugang zu diesen Inhalten zu desaktivieren (Artikel 4);
  - Hostingdiensteanbieter müssten auf der Grundlage von Meldungen durch zuständige Behörden der Mitgliedstaaten oder durch Einrichtungen der Union (wie Europol) beurteilen, ob die in der Meldung bezeichneten Inhalte gegen die jeweiligen Geschäftsbedingungen der Hostingdiensteanbieter verstoßen, und entscheiden, ob diese Inhalte zu entfernen oder der Zugang zu ihnen zu desaktivieren ist oder nicht (Artikel 5);
  - Hostingdiensteanbieter müssten proaktive Maßnahmen zum Schutz ihrer Dienste vor der Verbreitung terroristischer Inhalte durchführen, unter anderem

[1] COM (2018) 640 final, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte. Richtlinie 2008/115/EG des Europäischen Parlaments und des Rates vom 16. Dezember 2008 über gemeinsame Normen und Verfahren in den Mitgliedstaaten zur Rückführung illegal aufhältiger Drittstaatsangehöriger

[2] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG Text von Bedeutung für den EWR (ABl. L 295 vom 21.11.2018).

Postanschrift: rue Wiertz 60 - 1047 Brüssel, Belgien
Dienststelle: rue Montoyer 30
Email: edps@edps.europa.eu - Internetseite: www.edps.europa.eu
Tel.: +32 (0)2 283 19 00 – Fax: +32 (0)2 283 19 50

durch Einsatz automatisierter Werkzeuge zur Bewertung der gespeicherten Inhalte (Artikel 6);
- Hostingdiensteanbieter müssten die entfernten Inhalte und entsprechende Daten, die für spätere Verwaltungs- oder Gerichtsverfahren und die Verhinderung, Erkennung, Untersuchung oder strafrechtliche Verfolgung von Terroranschlägen notwendig sind, aufbewahren (Artikel 7);
- Hostingdiensteanbieter müssten einen relevanten Beschwerdemechanismus einführen, anhand dessen Personen, deren Inhalte aufgrund einer Meldung oder einer proaktiven Maßnahme entfernt wurden, Beschwerde beim Hostingdiensteanbieter einlegen können (Artikel 10);
- Hostingdiensteanbieter müssten Informationen an jene Personen übermitteln, deren Inhalte aufgrund einer Entfernungsanordnung, einer Meldung oder einer proaktiven Maßnahme entfernt wurden (Artikel 11);
- Mitgliedstaaten müssten eine oder mehrere Behörden festlegen, die für die Ausstellung von Entfernungsanordnungen, die Erkennung oder Identifizierung terroristischer Inhalte und deren Meldung an die Hostingdiensteanbieter, die Aufsicht über die Durchführung der proaktiven Maßnahmen und die Durchsetzung der durch den Vorschlag geschaffenen Pflichten durch die Auferlegung von Sanktionen zuständig sind (Artikel 17).

- Der EDSB versteht die Notwendigkeit der Bekämpfung der Verbreitung von terroristischen Online-Inhalten sowie der Festlegung von diesbezüglichen Sorgfaltspflichten für Hostingdiensteanbieter und unterstützt die Ziele des Vorschlags. Er empfiehlt **mögliche Verbesserungen**, um **jeden möglichen „Konflikt" mit den Grundrechten auf Privatsphäre und auf den Schutz personenbezogener Daten** wesentlich zu **reduzieren** und um letztendlich die Einhaltung dieser Grundrechte sicherzustellen, wie sie insbesondere durch den Gerichtshof der Europäischen Union (im Weiteren „Gerichtshof") zur Anwendung kommen.

- Der EDSB **nimmt zur Kenntnis**, dass der Rat am 6. Dezember 2018[3] einen allgemeinen Ansatz für den Vorschlag erzielt hat, sowie die Annahme des Entwurfs einer Stellungnahme durch den IMCO-Ausschuss am 13. Dezember 2018, des Entwurfs einer Stellungnahme durch den CULT-Ausschuss am 16. Januar 2019 und des Berichtentwurfs des LIBE-Ausschusses am 21. Januar 2019.[4]

- Diese förmliche Stellungnahme **konzentriert sich auf die mögliche Auswirkung des Vorschlags auf das Recht auf Privatsphäre und das Recht auf den Schutz personenbezogener Daten** unter Berücksichtigung von Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union (im Weiteren „die Charta") und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (im Weiteren „der AEUV"). **Insbesondere in Bezug auf diesen Vorschlag stellen wir** jedoch **fest, dass das Recht auf den Schutz personenbezogener Daten untrennbar mit anderen Grundrechten wie dem Recht auf Informations- und Meinungsfreiheit**[5] sowie den allgemeinen EU-

[3] Verfahren 2018/0331(COD), Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte – allgemeiner Ansatz.
[4] Die Stellungnahme und Berichte der Ausschüsse des Europäischen Parlaments zu dem Vorschlag (Dokumente im Zusammenhang mit Verfahren 2018/0331(COD)) sind unter folgender Adresse abrufbar: http://www.europarl.europa.eu/committees/de/draft-opinions.html?urefProcYear=2018&urefProcNum=0331&urefProcCode=COD&source=&linkedDocument=true&ufolderComCode=&ufolderLegId=&ufolderId=#documents
[5] Siehe Christopher Docksey, *Four fundamental rights: finding the balance*, International Data Privacy Law, 2016, Bd. 6, Nr. 3, Seite 203: „In manchen Zusammenhängen wie der Massenüberwachung und der unabhängigen Regulierung ergänzen sich das Recht auf Privatsphäre und auf den Schutz personenbezogener Daten und auf

Rechtsgrundsätzen wie dem Grundsatz der Nichtdiskriminierung **verbunden ist**. Die Berücksichtigung dieser Schnittstelle stimmt unter anderem mit Verordnung (EU) 2016/679 (im Weiteren „die DSGVO“) überein[6], die sich ausdrücklich auf „die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen“ bezieht.[7]

2. Allgemeine Bemerkungen

2.1. Das geltende Datenschutzgesetz

- Der EDSB nimmt positiv zur Kenntnis, dass in mehreren Bestimmungen des Vorschlags betont wird, dass der Schutz der betreffenden Grundrechte sichergestellt wird und dass Hostingdiensteanbieter die Grundrechte der Nutzer immer berücksichtigen sollten.[8] In dieser Hinsicht begrüßt der EDSB, dass in Erwägungsgrund 7 des Vorschlags ausdrücklich betont wird, dass „das Recht auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten“ durch die Verordnung sichergestellt wird. Aus Gründen der Klarheit empfiehlt der EDSB, dem obigen Erwägungsgrund den **ausdrücklichen Verweis auf das geltende Datenschutzgesetz**, und zwar die DSGVO und die Richtlinie (EU) 2016/680 (im Weiteren „die Strafverfolgungsrichtlinie“) hinzuzufügen.[9] Folgende Formulierung wäre möglich: „*Dieser Vorschlag hat keinen Einfluss auf die für die Verarbeitung personenbezogener Daten geltenden Regeln, insbesondere Verordnung (EU) 2016/679 und Richtlinie (EU) 2016/680*.“

2.2. Die Notwendigkeit einer klaren Definition der Pflichten, die den Hostingdiensteanbietern in dem Vorschlag auferlegt werden

- Da die gemäß dem Vorschlag zu ergreifenden Maßnahmen (die Ermittlung und Entfernung von terroristischen Inhalten) zu „Aufgaben im öffentlichen Interesse“ gehören, **müssen alle von Hostingdiensteanbietern gemäß dem Vorschlag zu ergreifenden Maßnahmen** vom Gesetzgeber **klar beschrieben werden,** und **wirksame Aufsicht muss durch klar kenntlich gemachte zuständige Behörden sichergestellt werden.** Dies würde dazu beitragen, die Bedenken über sogenannte „privatisierte“ (an Privatfirmen, in diesem Fall die Hostingdiensteanbieter, delegierte) Strafverfolgungsvollmachten anzugehen, und stünde im Einklang mit beiden

---

Meinungsfreiheit völlig und stärken sich gegenseitig.“ Hinsichtlich der Auswirkung der Maßnahme auf **mit dem Recht auf Privatsphäre und auf den Schutz personenbezogener Daten verbundene Grundrechte** vgl. unter anderem Rechtssache *Tele2* (EuGH, C-203/15 und C-698/15, ECLI:EU:C:2016:970): „(...) könnte die Vorratsspeicherung der Verkehrs- und Standortdaten jedoch Auswirkungen auf die Nutzung der elektronischen Kommunikationsmittel und infolgedessen auf die Ausübung der in Artikel 11 der Charta gewährleisteten Freiheit der Meinungsäußerung durch die Nutzer dieser Mittel haben (vgl. entsprechend in Bezug auf Richtlinie 2006/24 Urteil Digital Rights, Rn. 28)“.

[6] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1-88.

[7] Artikel 24 Absatz 1 der DSGVO.

[8] Vgl. insbesondere Erwägungsgründe 7 und 17 sowie Artikel 3 und 6 des Vorschlags.

[9] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4.5.2016, S. 89-131.

übergreifenden Grundsätzen „Rechtsqualität“[10] und „wirtschaftliche Sicherheit“ für Wirtschaftsbeteiligte (Klärung der gesetzlichen Pflichten von Hostingdiensteanbietern).

- Wie aus dieser förmlichen Stellungnahme weiter hervorgeht, weist der Vorschlag diesbezüglich einige Mängel auf. Beispielsweise enthält der Vorschlag keine Definition der von Hostingdiensteanbietern gemäß Artikel 7 aufzubewahrenden „**zugehörigen Daten**“, und in Erwägungsgrund 20 wird beispielsweise darauf eingegangen, dass solche Daten „beispielsweise ‚Teilnehmerdaten‘, insbesondere Daten, die sich auf die Identität des Inhalteanbieters beziehen, und ‚ Zugangsdaten‘ umfassen können, darunter das Datum und die Uhrzeit der Nutzung durch den Inhalteanbieter oder die Anmeldung bei und Abmeldung von dem Dienst, zusammen mit der IP-Adresse, die der Internetzugangsanbieter dem Inhalteanbieter zuweist“.

- Nach Ansicht des EDSB ist eine klare Definition von „zugehörigen Daten“ notwendig, um Ungewissheit für Hostingdiensteanbieter zu vermeiden und gleichzeitig auch Rechtssicherheit für alle Parteien zu gewährleisten. Er empfiehlt daher die klare Definition des Ausdrucks „zugehörige Daten“ unter Bereitstellung einer **erschöpfenden Liste** von Datenkategorien, die von den Hostingdiensteanbietern aufzubewahren sind.[11]

- Mit dem Ziel der Bereitstellung von mehr Rechtssicherheit für die Hostingdiensteanbieter schlägt der EDSB ferner vor, im Vorschlag **die Informationen im Einzelnen anzugeben und zu klären, die für die Gewährleistung der raschen Entfernung der terroristischen Inhalte durch den Hostingdiensteanbieter notwendig und verhältnismäßig** und von der „zuständigen Behörde“ (die anzugeben ist, wie in Abschnitt 3.2.2. dieser förmlichen Stellungnahme empfohlen) **in die Entfernungsanordnung aufzunehmen sind** (leicht lesbare, „standardisierte“ Informationen zur Lokalisierung der Inhalte wie die URL sowie andere Informationen, die zur prompten Ermittlung und Entfernung der terroristischen Inhalten dienen).

---

[10] In dem *Digital Rights Ireland*-Urteil (Verbundene Rechtssachen C-293/12 und C-594/12, ECLI:EU:C:2014:238) hat der Gerichtshof entschieden, dass der **Ermessensspielraum des Gesetzgebers** bei der Einschränkung von Grundrechten eingeschränkt ist: „da Grundrechtseingriffe in Rede stehen, kann der Gestaltungsspielraum des Unionsgesetzgebers anhand einer Reihe von Gesichtspunkten eingeschränkt sein; zu ihnen gehören u. a. der betroffene Bereich, das Wesen des fraglichen durch die Charta gewährleisteten Rechts, Art und Schwere des Eingriffs sowie dessen Zweck“ (Rn. 47). Die Frage „Welches Ausmaß hat der (eingeschränkte) Gestaltungsspielraum des Unionsgesetzgebers?“ beantwortete der Gerichtshof in der Sache wie folgt: „Daher **muss** die fragliche Unionsregelung **klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen** und Mindestanforderungen aufstellen, sodass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen.“ (Rn. 54).
Zu dem Konzept „gesetzlich vorgesehen“ vgl. auch das Gutachten des Generalanwalts des Gerichtshofs, 8. September 2015, Gutachten 1/15 über den Entwurf eines Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen, Rn. 193: „Nach der Rechtsprechung des EGMR verlangt dieser Ausdruck [„Rechtsqualität“] im Wesentlichen, dass die in Rede stehende Maßnahme **zugänglich** und **hinreichend vorhersehbar** ist, also mit anderen Worten klar genug formuliert ist, um jeden hinreichend erkennen zu lassen, unter welchen Umständen und unter welchen Voraussetzungen sie den Hoheitsträger ermächtigt, Maßnahmen zu ergreifen, die seine von der EMRK geschützten Rechte beeinträchtigen.“ (Hervorhebung hinzugefügt).
In diesem Zusammenhang vgl. das jüngere Urteil des EGMR, *Catt gegen United Kingdom*, 24. Januar 2019.

[11] Da die Pflichten der Hostingdiensteanbieter unklar sind, besteht das Risiko, dass für sie durch die Androhung von in der Verordnung festgelegten Sanktionen – vgl. Artikel 18 Absatz 1 Buchstabe e unter Bezug auf Artikel 7 – der „Anreiz“ geboten ist, **übermäßige Datenmengen** zu erheben, was schädlich für den Schutz personenbezogener Daten (sowie für andere Grundrechte wie freie Meinungsäußerung) wäre.

3. Besondere Bemerkungen

3.1. Definitionen der Begriffe terroristische Inhalte“ und „Verbreitung von terroristischen Inhalten“ und „Hostingdiensteanbieter“

- Der in Artikel 2 Absatz 1 Punkt 5 definierte Ausdruck „**terroristische Inhalte**“ umfasst eines oder mehrere der Folgenden: (a) „der Aufruf zu oder die Befürwortung von terroristischen Straftaten, auch durch ihre Verherrlichung, mit der damit einhergehenden Gefahr, dass solche Taten begangen werden könnten“; (b) „die Ermutigung, an terroristischen Straftaten mitzuwirken“; (c) „die Förderung der Aktivitäten einer terroristischen Vereinigung, insbesondere durch Ermutigung zur Beteiligung an oder Unterstützung einer terroristischen Vereinigung im Sinne des Artikels 2 Absatz 3 der Richtlinie (EU) 2017/541[12]“. In Artikel 2 Absatz 4 heißt es in dem Vorschlag, dass „terroristische Straftaten“ Straftaten im Sinne des Artikels 3 Absatz 1 der Richtlinie (EU) 2017/541 bedeuten. In Artikel 21 der genannten Richtlinie heißt es, dass „Mitgliedstaaten die erforderlichen Maßnahmen treffen, um sicherzustellen, dass Online-Inhalte, die eine öffentliche Aufforderung zur Begehung einer terroristischen Straftat im Sinne des Artikels 5 darstellen [...], unverzüglich entfernt werden.[13]“
  Zur Vermeidung von Widersprüchen zwischen dem Vorschlag und der oben genannten Richtlinie empfiehlt der EDSB, dass die Definition von durch die Hostingdiensteanbieter zu ermittelnden und zu entfernenden „terroristischen Inhalten“ in den beiden Rechtstexten **konsistent und eng angeglichen** ist.

- Der EDSB begrüßt, dass in Erwägungsgrund 9 insbesondere festgelegt wird, dass zuständige Behörden und Hostingdiensteanbieter den Zusammenhang, in dem derartige Inhalte erscheinen, berücksichtigen sollten und dass Inhalte, die für Bildungs-, Presse- oder Forschungszwecke verbreitet werden, angemessen geschützt werden sollten. Im obigen Erwägungsgrund wird auch verdeutlicht, dass die Formulierung radikaler, polemischer oder kontroverser Ansichten zu sensiblen politischen Fragen in der öffentlichen Debatte nicht als terroristischer Inhalt betrachtet werden sollten. Diese im Vorschlag in erster Linie als Absicherungen der Meinungsfreiheit vorgesehenen Spezifizierungen sind **auch aus Sicht des Schutzes der Privatsphäre und personenbezogener Daten relevant**, da durch sie Kategorien von Inhalten (und „zugehörigen Daten“) „herausgearbeitet werden“, die nicht zum Gegenstand von Ermittlung, Entfernung und letztendlich Aufbewahrung/Vorratsdatenspeicherung durch die Hostingdiensteanbieter gemacht würden.

- Der Ausdruck „**Verbreitung terroristischer Inhalte**“ gemäß Artikel 2 Absatz 1 Punkt 6 sollte auch auf Artikel 5 der Richtlinie 2017/541 abgestimmt werden. Im Gegensatz zu der derzeitigen Formulierung des Vorschlags (wo die unklare Formulierung „Dritte“ verwendet wird) bezieht sich Letzterer auf das „*öffentliche Zugänglichmachen*“ terroristischer Inhalte. Diese Formulierung würde dem Zweck des Vorschlags, der die Verhinderung der Verbreitung terroristischer Online-Inhalte zum Ziel hat, besser entsprechen. Dasselbe sollte für Artikel 2 Absatz 1 Punkt 1 bei der Definition von „**Hostingdiensteanbieter**“ gelten (Ersatz des Ausdrucks „Dritte“ durch

[12] Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. L 88 vom 31.3.2017, S. 6-21.
[13] Artikel 5 der Richtlinie 2017/541, Öffentliche Aufforderung zur Begehung einer terroristischen Straftat.

„die Öffentlichkeit“). Als Folge dieser Spezifizierung würden beispielsweise **Cloud-Dienste**, die keine Nutzerinhalte für die Verbreitung zugänglich machen, jedoch für Dritte zugänglich sind, in Übereinstimmung mit den Zielsetzungen des Vorschlags nicht in seinem Geltungsbereich liegen.

3.2. Entfernungsanordnungen

3.2.1. Entfernungsentscheidungen sind innerhalb einer Stunde nach dem Eingang der Anordnung durchzuführen

- Gemäß Artikel 4 Absatz 2 müssen Hostingdiensteanbieter **terroristische Inhalte innerhalb einer Stunde nach Eingang der Entfernungsanordnung** von der zuständige Behörde **entfernen**. In dieser Hinsicht merken wir an, dass terroristische Inhalte gemäß der Folgenabschätzung aufgrund der Geschwindigkeit ihrer Online-Verbreitung in den ersten Stunden nach ihrem „öffentlichen Zugänglichmachen“ besonders schädlich sind. Der EDSB berücksichtigt diese Erwägung im Zusammenhang mit der Effektivität der Maßnahme (bedeutend weniger effektiv nach einer Stunde). Wir weisen jedoch darauf hin, dass beachtet werden muss, dass die Durchführung einer solchen raschen Entfernung – insbesondere im Falle von kleinen und mittleren Hostingdiensteanbietern – eine Herausforderung darstellen[14] und Hostingdiensteanbietern die Möglichkeit nehmen könnte, die Entfernungsanordnung einer aussagekräftigen Prüfung zu unterziehen.

3.2.2. Authentifizierung der Entfernungsanordnungen

- Wesentliche Voraussetzungen dafür, dass Hostingdiensteanbieter die in Abschnitt 3.2.1 dieser förmlichen Stellungnahme erwähnte rasche Entfernung durchführen können, sind außerdem eine **reibungslose Zusammenarbeit und ein rasches Zusammenwirken von Hostingdiensteanbietern und den zuständigen Behörden.** Im Zusammenhang mit der „operativen“ Implementierung des Vorschlags schlägt der EDSB somit die Anwendung von **digitalen Signaturen für elektronisch übermittelte Entfernungsanordnungen** vor sowie die Aufstellung einer **offiziellen und leicht zugänglichen Liste zuständiger Behörden, die für das Ausstellen der Entfernungsanordnungen für jeden Mitgliedstaat verantwortlich sind**. Dadurch wären Hostingdiensteanbieter in der Lage, **die Authentizität** einer Entfernungsanordnung rasch **zu verifizieren** und in Zweifelsfällen im Zusammenhang mit der Anordnung die zuständigen Behörden zu kontaktieren (ausstellende Behörde, Inhalt, Modalitäten für ihre Ausführung usw.). Diese Spezifizierungen könnten zu Erwägungsgrund 14 hinzugefügt werden.

3.3. Proaktive Maßnahmen

3.3.1. Von Hostingdiensteanbietern zu ergreifende Maßnahmen, um die Verbreitung terroristischer Online-Inhalte in Übereinstimmung mit einem gezielten „risikobasierten Ansatz“ und unter Erfüllung der Rechenschaftspflicht zu verhindern

[14] In dieser Hinsicht geht aus der Folgenabschätzung, die dem Vorschlag beiliegt, SWD(2018)408 final, 12.9.2018, Seite 8, hervor, dass terroristische Inhalte in der ersten Stunde besonders schädlich sind. Es wird jedoch kein Nachweis dahingehend vorgelegt, dass eine derartig kurze Frist tatsächlich praktikabel ist. Auf Seite 86 heißt es nämlich im Gegensatz dazu, dass nach Angaben von Hostingdiensteanbietern eine derartig kurze Frist für kleinere Unternehmen undurchführbar erscheint.

- Gemäß Artikel 3 (Sorgfaltspflichten) „ergreifen“ Hostingdiensteanbieter „geeignete, angemessene und verhältnismäßige Maßnahmen“, um die Verbreitung terroristischer Inhalte zu verhindern, und sie „handeln dabei mit der gebotenen Sorgfalt, verhältnismäßig und ohne Diskriminierung sowie unter gebührender Berücksichtigung der Grundrechte der Nutzer“. In Artikel 6 wird als eine der Reihe von Maßnahmen, die von Hostingdiensteanbietern zur Erfüllung der in der Einleitungsbestimmung in Artikel 3 niedergelegten „Sorgfaltspflichten“ zu ergreifen sind (zusammen mit Maßnahmen im Zusammenhang mit Entfernungsanordnungen und Meldungen), festgelegt, dass Hostingdiensteanbieter „gegebenenfalls **proaktive Maßnahmen** ergreifen müssen, um ihre Dienste vor der Verbreitung terroristischer Inhalte zu schützen.“[15] Der EDSB hebt hervor, dass in Artikel 6 Absatz 1 auch das „Risiko und Ausmaß der möglichen Beeinflussung des Hostingdiensteanbieters durch terroristische Inhalte“ („risikobasierter Ansatz“) erwähnt werden, und empfiehlt die Straffung dieses Ansatzes im gesamten Vorschlag.

- In dieser Beziehung weist der EDSB auf den zu beachtenden übergreifenden Grundsatz hin, dass alle die Grundrechte und Grundfreiheiten einschränkenden Maßnahmen notwendig und verhältnismäßig sein sollten[16], d. h. dass sie **so gezielt wie möglich** sein sollten.

- In Übereinstimmung mit diesem Grundsatz empfiehlt der EDSB, dass folgende Verpflichtung für Hostingdiensteanbieter in den Vorschlag mit aufgenommen wird, und zwar *vor* dem Ergreifen einer proaktiven Maßnahme:

  (i) Durchführung und Veröffentlichung **einer Risikoabschätzung des Grades, zu dem sie** terroristischen Inhalten **ausgesetzt sind** (auch auf Grundlage der Anzahl von eingegangenen Entfernungsanordnungen und Meldungen);
  (ii) Erstellung eines **Rechtsbehelfsaktionsplans** zur Bekämpfung von terroristischen Inhalten im Verhältnis zu dem ermittelten Risikograd.[17] Die oben erwähnte Abschätzung und der genannte Aktionsplan würden auch nützliche Werkzeuge zur Erfüllung der **Rechenschaftspflicht** für eine regelmäßige Überprüfung der Maßnahmen darstellen.

  Als weiteres Werkzeug im Dienste der Rechenschaftspflicht sollten Hostingdiensteanbieter **in regelmäßigen Abständen** über die ergriffenen Maßnahmen und den verbleibenden Bedrohungsgrad (Exposition gegenüber terroristischen Inhalten) **Bericht erstatten**.

[15] Gemäß Erwägungsgrund 18 heißt es weiter, dass es sich bei den proaktiven Maßnahmen um Maßnahmen handeln könnte, mit denen das erneute Hochladen terroristischer Inhalte, die zuvor entfernt wurden, verhindert werden soll, wobei öffentliche oder in Privatbesitz befindliche Werkzeuge mit bekanntem terroristischen Inhalt zu prüfen sind, sowie um den Einsatz zuverlässiger technischer Hilfsmittel, um neue terroristische Inhalte zu erkennen.

[16] In Artikel 52 Absatz 1 der Charta heißt es wie folgt: „Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Vorbehaltlich des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der EU anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen“.

[17] In der Folgenabschätzung werden „Risikoabschätzung“ und „Rechtsbehelfsaktionsplan“ im Zusammenhang mit der Implementierung von Maßnahmen unter Artikel 6 gemäß einem risikobasierten Ansatz erwähnt. Derartige Anforderungen sind jedoch noch nicht endgültig in den Vorschlag aufgenommen worden.

3.3.2. Verwendung von automatisierten Werkzeugen im Zusammenhang mit proaktiven Maßnahmen und Schutzvorkehrungen für den Einsatz derartiger Maßnahmen

- In den Erwägungsgründen 16 und 18 und in Artikel 6 Absatz 2 ist spezifisch vorgesehen, dass proaktive Maßnahmen **die Verwendung automatisierter Werkzeuge** einschließen können. Der EDSB betont, dass derartige automatisierte Werkzeuge nur in **umsichtiger und gezielter** Weise auf der Basis des Ergebnisses der in Absatz 3.3.1 dieser formellen Stellungnahme erwähnten Risikoabschätzung verwendet werden sollten.

- Der EDSB betont, dass die in dem Vorschlag vorgesehenen Verfahren in einigen, wenn nicht allen Fällen, zu der **Ermittlung des Nutzers** führen, der die terroristischen Inhalte hochgeladen hat (es ist der Fall der Aufbewahrung von Daten, die mit entfernten Inhalten zusammenhängen und die gemäß Artikel 7 von Hostingdiensteanbietern zu speichern sind und auf die möglicherweise von Strafverfolgungsbehörden zugegriffen wird; eines Beschwerdemechanismus, der von dem Nutzer gemäß Artikel 10 genutzt wird; der Bereitstellung von Informationen an den Nutzer über die Entfernung durch den Hostingdiensteanbieter).

- In dieser Beziehung weist der EDSB auch darauf hin, dass nicht ausgeschlossen werden kann, dass die **proaktiven Maßnahmen der Hostingdiensteanbieter, einschließlich automatisierter Werkzeuge, für Erkennung und Entfernung von durch Nutzer hochgeladener Inhalte**, auch als „automatisierte Entscheidungsfindung und Profiling[18]“ im Sinne von Artikel 22 der DSGVO gelten können.

- Der EDSB erinnert daran, dass gemäß Artikel 22 Absatz 1 der DSGVO eine **vollständig automatisierte Entscheidung im Einzelfall**, die rechtliche Wirkung entfaltet oder betroffene Person in ähnlicher Weise erheblich beeinträchtigt, **generell verboten** ist.[19] In Artikel 22 Absatz 2 der DSGVO sind jedoch Ausnahmen für dieses allgemeine Verbot vorgesehen, und es werden spezielle Fälle und Anforderungen dargelegt, bei denen eine solche Entscheidungsfindung zulässig ist. Insbesondere wird in Artikel 22

[18] In Artikel 4 Absatz 4 DSGVO wird Profiling wie folgt definiert: „Jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.“
In Erwägungsgrund 30 der DSGVO heißt es wie folgt: „Natürlichen Personen werden unter Umständen **Online-Kennungen** wie **IP-Adressen** und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.“ (Hervorhebung hinzugefügt)

[19] Da das von dem Vorschlag vorgesehene automatisierte Werkzeug nicht nur zur Entfernung und Vorratsdatenspeicherung von Inhalten (und zugehörigen Daten) im Zusammenhang mit dem Hochlader führen könnte, sondern letztendlich auch zu strafrechtlichen Untersuchungen dieses Hochladers, würden diese Werkzeuge **bedeutende Auswirkungen** auf diese Person haben, sich erheblich nachteilig auf ihre Meinungsfreiheit auswirken und bedeutsame Risiken für ihre Rechte und Freiheiten darstellen.
Die Bestimmungen von Artikel 22 der DSGVO sind Gegenstand der Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling der Artikel-29-Datenschutzgruppe (jetzt EDSA), die auf folgender Internetseite zugänglich sind: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, dort heißt es auf Seite 23 wie folgt: „Auch wenn eine Entscheidungsfindung sich nicht auf die Rechte einer Person auswirkt, kann sie dennoch in den Anwendungsbereich von Artikel 22 fallen, wenn sie eine entsprechende Wirkung entfaltet oder die Person in ähnlicher Weise erheblich beeinträchtigt.“

Absatz 2 Buchstabe b der DSGVO festgelegt, dass die Entscheidung aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten zulässig ist, wenn diese Rechtsvorschriften „**angemessene Maßnahmen**“ zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten. Diesbezüglich wird in Erwägungsgrund 71 der DSGVO betont, dass zu derartigen „angemessenen Garantien“ in jedem Fall die spezifische Unterrichtung der betroffenen Person und der Anspruch auf direktes Eingreifen einer Person, auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung gehören sollten.

- Gemäß Artikel 8 Absatz 1 unter den „Transparenzanforderungen“ müssen Hostingdiensteanbieter in ihren Nutzungsbedingungen ihre Strategie zur Verhinderung der Verbreitung terroristischer Inhalte darlegen, **gegebenenfalls** mit einer **aussagekräftigen Erläuterung** der Funktionsweise proaktiver Maßnahmen, einschließlich der Verwendung automatisierter Werkzeuge“ (Hervorhebung hinzugefügt).

- Gemäß Artikel 9 Absatz 1 wird außerdem festgelegt, dass Hostingdiensteanbieter, die automatisierte Werkzeuge verwenden, wirksame und geeignete Schutzvorkehrungen treffen, um sicherzustellen, dass insbesondere Entscheidungen zur Entfernung oder Sperrung von Inhalten zutreffend und fundiert sind. Gemäß Artikel 9 Absatz 2 bestehen diese Schutzvorkehrungen, „**soweit angemessen, in einer Aufsicht und Überprüfung durch Menschen**, aber in jedem Fall immer dann, wenn eine eingehende Beurteilung des betreffenden Kontexts erforderlich ist, [...]“ (Hervorhebung hinzugefügt).

- Hinsichtlich dieser Schutzvorkehrungen empfiehlt der EDSB, in Artikel 8 Absatz 1 und Artikel 9 Absatz 2 die Formulierung „soweit angemessen“ durch „**auf jeden Fall**“ zu ersetzen oder alternativ die Formulierung „soweit angemessen“ zu streichen.[20]

- Der EDSB merkt des Weiteren an, dass gemäß Artikel 6 Absatz 2 Hostingdiensteanbieter der für die Überwachung der Durchführung der proaktiven Maßnahmen gemäß Artikel 17 Absatz 1 Buchstabe c **zuständigen Behörde einen Bericht über die ergriffenen proaktiven Maßnahmen, einschließlich der Verwendung automatisierter Werkzeuge**, vorlegen sollten.

  Der EDSB empfiehlt, in Erwägungsgrund 18 des Vorschlags festzulegen, dass Hostingdiensteanbieter den zuständigen Behörden alle notwendigen Informationen über die verwendeten automatisierten Werkzeuge vorlegen sollten, um eine gründliche öffentliche Aufsicht über die **Wirksamkeit** der Werkzeuge zu gestatten und um sicherzustellen, dass **diese nicht zu diskriminierenden, ungezielten, unspezifischen oder ungerechtfertigten Ergebnissen führen**.[21]

---

[20] Von einem „technischen“ Standpunkt aus gesehen, wird hinsichtlich der **Möglichkeiten und Grenzen automatisierter Erkennung von Inhalten**, wobei jedoch die spezifischen Einzelheiten der in Rede stehenden illegalen Inhalte und der Entwicklung von Technologien (der sogenannte „Stand der Technik“) berücksichtigt werden sollten, auf Folgendes verwiesen: *Mixed messages? The limits of automated media content analysis*, November 2017, CDT, auf Seite 21: „jede Verwendung automatisierter Inhaltsanalyse-Werkzeuge sollte mit einer Überprüfung der Ausgabe/Schlussfolgerungen des Werkzeugs durch Menschen erfolgen.“
verfügbar unter: https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf
Ein weiterer wesentlicher Punkt, der in diesem Papier hervorgehoben wird, ist die Notwendigkeit, **die Art der** zu ermittelnden **Inhalte klar, konsequent und präzise zu definieren**.

[21] Siehe die *Declaration on Ethics and Data Protection in Artificial Intelligence*, angenommen auf der 40. Internationalen Konferenz der Datenschutzbeauftragten, 23. Oktober 2018, verfügbar unter:

4. Obligatorische Aufbewahrung von Inhalten und zugehörigen Daten durch die Hostingdiensteanbieter

- Gemäß Artikel 7 müssen Hostingdiensteanbieter **terroristische Inhalte** (die infolge einer von drei möglichen Maßnahmen gemäß dem Vorschlag, d. h. Ausführung von Entfernungsanordnungen, Meldungen oder proaktiv, entfernt oder gesperrt wurden) sowie **zugehörige Daten**[22] zum Zwecke nachfolgender Verfahren der behördlichen oder gerichtlichen Überprüfung (als Schutzvorkehrung bei irrtümlicher Entfernung) sowie zum Zwecke der Prävention, Erkennung, Ermittlung und der Strafverfolgung bei terroristischen Straftaten **aufbewahren**.[23]

- Die Tatsache, dass die Hostingdiensteanbieter zu einer derartigen Vorratsdatenspeicherung verpflichtet werden, hat zur Folge, so merkt der EDSB an, dass private Rechtsträger zur Vorratsspeicherung von Daten (einschließlich personenbezogener Daten über Hochlader und in Bezug auf Straftaten, „terroristische Straftatbestände" mit strafrechtlicher Natur) zu Zwecken der Strafverfolgung für einen Zeitraum von sechs Monaten verpflichtet sind.[24] So sieht Artikel 10 DSGVO vor, worauf der EDSB hinweist, dass die Verarbeitung personenbezogener Daten über Straftaten nur unter behördlicher Aufsicht vorgenommen werden darf *oder* wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das **geeignete Garantien** für die persönlichen Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist.

---

https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.p

Siehe insbesondere Punkt 3 Buchstabe c: „Die Transparenz und Verständlichkeit von Künstliche-Intelligenz-Systemen sollten zum Zwecke einer effektiven Implementierung insbesondere dadurch verbessert werden, dass **die Praktiken von Organisationen transparenter gestaltet werden, insbesondere indem die Transparenz der Algorithmen und die Rechenschaftspflicht gefördert werden, während die Aussagekraft der bereitgestellten Informationen gewährleistet wird."**

Mit anderen Worten sind wir der Ansicht, dass die **Rechenschaftspflicht der Hostingdiensteanbieter** verstärkt werden sollte. Dies erfordert einen hohen Grad an **Transparenz** der Art und Weise, wie das mögliche „Herunternehmen" von hochgeladenen Inhalten erfolgt (klare Richtlinien für die Umstände, unter denen Inhalte gesperrt, entfernt oder eingeschränkt werden). Auf jeden Fall erscheint es sinnvoll, dass Herunternahmeentscheidungen einer **Überprüfung durch Menschen unterliegen** sollten und dass Hostingdiensteanbieter für **aussagekräftige Erläuterungen und Berichterstattung** über das Funktionieren und die Wirksamkeit der geplanten Maßnahmen sorgen sollten. Dadurch könnte auch **überprüft und sichergestellt** werden, dass durch etwaige vom Hostingdiensteanbieter ergriffene Maßnahmen a) der Grundsatz der Zweckbindung streng eingehalten wird (keine Verwendung für andere „Ziele") und b) keine diskriminierenden, unspezifischen oder ungerechtfertigten Ergebnisse erhalten werden (ebenfalls unter Berücksichtigung der „Verteilung" von falsch positiven Ergebnissen und nicht nur ihrer Menge).

[22] Hinsichtlich der Notwendigkeit einer Definition von „zugehörigen Daten" siehe Anmerkungen in Abschnitt 2.2. dieser förmlichen Stellungnahme.

[23] Siehe Erwägungsgrund 21.

[24] Insbesondere heißt es in Erwägungsgrund 22: „Um die Verhältnismäßigkeit zu gewährleisten, sollte der Aufbewahrungszeitraum auf sechs Monate begrenzt werden, damit die Inhalteanbieter ausreichend Zeit haben, das Überprüfungsverfahren einzuleiten, **und damit die Strafverfolgungsbehörden auf die für die Ermittlung und Verfolgung terroristischer Straftaten relevanten Daten zugreifen können**. **Dieser Zeitraum kann** jedoch **auf Antrag der Behörde, die die Überprüfung durchführt, nach Bedarf verlängert werden, falls das Überprüfungsverfahren innerhalb des sechsmonatigen Zeitraums zwar eingeleitet, aber nicht abgeschlossen wurde. Diese Dauer sollte so bemessen sein, dass die Strafverfolgungsbehörden die** für die Ermittlungen **erforderlichen Beweismittel** unter Wahrung des Gleichgewichts mit den betreffenden Grundrechten sichern können" (Hervorhebung hinzugefügt).

- Da die betreffende Verarbeitung (Aufbewahrung von terroristischen Inhalten und damit zusammenhängenden Daten) jedoch *nicht* unter der Kontrolle einer Behörde erfolgen würde, ist die Sicherstellung eines angemessenen Niveaus von Schutzvorkehrungen von ausschlaggebender Bedeutung. Der EDSB stellt fest, dass in Artikel 7 Absatz 3 festgelegt ist, dass HSP „dafür sorgen [müssen], dass die terroristischen Inhalte und die damit verbundenen Daten angemessenen technischen und organisatorischen Sicherheitsvorkehrungen unterliegen", und diese „technischen und organisatorischen Schutzmaßnahmen tragen dafür Sorge, dass der Zugang zu den terroristischen Inhalten und den damit zusammenhängenden Daten nur für die Zwecke [...] gewährleistet ist und ein hohes Maß an Sicherheit für die betreffenden personenbezogenen Daten gewährleistet wird".

- Der EDSB weist darauf hin, dass in Artikel 7 der aufgehobenen Richtlinie 2006/24 (im Weiteren "die Richtlinie über die Vorratsspeicherung von Daten")[25] Folgendes mit einer ähnlichen Formulierung wie im Vorschlag festgelegt war: „in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen" und „in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist". Der Gerichtshof kam jedoch in *Digital Rights Ireland* zu dem Schluss, dass in der Richtlinie über die Vorratsspeicherung von Daten *keine* hinreichenden Schutzvorkehrungen getroffen waren, um einen wirksamen Schutz der vorratsgespeicherten Daten vor dem Risiko des Missbrauchs, des unrechtmäßigen Zugriffs und der nachfolgenden Benutzung der Daten sicherzustellen.[26]

- Nach dem Dafürhalten des EDSB kann argumentiert werden, dass in dem Vorschlag, ähnlich wie in der Richtlinie über die Vorratsspeicherung von Daten, *keine* sachlichen und verfahrenstechnischen Bedingungen über **den Zugang** der „zuständigen Behörden" **zu den aufbewahrten Daten und deren spätere Nutzung** festgelegt werden, wie dies vom Gerichtshof in *Digital Rights Ireland* gefordert wird.[27] Das bloße Erwähnen in

[25] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13.4.2006, S. 54-63.

[26] Verbundene Rechtssachen C-293/12 und C-594/1, *Digital Rights Ireland*, siehe insbesondere bei Rn. 54-55 und 65-67. Es wird besonders auf Randnummer 55 hingewiesen: „Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten, wie in der Richtlinie 2006/24 vorgesehen, **automatisch verarbeitet** werden und eine erhebliche Gefahr des unberechtigten Zugangs zu diesen Daten besteht", sowie auf Randnummer 67: „Artikel 7 der Richtlinie 2006/24 (...) gewährleistet nicht, dass die genannten Anbieter oder Betreiber durch technische und organisatorische Maßnahmen für ein besonders hohes Schutz- und Sicherheitsniveau sorgen, sondern gestattet es ihnen u. a., bei der Bestimmung des von ihnen angewandten Sicherheitsniveaus wirtschaftliche Erwägungen hinsichtlich der Kosten für die Durchführung der Sicherheitsmaßnahmen zu berücksichtigen. Vor allem gewährleistet die Richtlinie 2006/24 nicht, dass die Daten nach Ablauf ihrer Speicherungsfrist unwiderruflich vernichtet werden." (Hervorhebung hinzugefügt).

[27] Siehe *Digital Rights Ireland*, Rn. 61-62, "(...) Richtlinie 2006/24 enthält keine sachlichen und verfahrensbezogenen Bedingungen über den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung. In Artikel 4 der Richtlinie, in dem der Zugang dieser Behörden zu den auf Vorrat gespeicherten Daten geregelt wird, wird nicht ausdrücklich festgelegt, dass dieser Zugang und die spätere Nutzung der betreffenden Daten streng auf den Zweck der Verhinderung und der Feststellung von präzise definierten schwerwiegenden Straftatbeständen oder des Ergreifens von Strafverfolgungsmaßnahmen im Zusammenhang damit beschränkt werden müssen; es **wird dort lediglich festgelegt, dass jeder Mitgliedstaat die durchzuführenden Verfahren und die zu erfüllenden Bedingungen definieren muss**, um gemäß den Notwendigkeits- und Verhältnismäßigkeitsanforderungen Zugang zu den auf Vorrat gespeicherten Daten zu

Erwägungsgrund 23, dass der Vorschlag „die Verfahrensgarantien und die verfahrensbezogenen Ermittlungsmaßnahmen im Zusammenhang mit dem Zugang zu Inhalten und damit zusammenhängenden Daten, die für die Zwecke der Ermittlung und Verfolgung terroristischer Straftaten im Einklang mit den nationalen Rechtsvorschriften der Mitgliedstaaten und den Rechtsvorschriften der Union aufbewahrt werden, nicht berührt“[28], kann **für die Bereitstellung der erforderlichen sachlichen und verfahrensbezogenen Bedingungen für den Zugang zu den** von den Hostingdiensteanbietern gemäß der im Vorschlag festgelegten Datenvorratsspeicherung zwingend auf Vorrat zu speichernden Daten und deren Nutzung **nicht als angemessen** gelten.

- Ferner ist der EDSB nicht davon überzeugt, dass die Vorratsdatenspeicherungsverpflichtung der Hostingdiensteanbieter zum Zwecke der Erkennung, Ermittlung und Strafverfolgung bei terroristischen Straftaten **notwendig und verhältnismäßig** ist, da Hostingdiensteanbieter gemäß Artikel 13 Absatz 4 bereits verpflichtet sind, die zuständigen Strafverfolgungsbehörden unverzüglich über etwaige Beweise terroristischer Straftaten, von denen sie Kenntnis erlangen, zu unterrichten. Darüber hinaus heißt es in Artikel 13 Absatz 4 des Vorschlags, dass die Hostingdiensteanbieter im Zweifelsfall diese Informationen an Europol zur geeigneten Bearbeitung übermitteln können.

- Im Lichte des Obigen empfiehlt der EDSB, die **vorgeschlagene Vorratsdatenspeicherungsverpflichtung** der Hostingdiensteanbieter für terroristische Inhalte und damit zusammenhängende Daten gemäß Artikel 7 Absatz 1 Buchstabe b **zu überdenken**.

5. Der Beschwerdemechanismus

- Gemäß Artikel 10 müssen Hostingdiensteanbieter wirksame und zugängliche Mechanismen einrichten, die Inhalteanbietern, deren Inhalte entfernt oder gesperrt wurden, die Möglichkeit geben, Beschwerde gegen die Maßnahme des Hostingdiensteanbieters einzulegen. Gemäß Artikel 10 Absatz 2 prüft der Hostingdiensteanbieter umgehend die Beschwerde und setzt den Inhalteanbieter über das Ergebnis der Prüfung in Kenntnis.

- Der EDSB begrüßt die Einrichtung eines **Beschwerdemechanismus**, da dieser zu der Verstärkung der Schutzvorkehrungen für die Hochlader vor irrtümlichen Entfernungen beitragen kann. Der EDSB empfiehlt jedoch, in Artikel 10 Buchstabe a eine **Frist für die Entscheidung des Hostingdiensteanbieters** über die Beschwerde sowie die Angabe, dass der vom Hostingdiensteanbieter einzurichtende Beschwerdemechanismus **die geltenden Gesetze und Verfahren** der Mitgliedstaaten (einschließlich der

---

erlangen. (62) Insbesondere wird in der Richtlinie 2006/24 kein objektives Kriterium festgelegt, nach dem die Anzahl der Personen, die zum Zugang zu den auf Vorrat gespeicherten Daten und zu deren späteren Nutzung ermächtigt sind, darauf begrenzt wird, was im Lichte des verfolgten Ziels unbedingt notwendig ist. Vor allem unterliegt der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll und im Anschluss an einen mit Gründen versehenen Antrag der genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten eingreift. Eine spezifische Verpflichtung der Mitgliedstaaten zur Festlegung solcher Beschränkungen wird dort auch nicht angegeben. (Hervorhebung hinzugefügt)

[28] Siehe ähnliche Formulierung in Artikel 4 *Zugang zu Daten* der Richtlinie 2006/24.

Nichtbeeinflussung der unter dem geltenden Datenschutzgesetz zur Verfügung stehenden Rechtsbehelfe) **nicht beeinflusst**, einzufügen.

Brüssel, den 12. Februar 2019

Giovanni BUTTARELLI