Europäisches Parlament
2014-2019

ANGENOMMENE TEXTE

P8_TA(2019)0421

Verhinderung der Verbreitung terroristischer Online-Inhalte ***I

Legislative Entschließung des Europäischen Parlaments vom 17. April 2019 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

Das Europäische Parlament,

– unter Hinweis auf den Vorschlag der Kommission an das Europäische Parlament und den Rat (COM(2018)0640),

– gestützt auf Artikel 294 Absatz 2 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage ihm der Vorschlag der Kommission unterbreitet wurde (C8-0405/2018),

– gestützt auf Artikel 294 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union,

– unter Hinweis auf die vom tschechischen Abgeordnetenhaus im Rahmen des Protokolls Nr. 2 über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit vorgelegte begründete Stellungnahme, in der geltend gemacht wird, dass der Entwurf eines Gesetzgebungsakts nicht mit dem Subsidiaritätsprinzip vereinbar ist,

– unter Hinweis auf die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 12. Dezember 2018[1],

– gestützt auf Artikel 59 seiner Geschäftsordnung,

– unter Hinweis auf den Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres sowie die Stellungnahmen des Ausschusses für Kultur und Bildung und des Ausschusses für Binnenmarkt und Verbraucherschutz (A8-0193/2019),

1. legt den folgenden Standpunkt in erster Lesung fest;

[1] ABl. C 110 vom 22.3.2019, S. 67.

2. fordert die Kommission auf, es erneut zu befassen, falls sie ihren Vorschlag ersetzt, entscheidend ändert oder beabsichtigt, ihn entscheidend zu ändern;

3. beauftragt seinen Präsidenten, den Standpunkt des Parlaments dem Rat und der Kommission sowie den nationalen Parlamenten zu übermitteln.

P8_TC1-COD(2018)0331

Standpunkt des Europäischen Parlaments festgelegt in erster Lesung am 17. April 2019 im Hinblick auf den Erlass der Verordnung (EU) 2019/... des Europäischen Parlaments und des Rates zur ~~Verhinderung~~ *Bekämpfung* der Verbreitung terroristischer Online-Inhalte [Abänd. 1]

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION -

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[1],

gemäß dem ordentlichen Gesetzgebungsverfahren,[2]

---

1 ABl. C 110 vom 22.3.2019, S. 67.

2 Standpunkt des Europäischen Parlaments vom 17. April 2019.

in Erwägung nachstehender Gründe:

(1) Diese Verordnung soll das reibungslose Funktionieren des digitalen Binnenmarkts in einer offenen und demokratischen Gesellschaft gewährleisten, indem der Missbrauch von Hostingdiensten für terroristische Zwecke ~~verhindert~~ ***bekämpft und ein Beitrag zur öffentlichen Sicherheit in den europäischen Gesellschaften geleistet*** wird. Das Funktionieren des digitalen Binnenmarkts sollte verbessert werden, indem die Rechtssicherheit für die Hostingdiensteanbieter erhöht, das Vertrauen der Nutzer in das Online-Umfeld gestärkt und die Schutzvorkehrungen für ~~die~~ ***das Recht auf*** freie Meinungsäußerung ~~und die Informationsfreiheit erhöht~~***, für die Freiheit, Informationen und Ideen in einer offenen und demokratischen Gesellschaft zu erhalten und weiterzugeben, sowie*** **für** ***die Freiheit und den Pluralismus der Medien ausgebaut*** werden. **[Abänd. 2]**

(1a) Die Regulierung von Anbietern von Hosting-Diensten kann die Strategien der Mitgliedstaaten zur Bekämpfung des Terrorismus nur ergänzen, bei denen der Schwerpunkt auf Offline-Maßnahmen wie Investitionen in die Sozialarbeit, Deradikalisierungsinitiativen und die Zusammenarbeit mit den betroffenen Gemeinschaften gelegt werden muss, um eine Radikalisierung in der Gesellschaft auf Dauer zu verhindern. **[Abänd. 3]**

(1b) ***Terroristische Inhalte sind Teil eines umfassenderen Problems illegaler Online-Inhalte, zu dem auch Inhalte anderer Art etwa in Zusammenhang mit der sexuellen Ausbeutung von Kindern, illegalen Geschäftspraktiken und der Verletzung von Rechten des geistigen Eigentums gehören. Der Handel mit illegalen Inhalten wird oft von terroristischen und anderen kriminellen Organisationen betrieben, um Geld zu waschen und Startkapital für die Finanzierung ihrer Aktivitäten aufzubringen. Dieses Problem erfordert eine Kombination aus legislativen, nichtlegislativen und freiwilligen Maßnahmen, basierend auf der Zusammenarbeit zwischen Behörden und Anbietern und unter uneingeschränkter Achtung der Grundrechte. Zwar wurde die von illegalen Inhalten ausgehende Bedrohung durch erfolgreiche Initiativen wie den von der Branche erstellten Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet und die „WePROTECT Global Alliance to end child sexual abuse online" eingedämmt, aber dennoch ist es notwendig, einen Rechtsrahmen für die grenzüberschreitende Zusammenarbeit zwischen den nationalen Regulierungsbehörden zur Entfernung illegaler Inhalte zu schaffen.*** **[Abänd. 4]**

(2) Hostingdiensteanbieter, die im Internet aktiv sind, spielen in der digitalen Wirtschaft eine zentrale Rolle, indem sie Unternehmen und Bürger miteinander verbinden***,*** ***Lernangebote bereitstellen*** und öffentliche Debatten sowie die Verbreitung und den Erhalt von Informationen, Meinungen und Ideen ermöglichen, was erheblich zu Innovation, Wirtschaftswachstum und der Schaffung von Arbeitsplätzen in der Union beiträgt. Mitunter werden ihre Dienste allerdings von Dritten für illegale Aktivitäten im Internet ausgenutzt. Besonders besorgniserregend ist der Missbrauch von Hostingdiensten durch terroristische Vereinigungen und ihre Unterstützer mit dem Ziel, terroristische Online-Inhalte zu verbreiten und so ihre Botschaften weiterzutragen, Menschen zu radikalisieren und anzuwerben sowie terroristische Aktivitäten zu erleichtern und zu lenken. **[Abänd. 5]**

(3) ~~Das Vorhandensein terroristischer~~ ***Terroristische*** Online-Inhalte ~~hat~~ ***haben sich, wenn auch nicht als einziger Faktor, als Katalysator für die Radikalisierung von Einzelpersonen erwiesen***, ***die terroristische Handlungen begangen haben, und haben daher*** schwerwiegende negative Folgen für die Nutzer, die Bürger und die Gesellschaft insgesamt ~~sowie~~***, aber auch*** für die Anbieter von Online-Diensten, die solche Inhalte zur Verfügung stellen, da dies das Vertrauen ihrer Nutzer untergräbt und ihre Geschäftsmodelle schädigt. Die Anbieter von Online-Diensten tragen angesichts ihrer zentralen Rolle und ~~der~~ ***proportional zu den*** mit ihrem Diensteangebot verbundenen technologischen ~~Mittel~~ ***Mitteln*** und Kapazitäten eine besondere gesellschaftliche Verantwortung dafür, ihre Dienste vor dem Missbrauch durch Terroristen zu schützen und ~~beim Umgang mit terroristischen Inhalten, die durch die Nutzung ihrer~~ ***den zuständigen Behörden dabei zu helfen***, ***gegen terroristische Inhalte vorzugehen, die über ihre*** Dienste verbreitet werden, ~~zu helfen~~ ***und dabei die grundlegende Bedeutung des Rechts auf freie Meinungsäußerung und der Freiheit zu berücksichtigen, Informationen und Ideen in einer offenen und demokratischen Gesellschaft zu erhalten und weiterzugeben***. **[Abänd. 6]**

(4) Die 2015 ~~begonnenen~~ ***eingeleiteten*** Bemühungen der Union zur Bekämpfung terroristischer Online-Inhalte durch einen Rahmen für die freiwillige Zusammenarbeit zwischen den Mitgliedstaaten und den Hostingdiensteanbietern müssen durch einen klaren Rechtsrahmen ergänzt werden, um den Zugang zu terroristischen Online-Inhalten weiter ~~zu verringern~~ ***einzudämmen*** und dem sich rasch ~~verändernden~~ ***ändernden*** Problem gerecht zu werden. Dieser Rechtsrahmen soll auf den freiwilligen Bemühungen aufbauen, die durch die Empfehlung (EU) 2018/334 der Kommission[3] verstärkt wurden, und entspricht der Forderung des Europäischen Parlaments, die Maßnahmen zur Bekämpfung illegaler und schädlicher Inhalte ***im Einklang mit dem in der Richtlinie 2000/31/EG festgelegten horizontalen Rahmen*** zu intensivieren, sowie des Europäischen Rats, die ~~automatische~~ Erkennung und Entfernung von zu terroristischen Handlungen anstiftenden Inhalten zu verbessern. **[Abänd. 7]**

---

3 Empfehlung (EU) 2018/334 der Kommission vom 1. März 2018 für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten (ABl. L 63 vom 6.3.2018, S. 50).

(5) Die Anwendung dieser Verordnung sollte die Anwendung ~~des Artikels 14~~ der Richtlinie 2000/31/EG[4] unberührt lassen. ~~Insbesondere sollten etwaige Maßnahmen, die der Hostingdiensteanbieter im Einklang mit dieser Verordnung ergriffen hat, darunter auch proaktive Maßnahmen, nicht automatisch dazu führen, dass der Diensteanbieter den in dieser Bestimmung vorgesehenen Haftungsausschluss nicht in Anspruch nehmen kann.~~ Diese Verordnung berührt nicht die Befugnisse der nationalen Behörden und Gerichte, in besonderen Fällen, in denen die Voraussetzungen ~~des Artikels 14~~ der Richtlinie 2000/31/EG für den Haftungsausschluss nicht erfüllt sind, die Haftung von Hostingdiensteanbietern festzustellen. **[Abänd. 8]**

(6) Bei der Festlegung der in dieser Verordnung enthaltenen Vorschriften zur Verhinderung des Missbrauchs von Hostingdiensten zur ~~Verbreitung~~ ***Bekämpfung*** terroristischer Online-Inhalte, die das reibungslose Funktionieren des Binnenmarkts gewährleisten sollen, ~~wurden~~ ***sollten*** die ~~durch die~~ ***in der*** Rechtsordnung der Union geschützten und in der Charta der Grundrechte der Europäischen Union ***uneingeschränkt*** garantierten ~~Grundrechte vollständig gewahrt~~ ***werden***. **[Abänd. 9]**

---

4 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) (ABl. L 178 vom 17.7.2000, S. 1).

(7) Diese Verordnung ~~trägt~~ ***soll*** zum Schutz der öffentlichen Sicherheit ~~bei~~ ***beitragen*** und ~~enthält~~ ***sollte*** gleichzeitig angemessene und solide Vorkehrungen zum Schutz der betreffenden Grundrechte ***enthalten***. Dazu gehören das Recht auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, das Recht auf wirksamen Rechtsbehelf, das Recht auf freie Meinungsäußerung, einschließlich der Freiheit, Informationen zu erhalten und weiterzugeben, die unternehmerische Freiheit und der Grundsatz der Nichtdiskriminierung. Die zuständigen Behörden und Hostingdiensteanbieter sollten nur Maßnahmen ergreifen, die ~~innerhalb~~ ***in*** einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sind, wobei der besonderen Bedeutung der ~~Meinungs- und Informationsfreiheit, die eine der~~ ***Meinungsfreiheit, der Freiheit***, ***Informationen und Ideen zu erhalten und weiterzugeben, der Rechte auf Achtung des Privat- und Familienlebens und des Schutzes personenbezogener Daten, die die*** wesentlichen Grundlagen einer pluralistischen, demokratischen Gesellschaft ~~und einen der~~ ***bilden und die*** grundlegenden Werte der Union ~~darstellt~~ ***darstellen***, Rechnung zu tragen ist. Maßnahmen~~, die~~ ***sollten*** sich ***nicht*** auf die Meinungs- und Informationsfreiheit auswirken~~, sollten in dem Sinne streng zielgerichtet sein, dass sie~~ ***und nach Möglichkeit*** dazu dienen müssen, die Verbreitung terroristischer Inhalte ~~zu verhindern~~ ***unter Verfolgung eines streng zielgerichteten Ansatzes zu bekämpfen***, ohne dadurch das Recht auf den rechtmäßigen Erhalt und die rechtmäßige Weitergabe von Informationen zu beeinträchtigen, wobei ~~der zentralen~~ ***die zentrale*** Rolle der Hostingdiensteanbieter, öffentliche Debatten sowie die Verbreitung und den Erhalt von Informationen, Meinungen und Ideen nach geltendem Recht zu erleichtern, zu berücksichtigen ist. ***Wirksame Maßnahmen zur Terrorismusbekämpfung im Internet und der Schutz des Rechts auf freie Meinungsäußerung sind keine widersprüchlichen, sondern vielmehr einander ergänzende und sich gegenseitig verstärkende Ziele.*** **[Abänd. 10]**

(8) Das Recht auf einen wirksamen Rechtsbehelf ist in Artikel 19 EUV und Artikel 47 der Charta der Grundrechte der Europäischen Union verankert. Jede natürliche oder juristische Person hat das Recht, gegen etwaige aufgrund dieser Verordnung getroffene Maßnahmen, die sich nachteilig auf ihre Rechte auswirken können, vor dem zuständigen nationalen Gericht Rechtsmittel einzulegen. Das Recht umfasst insbesondere die Möglichkeit der Hostingdienste- und Inhalteanbieter, Entfernungsanordnungen vor dem Gericht des Mitgliedstaats, dessen Behörden die Entfernungsanordnung ausgestellt haben, anzufechten***, sowie die Möglichkeiten der Inhalteanbieter, die von Hostingdiensteanbietern ergriffenen spezifischen Maßnahmen anzufechten***. **[Abänd. 11]**

(9) Um Klarheit über die Maßnahmen zu schaffen, die sowohl die Hostingdiensteanbieter als auch die zuständigen Behörden ergreifen sollten, um die Verbreitung terroristischer Online-Inhalte zu ~~verhindern~~ ***bekämpfen***, sollte in dieser Verordnung aufbauend auf der Definition terroristischer Straftatbestände in der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates[5] der Begriff „terroristische Inhalte“ präventiv definiert werden. In Anbetracht der Notwendigkeit, besonders schädliche terroristische ~~Online-Propaganda~~ ***Online-Inhalte*** zu bekämpfen, ~~sollten~~ ***sollte*** in der Definition ~~Materialien und Informationen~~ ***Material*** erfasst werden, ~~die~~ ***mit dem*** zur Begehung terroristischer Straftaten oder zu einem ~~Betrag~~ ***Beitrag*** zu diesen Straftaten anstifte~~n,~~ ~~diese(n) fördern oder befürworten, die Anweisungen für die Begehung solcher Straftaten enthalten oder für die Beteiligung an Handlungen einer terroristischen Vereinigung werben~~ ***angestiftet oder dazu aufgerufen oder für die Beteiligung an Handlungen einer terroristischen Vereinigung geworben wird und das somit mit der Gefahr einhergeht***, ***dass eine oder mehrere Straftaten dieser Art vorsätzlich begangen werden. Die Definition sollte ebenfalls Inhalte umfassen, die zum Zweck der Begehung terroristischer Straftaten Anleitungen zur Herstellung oder Verwendung von Sprengstoffen, Schusswaffen oder anderen Waffen oder schädlichen oder gefährlichen Stoffen sowie chemischen, biologischen, radiologischen und nuklearen Stoffen (CBRN-Stoffen) oder zu anderen Methoden oder Techniken einschließlich zur Auswahl von Anschlagszielen enthalten***. Bei solchen Informationen kann es sich um Texte, Bilder, Tonaufzeichnungen und Videos handeln. Bei der Beurteilung, ob es sich bei Inhalten um terroristische Inhalte im Sinne dieser Verordnung handelt, sollten die zuständigen Behörden und die Hostingdiensteanbieter Faktoren wie Art und Wortlaut der Aussagen, den Kontext, in dem die Aussagen getroffen wurden und ihr Gefährdungspotenzial und somit ihr Potenzial zur Beeinträchtigung der Sicherheit von Personen berücksichtigen. Die Tatsache, dass das Material von einer in der EU-Liste aufgeführten terroristischen Vereinigung oder Person hergestellt wurde, ihr zuzuschreiben ist oder in ihrem Namen verbreitet wird, stellt einen wichtigen Faktor bei der Beurteilung dar. Inhalte, die für Bildungs-, Presse- oder Forschungszwecke ***oder zum Zweck der Sensibilisierung gegenüber terroristischen Aktivitäten*** verbreitet werden, sollten angemessen

---

5 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).

geschützt werden. ***Insbesondere in Fällen, in denen der Inhalteanbieter eine redaktionelle Verantwortung trägt, sind Entscheidungen über die Entfernung verbreiteter Materialien unter Berücksichtigung der in einschlägigen Presse- und Medienvorschriften festgelegten journalistischen Standards, die im Einklang mit dem Unionsrecht und der Charta der Grundrechte stehen, zu treffen.*** Ferner sollte die Formulierung radikaler, polemischer oder kontroverser Ansichten zu sensiblen politischen Fragen in der öffentlichen Debatte nicht als terroristischer Inhalt betrachtet werden. **[Abänd. 12]**

(10) Zur Abdeckung solcher Online-Hostingdienste, in denen terroristische Inhalte verbreitet werden, sollte diese Verordnung für Dienste der Informationsgesellschaft gelten, die die durch einen Nutzer des Dienstes bereitgestellten Informationen in seinem Auftrag speichern und die gespeicherten Informationen ~~Dritten~~ ***der Öffentlichkeit*** zur Verfügung ~~zu~~ stellen, unabhängig davon, ob diese Tätigkeit rein technischer, automatischer und passiver Art ist. Beispiele für solche Anbieter von Diensten der Informationsgesellschaft sind Plattformen sozialer Medien, Videostreamingdienste, Video-, Bild- und Audio-Sharing-Dienste, File-Sharing- und andere Cloud-Dienste, sofern sie die Informationen ~~Dritten~~ ***der Öffentlichkeit*** zur Verfügung stellen, sowie Websites, auf denen die Nutzer Kommentare oder Rezensionen abgeben können. Die Verordnung sollte auch für Hostingdiensteanbieter gelten, die außerhalb der Union niedergelassen sind, aber innerhalb der Union Dienstleistungen anbieten, da ein erheblicher Teil der Hostingdiensteanbieter, die im Rahmen ihrer Dienstleistungen terroristischen Inhalten ausgesetzt sind, in Drittländern niedergelassen sind. Damit sollte sichergestellt werden, dass alle im digitalen Binnenmarkt tätigen Unternehmen unabhängig vom Land ihrer Niederlassung dieselben Anforderungen erfüllen. Damit festgestellt werden kann, ob ein Diensteanbieter Dienstleistungen in der Union anbietet, muss geprüft werden, ob der Diensteanbieter juristische oder natürliche Personen in einem oder mehreren Mitgliedstaaten in die Lage versetzt, seine Dienste in Anspruch zu nehmen. Allerdings sollte die bloße Zugänglichkeit der Website des Diensteanbieters oder einer E-Mail-Adresse oder anderer Kontaktdaten in einem oder mehreren Mitgliedstaaten, für sich genommen keine ausreichende Voraussetzung für die Anwendung dieser Verordnung sein. ***Sie sollte nicht für Cloud-Dienste – einschließlich Cloud-Diensten zwischen Unternehmen – gelten, bei denen der Diensteanbieter keine vertraglichen Verfügungsrechte dahingehend hat, welche Inhalte gespeichert werden oder wie diese verarbeitet oder durch seine Kunden oder die Endnutzer dieser Kunden veröffentlicht werden, und bei denen der Diensteanbieter technisch keine Möglichkeit hat, konkrete Inhalte zu löschen, die von seinen Kunden oder den Endnutzern seiner Dienste gespeichert werden.*** **[Abänd. 13]**

(11) Eine wesentliche Verbindung zur Union sollte für die Bestimmung des Anwendungsbereichs dieser Verordnung ebenfalls relevant sein. Eine solche wesentliche Verbindung zur Union sollte dann als gegeben gelten, wenn der Diensteanbieter eine Niederlassung in der Union hat, oder – in Ermangelung einer solchen – ~~anhand~~ ***aufgrund*** der Existenz einer erheblichen Zahl von Nutzern in einem oder mehreren Mitgliedstaaten oder der Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten ~~beurteilt~~ ***angenommen*** werden. Die Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten lässt sich anhand aller relevanten Umstände, einschließlich Faktoren wie der Verwendung einer in dem betreffenden Mitgliedstaat gebräuchlichen Sprache oder Währung ~~oder der Möglichkeit, Waren oder Dienstleistungen zu bestellen,~~ bestimmen. Ferner ließe sich die Ausrichtung von Tätigkeiten auf einen Mitgliedstaat auch von der Verfügbarkeit einer Anwendung im jeweiligen nationalen App-Store, von der Schaltung lokaler Werbung oder Werbung in der in dem betreffenden Mitgliedstaat verwendeten Sprache oder vom Management der Kundenbeziehungen, zum Beispiel durch die Bereitstellung eines Kundendienstes in der in dem betreffenden Mitgliedstaat gebräuchlichen Sprache, ableiten. Das Vorhandensein einer wesentlichen Verbindung sollte auch dann angenommen werden, wenn ein Diensteanbieter seine Tätigkeit nach Artikel 17 Absatz 1 Buchstabe c der Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates[6] auf einen oder mehrere Mitgliedstaaten ausrichtet. Andererseits kann die Erbringung der Dienstleistung zum Zwecke der bloßen Einhaltung des in der Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates[7] festgelegten Verbots der Diskriminierung nicht allein aus diesem Grund als Ausrichtung von Tätigkeiten auf ein bestimmtes Gebiet innerhalb der Union betrachtet werden. **[Abänd. 14]**

---

6 Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates vom 12. Dezember 2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (ABl. L 351 vom 20.12.2012, S. 1).

7 Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates vom 28. Februar 2018 über Maßnahmen gegen ungerechtfertigtes Geoblocking und andere Formen der Diskriminierung aufgrund der Staatsangehörigkeit, des Wohnsitzes oder des Ortes der Niederlassung des Kunden innerhalb des Binnenmarkts und zur Änderung der Verordnungen (EG) Nr. 2006/2004 und (EU) 2017/2394 sowie der Richtlinie 2009/22/EG (ABl. L 601 vom 2.3.2018, S. 1).

(12) Hostingdiensteanbieter sollten bestimmten Sorgfaltspflichten nachkommen, um die ***öffentliche*** Verbreitung terroristischer Inhalte über ihre Dienste zu ~~verhindern~~ ***bekämpfen***. Diese Sorgfaltspflichten sollten ~~nicht~~ ***weder auf eine allgemeine Verpflichtung der Hostingdiensteanbieter zur Überwachung der von ihnen gespeicherten Informationen noch*** auf eine allgemeine ~~Überwachungspflicht~~ ***Verpflichtung zur aktiven Suche nach Fakten oder Umständen, die auf illegale Aktivitäten hindeuten,*** hinauslaufen. Zu den Sorgfaltspflichten sollte gehören, dass die Hostingdiensteanbieter bei der Anwendung dieser Verordnung im Hinblick auf die von ihnen gespeicherten Inhalte insbesondere bei der Umsetzung ihrer eigenen Nutzungsbedingungen ***transparent,*** mit der gebotenen Sorgfalt, verhältnismäßig und ohne Diskriminierung handeln, um zu vermeiden, dass Inhalte nicht terroristischer Art entfernt werden. Die Entfernung oder Sperrung des Zugangs muss unter Beachtung der ~~Meinungs- und Informationsfreiheit~~ ***Meinungsfreiheit, der Freiheit, Informationen und Ideen in einer offenen und demokratischen Gesellschaft zu erhalten und weiterzugeben, sowie der Freiheit und der Pluralität der Medien*** erfolgen. **[Abänd. 15]**

(13) Das Verfahren und die Verpflichtungen, die sich nach einer Beurteilung durch die zuständigen Behörden aus den ~~gesetzmäßigen Anordnungen an die Hostingdiensteanbieter~~ ***Entfernungsanordnungen, mit denen Hostingdiensteanbieter aufgefordert werden***, terroristische Online-Inhalte zu entfernen oder den Zugang zu ihnen zu sperren, ergeben, sollten harmonisiert werden. Den Mitgliedstaaten sollte die Wahl der zuständigen Behörden frei stehen, sodass sie ~~Verwaltungs-, Strafverfolgungs- oder Justizbehörden~~ ***eine Justizbehörde oder eine funktional unabhängige Verwaltungs- oder Strafverfolgungsbehörde*** mit dieser Aufgabe betrauen können. Angesichts der Geschwindigkeit, mit der terroristische Inhalte über Online-Dienste hinweg verbreitet werden, erlegt diese Bestimmung den Hostingdiensteanbietern die Verpflichtung auf, dafür zu sorgen, dass die in der Entfernungsanordnung genannten terroristischen Inhalte innerhalb einer Stunde nach Erhalt der Entfernungsanordnung entfernt werden oder der Zugang dazu gesperrt wird. ~~Es obliegt den Hostingdiensteanbietern zu entscheiden, ob sie die betreffenden Inhalte entfernen oder den Zugang zu den Inhalten für Nutzer in der Union sperren.~~

[Abänd. 16]

(14) Die zuständige Behörde sollte die Entfernungsanordnung durch elektronische Mittel, die einen schriftlichen Nachweis unter Bedingungen ermöglichen, die dem Diensteanbieter die Authentifizierung des Absenders, einschließlich der Richtigkeit des Datums und der ~~Zeit~~ ***Uhrzeit*** der Absendung und des Eingangs der Anordnung, gestatten (z. B. über ein gesichertes E-Mail-System und ***gesicherte*** Plattformen oder sonstige gesicherte Kanäle, einschließlich der vom Diensteanbieter zur Verfügung gestellten), im Einklang mit den Vorschriften zum Schutz personenbezogener Daten direkt ~~an den Adressaten und die Kontaktstelle~~ ***der Kontaktstelle des Hostingdiensteanbieters und – wenn sich die Hauptniederlassung des Hostingdiensteanbieters in einem anderen Mitgliedstaat befindet – der zuständigen Behörde des betreffenden Mitgliedstaats*** übermitteln. Diese Anforderung kann insbesondere durch die Verwendung von qualifizierten Diensten für die Zustellung elektronischer Einschreiben gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates[8] erfüllt werden. **[Abänd. 17]**

[8] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

(15) Meldungen der zuständigen Behörden oder von Europol stellen ein wirksames und schnelles Mittel dar, um die Hostingdiensteanbieter auf die konkreten Inhalte ihrer Dienste aufmerksam zu machen. Neben den Entfernungsanordnungen sollte dieser Mechanismus, mit dem Hostingdiensteanbieter auf Informationen aufmerksam gemacht werden, die als terroristische Inhalte angesehen werden können und deren Vereinbarkeit mit ihren Nutzungsbedingungen sie somit freiwillig prüfen können, weiterhin verfügbar sein. Es ist wichtig, dass Hostingdiensteanbieter solche Meldungen vorrangig prüfen und rasch Rückmeldung zu den getroffenen Maßnahmen geben. Die endgültige Entscheidung darüber, ob der Inhalt aufgrund der Nichtvereinbarkeit mit den Nutzungsbedingungen entfernt wird oder nicht, bleibt beim Hostingdiensteanbieter. Das in der Verordnung (EU) 2016/794[9] festgelegte Mandat von Europol bleibt von der Durchführung dieser Verordnung im Hinblick auf die Meldungen unberührt. **[Abänd. 18]**

[9] Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.2016, S. 53).

(16) Angesichts des Umfangs und der Schnelligkeit, die für eine wirksame Erkennung und Entfernung terroristischer Inhalte erforderlich sind, sind verhältnismäßige ~~proaktive~~ ***spezifische*** Maßnahmen~~, einschließlich automatisierter Verfahren in bestimmten Fällen,~~ ein wesentliches Element bei der Bekämpfung terroristischer Online-Inhalte. Im Hinblick auf die Verringerung der Zugänglichkeit terroristischer Inhalte in ihren Diensten sollten die Hostingdiensteanbieter ***insbesondere in Fällen, in denen das Ausmaß der möglichen Beeinflussung durch terroristische Inhalte und der eingehenden Entfernungsanordnungen beträchtlich ist,*** prüfen, ob es in Abhängigkeit von Risiko und Ausmaß der möglichen Beeinflussung durch terroristische Inhalte sowie ~~von den~~ ***der*** Auswirkungen auf die Rechte Dritter und auf das öffentliche ~~Informationsinteresse~~ ***Interesse, Informationen zu erhalten und weiterzugeben,*** angemessen ist, ~~proaktive~~ ***spezifische*** Maßnahmen zu ergreifen. Aus diesem Grund sollten Hostingdiensteanbieter festlegen, welche geeigneten, ***gezielten,*** wirksamen und verhältnismäßigen ~~proaktiven~~ ***spezifischen*** Maßnahmen ergriffen werden sollten. Diese Anforderung sollte nicht mit einer allgemeinen Überwachungspflicht verbunden sein. ***Diese spezifischen Maßnahmen können eine regelmäßige Berichterstattung an die zuständigen Behörden, eine Aufstockung des mit Maßnahmen zum Schutz der Dienste vor einer öffentlichen Verbreitung terroristischer Inhalte befassten Personals und den Austausch bewährter Verfahren umfassen.*** Im Rahmen dieser Prüfung ist ~~das Fehlen von an einen~~ ***der Umstand, dass noch keine Entfernungsanordnungen an den*** Hostingdiensteanbieter ~~gerichteten Entfernungsanordnungen~~ ***ergangen sind,*** ein Hinweis auf eine geringe Beeinflussung durch terroristische Inhalte. **[Abänd. 19]**

(17) Bei der Durchführung ~~proaktiver~~ ***spezifischer*** Maßnahmen sollten die Hostingdiensteanbieter dafür sorgen, dass das Recht der Nutzer auf ~~Meinungs- und Informationsfreiheit – darunter das Recht~~ ***freie Meinungsäußerung und ihre Freiheit***, Informationen ~~frei zu empfangen und zu weitergeben –~~ ***und Ideen in einer offenen und demokratischen Gesellschaft zu erhalten und weiterzugeben,*** gewahrt ~~bleibt~~ ***bleiben***. Zusätzlich zu den gesetzlich festgelegten Anforderungen, einschließlich der Rechtsvorschriften über den Schutz personenbezogener Daten, sollten die Hostingdiensteanbieter mit der gebotenen Sorgfalt handeln und Schutzvorkehrungen ~~treffen, insbesondere durch menschliche~~ ***insbesondere in Form von menschlicher*** Aufsicht und Überprüfung ***treffen***, um gegebenenfalls unbeabsichtigte und irrtümliche Entscheidungen zu vermeiden, die dazu führen, dass nicht terroristische Inhalte entfernt werden. ~~Dies ist von besonderer Bedeutung, wenn Hostingdiensteanbieter automatisierte Verfahren zur Erkennung terroristischer Inhalte nutzen. Jede Entscheidung über die Verwendung automatisierter Verfahren, unabhängig davon, ob sie vom Hostingdiensteanbieter selbst oder auf Ersuchen der zuständigen Behörde getroffen wird, sollte im Hinblick auf die Zuverlässigkeit der zugrunde liegenden Technologie und die sich daraus ergebenden Auswirkungen auf die Grundrechte beurteilt werden.~~ **[Abänd. 20]**

(18) Um sicherzustellen, dass Hostingdiensteanbieter, die terroristischen Inhalten ausgesetzt sind, geeignete Maßnahmen ergreifen, um den Missbrauch ihrer Dienste zu verhindern, ~~sollten die zuständigen Behörden~~ ***sollte die zuständige Behörde*** die Hostingdiensteanbieter, ***an*** die ~~eine rechtskräftig gewordene Entfernungsanordnung erhalten haben~~ ***rechtskräftige Entfernungsanordnungen in großer Zahl ergangen sind***, ersuchen, über die ergriffenen ~~proaktiven~~ ***spezifischen*** Maßnahmen Bericht zu erstatten. ~~Dabei könnte es sich um Maßnahmen handeln, mit denen das erneute Hochladen terroristischer Inhalte, die aufgrund einer Entfernungsanordnung oder Meldung entfernt oder gesperrt wurden, verhindert werden soll, wobei öffentliche oder in Privatbesitz befindliche Werkzeuge mit bekanntem terroristischen Inhalt zu prüfen sind.~~ Sie können auch auf zuverlässige technische Hilfsmittel zurückgreifen, um neue terroristische Inhalte zu erkennen~~, und zwar entweder mithilfe der auf dem Markt verfügbaren oder der vom Hostingdiensteanbieter entwickelten Werkzeuge~~. Der Diensteanbieter sollte über die spezifischen ~~proaktiven~~ Maßnahmen Bericht erstatten, damit die zuständige Behörde beurteilen kann, ob die Maßnahmen ***notwendig,*** wirksam und verhältnismäßig sind und ob der Hostingdiensteanbieter – sofern automatisierte Verfahren zum Einsatz kommen – über die notwendigen Kapazitäten für die menschliche Aufsicht und Überprüfung verfügt. Bei der Bewertung der Wirksamkeit***, Notwendigkeit*** und Verhältnismäßigkeit der Maßnahmen sollten die zuständigen Behörden die einschlägigen Parameter berücksichtigen, einschließlich der Anzahl der an den Anbieter gerichteten Entfernungsanordnungen ~~und Meldungen~~, seiner ***Größe und*** wirtschaftlichen Leistungsfähigkeit und der Wirkung seines Dienstes bei der Verbreitung terroristischer Inhalte (z. B. unter Berücksichtigung der Zahl der Nutzer in der Union) ***sowie der Vorkehrungen für den Schutz des Rechts auf freie Meinungsäußerung und der Informationsfreiheit und der Anzahl der Fälle von Beschränkungen legaler Inhalte***. **[Abänd. 21]**

(19) Nach dem Ersuchen sollte die zuständige Behörde mit dem Hostingdiensteanbieter einen Dialog über die erforderlichen ~~proaktiven~~ ***spezifischen*** Maßnahmen aufnehmen. Falls erforderlich, sollte die zuständige Behörde ***den Hostingdiensteanbieter auffordern, die erforderlichen Maßnahmen erneut zu prüfen, oder verlangen, dass*** geeignete, wirksame und verhältnismäßige ~~proaktive~~ ***spezifische*** Maßnahmen ~~auferlegen~~ ***ergriffen werden***, wenn sie der Auffassung ist, dass die getroffenen Maßnahmen ***gegen die Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit verstoßen oder*** den Risiken nicht hinreichend gerecht werden. ~~Die Entscheidung,~~ ***Die zuständige Behörde sollte ausschließlich spezifische Maßnahmen verlangen, deren Durchführung unter Berücksichtigung verschiedener Faktoren wie der finanziellen und anderweitigen Ressourcen des Hostingdiensteanbieters vernünftigerweise von diesem erwartet werden kann. Eine Aufforderung,*** solche spezifischen ~~proaktiven~~ Maßnahmen ~~aufzuerlegen~~, sollte ~~grundsätzlich~~ nicht zur Auferlegung einer allgemeinen Überwachungspflicht nach Artikel 15 Absatz 1 der Richtlinie 2000/31/EG führen. ~~Angesichts der besonders schwerwiegenden Risiken, die mit der Verbreitung terroristischer Inhalte verbunden sind, könnten die Entscheidungen der zuständigen Behörden auf der Grundlage dieser Verordnung im Hinblick auf bestimmte gezielte Maßnahmen, deren Annahme aus übergeordneten Gründen der öffentlichen Sicherheit erforderlich ist, von dem Ansatz nach Artikel 15 Absatz 1 der Richtlinie 2000/31/EG abweichen. Vor der Annahme solcher Entscheidungen sollte die zuständige Behörde ein ausgewogenes Verhältnis zwischen den Zielen des Allgemeininteresses und den entsprechenden Grundrechten, insbesondere der Meinungs- und Informationsfreiheit sowie der unternehmerischen Freiheit, herstellen und eine angemessene Begründung liefern.~~ **[Abänd. 22]**

(20) Den Hostingdiensteanbietern sollte die Verpflichtung auferlegt werden, entfernte Inhalte und damit zusammenhängende Daten für bestimmte Zwecke für den unbedingt erforderlichen Zeitraum aufzubewahren. Es ist notwendig, die Aufbewahrungspflicht auf damit zusammenhängende Daten auszudehnen, soweit solche Daten andernfalls infolge der Entfernung des betreffenden Inhalts verloren gehen würden. Mit den Inhalten zusammenhängende Daten können beispielsweise „Teilnehmerdaten“, insbesondere Daten, die sich auf die Identität des Inhalteanbieters beziehen, und „Zugangsdaten“ umfassen, darunter das Datum und die Uhrzeit der Nutzung oder die Anmeldung bei und Abmeldung von dem Dienst, zusammen mit der IP-Adresse, die der Internetzugangsanbieter dem Inhalteanbieter zuweist.

(21) Die Verpflichtung zur Aufbewahrung der Inhalte für Verfahren der behördlichen oder gerichtlichen Kontrolle ***oder des verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs*** ist notwendig und gerechtfertigt, damit je nach ~~dem~~ Ergebnis des Überprüfungsverfahrens Rechtsbehelfe auch für den Inhalteanbieter, dessen Inhalte entfernt oder gesperrt wurden, wirksam sind ~~sowie~~ ***und*** die Reaktivierung dieses Inhalts in seiner vor der Entfernung bestehenden Form sichergestellt ~~werden~~ ***wird***. Die Verpflichtung zur Aufbewahrung der Inhalte für Ermittlungs- und Strafverfolgungszwecke ist notwendig und gerechtfertigt, da dieses Material ~~zur Störung oder Verhinderung terroristischer~~ ***wichtig sein könnte, um terroristische*** Aktivitäten ~~wertvoll sein könnte~~ ***zu stören oder zu verhindern***. Wenn Unternehmen~~,~~ ~~insbesondere durch ihre eigenen proaktiven~~ ***im Wege eigener spezifischer*** Maßnahmen~~,~~ Material entfernen oder den Zugang dazu sperren~~, und die zuständige Behörde nicht~~ ***sollten sie die zuständigen Strafverfolgungsbehörden unverzüglich*** davon in Kenntnis setzen***.*** ~~, weil sie der Auffassung sind, dass es nicht in den Anwendungsbereich von Artikel 13 Absatz 4 dieser Verordnung fällt, ist den Strafverfolgungsbehörden das Bestehen der Inhalte möglicherweise nicht bekannt~~. ~~Daher ist die~~ ***Die*** Aufbewahrung von Inhalten zu Zwecken der Verhinderung, Erkennung, Ermittlung und Verfolgung terroristischer Straftaten ebenfalls gerechtfertigt. ~~Aus diesen Gründen~~ ***Für diese Zwecke sollten terroristische Inhalte und die damit verbundenen Daten nur für einen bestimmten Zeitraum gespeichert werden***, ***der es den Strafverfolgungsbehörden ermöglicht, die Inhalte zu überprüfen und zu entscheiden, ob sie für diese konkreten Zwecke benötigt werden***. ***Diese Aufbewahrungsfrist sollte sechs Monate nicht überschreiten. Für die Zwecke der Verhinderung, Erkennung, Ermittlung und Verfolgung terroristischer Straftaten*** beschränkt sich die Verpflichtung zur Datenaufbewahrung auf Daten, die wahrscheinlich eine Verbindung mit terroristischen Straftaten aufweisen und die daher zur Verfolgung terroristischer Straftaten oder zur Verhütung ernsthafter Bedrohungen der öffentlichen Sicherheit beitragen können. **[Abänd. 24]**

(22) Um die Verhältnismäßigkeit zu gewährleisten, sollte der Aufbewahrungszeitraum auf sechs Monate begrenzt werden, damit die Inhalteanbieter ausreichend Zeit haben, das Überprüfungsverfahren einzuleiten, ~~und~~ ***oder*** 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~~ ***Überprüfungs- oder Rechtsbehelfsverfahren*** innerhalb des sechsmonatigen Zeitraums zwar eingeleitet, aber nicht abgeschlossen wurde. Diese Dauer sollte ***außerdem*** so bemessen sein, dass die Strafverfolgungsbehörden ~~die~~ ***das*** für die Ermittlungen ~~erforderlichen Beweismittel~~ ***und die Strafverfolgung benötigte Material*** unter Wahrung des Gleichgewichts mit den betreffenden Grundrechten sichern können. **[Abänd. 25]**

(23) Diese Verordnung berührt nicht 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.

(24) Im Hinblick auf terroristische Inhalte kommt es bei den Hostingdiensteanbietern auf die Transparenz ihrer Strategien an, denn nur so können sie ihrer Rechenschaftspflicht gegenüber ihren Nutzern nachkommen und das Vertrauen der Bürger in den digitalen Binnenmarkt stärken. ~~Die~~ ***Nur*** Hostingdiensteanbieter***, an die im betreffenden Jahr Entfernungsanordnungen ergangen sind,*** sollten jährliche Transparenzberichte mit aussagekräftigen Informationen über ihre Maßnahmen im Zusammenhang mit der Erkennung, Ermittlung und Entfernung terroristischer Inhalte veröffentlichen ***müssen***. **[Abänd. 26]**

(24a) Die zur Ausstellung von Entfernungsanordnungen befugten Behörden sollten ebenfalls Transparenzberichte veröffentlichen, die Angaben zur Anzahl der ausgestellten Entfernungsanordnungen, zur Anzahl der Ablehnungen, zur Anzahl der Fälle, in denen terroristische Inhalte erkannt wurden, die Untersuchungen und die Verfolgung terroristischer Straftaten nach sich zogen, und zur Anzahl der Fälle, in denen Inhalte fälschlicherweise als terroristische Inhalte identifiziert wurden, enthalten. **[Abänd. 27]**

(25) Beschwerdeverfahren stellen eine notwendige Schutzvorkehrung gegen die irrtümliche Entfernung von Inhalten dar, die im Rahmen der ~~Meinungs- und Informationsfreiheit~~ ***Meinungsfreiheit und der Freiheit, Informationen und Ideen in einer offenen und demokratischen Gesellschaft zu erhalten und weiterzugeben,*** geschützt sind. Die Hostingdiensteanbieter sollten daher nutzerfreundliche Beschwerdeverfahren einrichten und dafür sorgen, dass Beschwerden unverzüglich und in voller ***vollkommener*** Transparenz gegenüber dem Inhalteanbieter bearbeitet werden. Die Anforderung, dass Hostingdiensteanbieter irrtümlich entfernte Inhalte reaktivieren müssen, lässt die Möglichkeit unberührt, dass die Hostingdiensteanbieter ihre Nutzungsbedingungen aus anderen Gründen durchsetzen können. **[Abänd. 28]**

(26) Wirksame Rechtsbehelfe nach Artikel 19 EUV und Artikel 47 der Charta der Grundrechte der Europäischen Union setzen voraus, dass die betreffenden Personen in Erfahrung bringen können, warum die von ihnen hochgeladenen Inhalte entfernt oder gesperrt wurden. Zu diesem Zweck sollte der Hostingdiensteanbieter dem ~~Inhaltsanbieter~~ ***Inhalteanbieter*** aussagekräftige Informationen ***wie etwa die Gründe für die Entfernung oder Sperrung und die Rechtsgrundlage für die Maßnahme*** zur Verfügung stellen, die dem Inhalteanbieter die Anfechtung der Entscheidung ermöglichen. ~~Dies erfordert jedoch nicht notwendigerweise eine Benachrichtigung des Inhalteanbieters.~~ Je nach ~~den Umständen~~ ***Sachverhalt*** können Hostingdiensteanbieter Inhalte, die als terroristische Inhalte gelten, durch eine Nachricht ersetzen, dass sie im Einklang mit dieser Verordnung entfernt oder gesperrt wurden~~. Auf Anfrage sollten weitere Informationen über die Gründe und die Möglichkeiten des Inhalteanbieters zur Anfechtung der Entscheidung erteilt werden.~~ Sind die zuständigen Behörden der Auffassung, dass es aus Gründen der öffentlichen Sicherheit, auch im Rahmen einer Ermittlung, als unangemessen oder kontraproduktiv anzusehen ist, den Inhalteanbieter unmittelbar von der Entfernung oder Sperrung der Inhalte in Kenntnis zu setzen, sollten sie den Hostingdiensteanbieter hierüber informieren. **[Abänd. 29]**

(27) ~~Zur Vermeidung von~~ ***Um*** Doppelarbeit und ~~einer gegenseitigen~~ ***eine gegenseitige*** Behinderung bei (nationalen) Ermittlungen ***zu vermeiden und den Aufwand für die betroffenen Diensteanbieter so gering wie möglich zu halten,*** sollten ***sich*** die zuständigen Behörden bei der Erteilung von Entfernungsanordnungen ~~oder bei Meldungen~~ an die Hostingdiensteanbieter ~~sich~~ gegenseitig informieren und ~~miteinander~~ ***sich untereinander*** sowie gegebenenfalls mit Europol ~~koordinieren~~ ***abstimmen*** und kooperieren. Bei der Umsetzung der Bestimmungen dieser Verordnung könnte Europol im Einklang mit seinem derzeitigen Mandat und bestehenden Rechtsrahmen Unterstützung leisten. **[Abänd. 30]**

(27a) Meldungen von Europol stellen ein wirksames und schnelles Mittel dar, die Hostingdiensteanbieter auf bestimmte Inhalte ihrer Dienste aufmerksam zu machen. Neben den Entfernungsanordnungen sollte dieser Mechanismus, mit dem Hostingdiensteanbieter auf Informationen aufmerksam gemacht werden, die als terroristische Inhalte gelten können und deren Vereinbarkeit mit ihren Nutzungsbedingungen sie somit freiwillig prüfen können, weiterhin verfügbar sein. Aus diesem Grunde ist es wichtig, dass Hostingdiensteanbieter mit Europol zusammenarbeiten und der Prüfung der Meldungen von Europol große Bedeutung beimessen und rasch Rückmeldung zu den getroffenen Maßnahmen geben. Die endgültige Entscheidung darüber, ob der Inhalt aufgrund der Nichtvereinbarkeit mit den Nutzungsbedingungen entfernt wird oder nicht, bleibt dem Hostingdiensteanbieter vorbehalten. Das in der Verordnung (EU) 2016/794[10] festgelegte Mandat von Europol bleibt von der Durchführung dieser Verordnung unberührt. **[Abänd. 31]**

10 *Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.2016, S. 53).*

(28) Um die wirksame und ausreichend kohärente Durchführung ~~proaktiver~~ ***von*** Maßnahmen ***seitens der Hostingdiensteanbieter*** zu gewährleisten, sollten die zuständigen Behörden der Mitgliedstaaten in Bezug auf die Gespräche, die sie mit den Hostingdiensteanbietern ***zu Entfernungsanordnungen und der Ermittlung***, ***Umsetzung und Bewertung spezifischer Maßnahmen*** führen, zusammenarbeiten~~, um spezifische proaktive Maßnahmen zu ermitteln, umzusetzen und zu bewerten. In ähnlicher Weise ist.~~ ~~eine~~ ***Eine*** solche Zusammenarbeit ***ist*** auch hinsichtlich der Annahme von Vorschriften über Sanktionen sowie der Um- und Durchsetzung von Sanktionen erforderlich. **[Abänd. 32]**

(29) Es ist von wesentlicher Bedeutung, dass die zuständige Behörde in dem für die Verhängung der Sanktionen zuständigen Mitgliedstaat umfassend über die Erteilung von Entfernungsanordnungen ~~und Meldungen~~ sowie den anschließenden Austausch zwischen dem Hostingdiensteanbieter und ~~der~~ ***den*** jeweils zuständigen ~~Behörde~~ ***Behörden in anderen Mitgliedstaaten*** informiert ist. Zu diesem Zweck sollten die Mitgliedstaaten geeignete ***und sichere*** Kommunikationskanäle oder -mechanismen vorsehen, die die rechtzeitige Übermittlung der relevanten Informationen ermöglichen. **[Abänd. 33]**

(30) Um den raschen Austausch zwischen den zuständigen Behörden untereinander und mit den Hostingdiensteanbietern zu erleichtern und Doppelarbeit zu vermeiden, können die Mitgliedstaaten von Europol entwickelte Werkzeuge wie die aktuelle Verwaltungsanwendung für die Meldung von Internetinhalten (*Internet Referral Management application*, IRMa) oder deren Nachfolgewerkzeuge nutzen.

(31) Angesichts der besonders schwerwiegenden Folgen bestimmter terroristischer Inhalte sollten die Hostingdiensteanbieter unverzüglich die Behörden des betreffenden Mitgliedstaats oder die zuständigen Behörden des Mitgliedstaats, in dem sie niedergelassen sind oder einen gesetzlichen Vertreter haben, über das Vorliegen etwaiger Nachweise für terroristische Straftaten, von denen sie Kenntnis erlangen, informieren. Um die Verhältnismäßigkeit zu gewährleisten, ist diese Verpflichtung auf terroristische Straftaten im Sinne von Artikel 3 Absatz 1 der Richtlinie (EU) 2017/541 beschränkt. Die Informationspflicht bedeutet nicht, dass sich die Hostingdiensteanbieter aktiv um solche Nachweise bemühen müssen. Der betreffende Mitgliedstaat ist der Mitgliedstaat, der für die Ermittlung und strafrechtliche Verfolgung der terroristischen Straftaten gemäß der Richtlinie (EU) 2017/541 zuständig ist, und zwar auf der Grundlage der Staatsangehörigkeit des Täters bzw. des potenziellen Opfers der Straftat oder des Zielstandorts der terroristischen Handlung. Im Zweifelsfall können Hostingdiensteanbieter die Informationen an Europol übermitteln, das entsprechend seinem Mandat diese Informationen weiterverfolgen und auch an die zuständigen nationalen Behörden weiterleiten sollte.

(32) Die zuständigen Behörden in den Mitgliedstaaten sollten die Möglichkeit haben, solche Informationen zu nutzen, um Ermittlungsmaßnahmen zu ergreifen, die nach den nationalen Rechtsvorschriften oder Unionsrecht zur Verfügung stehen, einschließlich des Erlasses einer Europäischen Herausgabeanordnung gemäß der Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen[11].

[11] COM(2018)0225.

(33) Sowohl die Hostingdiensteanbieter als auch die Mitgliedstaaten sollten Kontaktstellen einrichten, um die rasche Bearbeitung von Entfernungsanordnungen ~~und Meldungen~~ zu erleichtern. Im Gegensatz zum gesetzlichen Vertreter dient die Kontaktstelle operativen Zwecken. Die Kontaktstelle des Hostingdiensteanbieters sollte in einer speziellen Einrichtung bestehen, die die elektronische Übermittlung von Entfernungsanordnungen ~~und Meldungen~~ ermöglicht, sowie technisch und personell so ausgestattet sein, dass eine ~~zügige~~ ***rasche*** Bearbeitung möglich ist. Die Kontaktstelle des Hostingdiensteanbieters muss sich nicht in der Union befinden; es steht dem Hostingdiensteanbieter frei, eine bestehende Kontaktstelle zu benennen, sofern diese Kontaktstelle in der Lage ist, die in dieser Verordnung vorgesehenen Aufgaben zu erfüllen. Um zu gewährleisten, dass terroristische Inhalte innerhalb einer Stunde nach Eingang der Entfernungsanordnung entfernt oder gesperrt werden, sollten die Hostingdiensteanbieter sicherstellen, dass die Kontaktstelle ständig rund um die Uhr erreichbar ist. In den Informationen über die Kontaktstelle sollte die Sprache angegeben werden, in der ~~die Kontaktstelle angeschrieben werden kann~~ ***eine Kontaktaufnahme mit der Kontaktstelle möglich ist***. Um die Kommunikation zwischen den Hostingdiensteanbietern und den zuständigen Behörden zu erleichtern, wird den Hostingdiensteanbietern empfohlen, die Kommunikation in einer der Amtssprachen der Union, in der ihre Nutzungsbedingungen verfügbar sind, zu ermöglichen. **[Abänd. 34]**

(34) Da für Diensteanbieter keine allgemeine Anforderung einer physischen Präsenz im Gebiet der Union besteht, muss der Mitgliedstaat bestimmt werden, unter dessen Gerichtsbarkeit der Hostingdiensteanbieter, der in der Union Dienstleistungen anbietet, fällt. In der Regel fällt der Hostingdiensteanbieter unter die Gerichtsbarkeit des Mitgliedstaats, in dem es seinen Hauptsitz hat oder einen gesetzlichen Vertreter benannt hat. ~~Wenn jedoch ein anderer Mitgliedstaat Entfernungsanordnung erteilt, sollten seine Behörden in der Lage sein, ihre Anordnungen durch Zwangsmaßnahmen ohne Strafcharakter, wie z. B. Strafzahlungen, durchzusetzen.~~ In Bezug auf einen Hostingdiensteanbieter, der nicht in der Union ansässig ist und keinen gesetzlichen Vertreter benennt, sollte jeder Mitgliedstaat in der Lage sein, dennoch Sanktionen zu verhängen, sofern der Grundsatz „*ne bis in idem*“ eingehalten wird. **[Abänd. 35]**

(35) Diese Hostingdiensteanbieter, die nicht in der Union niedergelassen sind, sollten schriftlich einen gesetzlichen Vertreter benennen, der die Einhaltung und Durchsetzung der sich aus dieser Verordnung ergebenden Verpflichtungen gewährleistet. ***Hostingdiensteanbieter können auf einen bestehenden gesetzlichen Vertreter zurückgreifen, sofern dieser in der Lage ist, die in dieser Verordnung dargelegten Aufgaben auszuführen.*** **[Abänd. 36]**

(36) Der gesetzliche Vertreter sollte rechtlich befugt sein, im Namen des Hostingdiensteanbieters zu handeln.

(37) Für die Zwecke dieser Verordnung sollten die Mitgliedstaaten ~~zuständige Behörden~~ ***eine einzige Justizbehörde oder funktional unabhängige Verwaltungsbehörde*** benennen. ~~Aus der Anforderung, zuständige Behörden zu benennen, folgt~~ ***Diese Anforderung erfordert*** nicht ~~notwendigerweise~~ die Einrichtung ~~neuer Behörden~~ ***einer neuen Behörde***, sondern es kann sich um ***eine*** bereits bestehende ~~Stellen~~ ***Stelle*** handeln, die mit den in dieser Verordnung festgelegten Aufgaben betraut ~~werden~~ ***wird***. Diese Verordnung schreibt die Benennung ~~der Behörden~~ ***einer Behörde*** vor, die für die Erteilung von Entfernungsanordnungen ~~und Meldungen~~ sowie die Aufsicht über ~~proaktive~~ ***spezifische*** Maßnahmen und die Verhängung von Sanktionen zuständig ~~sind~~ ***ist***. ~~Es ist Sache der~~ ***Die Mitgliedstaaten sollten der Kommission mitteilen, welche Behörde sie gemäß dieser Verordnung für zuständig erklärt haben, und die Kommission sollte im Internet eine Liste der in den einzelnen*** Mitgliedstaaten ~~zu entscheiden, wie viele Behörden sie für diese Aufgaben benennen wollen~~ ***jeweils zuständigen Behörde veröffentlichen. Dieses Online-Register sollte leicht zugänglich sein, damit die Hostingdiensteanbieter die Echtheit von Entfernungsanordnungen rasch prüfen können***. **[Abänd. 37]**

(38) Sanktionen sind erforderlich, damit gewährleistet ist, dass die Hostingdiensteanbieter die ihnen aus dieser Verordnung erwachsenden Verpflichtungen wirksam umsetzen. Die Mitgliedstaaten sollten Regeln für Sanktionen, gegebenenfalls auch Leitlinien für die Verhängung von Geldbußen, erlassen. ~~Besonders schwere~~ Sanktionen ***sollten*** ~~werden~~ für den Fall festgelegt ***werden***, ~~dass der Hostingdiensteanbieter terroristische Inhalte systematisch nicht innerhalb einer Stunde nach Eingang einer Entfernungsanordnung entfernt oder sperrt. Verstöße in Einzelfällen könnten sanktioniert werden, während gleichzeitig der Grundsatz „*ne bis in idem*“ sowie die Verhältnismäßigkeit gewahrt bleiben und sichergestellt wird, dass solche Sanktionen systematischen Verstößen Rechnung tragen. Um Rechtssicherheit zu gewährleisten, sollte in der~~ ***dass die Hostingdiensteanbieter den ihnen aus dieser*** Verordnung ~~festgelegt werden, in welchem Umfang die einschlägigen~~ ***erwachsenden*** Verpflichtungen ~~mit Sanktionen belegt werden können~~ ***systematisch und ständig nicht nachkommen***. Sanktionen für Verstöße gegen Artikel 6 sollten nur im Zusammenhang mit ~~der Berichtspflicht nach Artikel 6 Absatz 2 oder einer Entscheidung zur Auferlegung~~ ***den Pflichten, die sich aus einer Aufforderung zur Umsetzung*** zusätzlicher ~~proaktiver~~ ***spezifischer*** Maßnahmen nach Artikel 6 Absatz 4 ***ergeben,*** verhängt werden. Bei der Entscheidung, ob finanzielle Sanktionen verhängt werden sollen, sollten die finanziellen Mittel des Anbieters gebührend berücksichtigt werden. ***Darüber hinaus sollte die zuständige Behörde berücksichtigen, ob es sich bei dem Hostingdiensteanbieter um ein Start-up oder ein kleines oder mittleres Unternehmen handelt, und fallbezogen prüfen, ob der Anbieter in der Lage war, der Anordnung angemessen nachzukommen.*** Die Mitgliedstaaten ~~stellen sicher~~ ***sollten sicherstellen***, dass Sanktionen nicht dazu führen, dass nicht terroristische Inhalte entfernt werden. **[Abänd. 38]**

(39) Die Verwendung standardisierter Formulare erleichtert die Zusammenarbeit und den Informationsaustausch zwischen den zuständigen Behörden und den Diensteanbietern, sodass sie schneller und wirksamer kommunizieren können. Besonders wichtig ist es, nach Eingang einer Entfernungsanordnung rasches Handeln zu gewährleisten. Solche Formulare senken die Übersetzungskosten und tragen zu einem hohen Qualitätsstandard bei. Auch die Antwortformulare sollten einen standardisierten Informationsaustausch ermöglichen, was besonders wichtig ist, wenn die Diensteanbieter der Anordnung nicht nachkommen können. Mithilfe authentifizierter Übertragungskanäle kann die Echtheit der Entfernungsanordnung, einschließlich der Richtigkeit des Datums und der Zeit der Absendung und des Eingangs der Anordnung, gewährleistet werden.

(40) Um gegebenenfalls eine rasche Änderung des Inhalts der für die Zwecke dieser Verordnung zu verwendenden Formulare zu ermöglichen, sollte der Kommission die Befugnis übertragen werden, nach Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union Rechtsakte zur Änderung der Anhänge I, II und III dieser Verordnung zu erlassen. Damit der Entwicklung der Technik und des damit verbundenen Rechtsrahmens Rechnung getragen werden kann, sollte der Kommission ferner die Befugnis übertragen werden, delegierte Rechtsakte zu erlassen, um diese Verordnung durch technische Anforderungen an die von den zuständigen Behörden für die Übermittlung von Entfernungsanordnungen zu verwendenden elektronischen Mittel zu ergänzen. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, und dass diese Konsultationen mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[12] niedergelegt wurden. Um insbesondere eine gleichberechtigte Beteiligung an der Ausarbeitung der delegierten Rechtsakte zu gewährleisten, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Ausarbeitung der delegierten Rechtsakte befasst sind.

---

12 ABl. L 123 vom 12.5.2016, S. 1.

(41) Die Mitgliedstaaten sollten Informationen über die Umsetzung der Rechtsvorschriften sammeln***, einschließlich Informationen über die Anzahl der Fälle, in denen terroristische Straftaten als Folge dieser Verordnung erfolgreich aufgedeckt, untersucht und verfolgt wurden***. Es sollte ein detailliertes Programm zur Überwachung der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung erstellt werden, um die Bewertung zu erleichtern. **[Abänd. 39]**

(42) Anhand der Ergebnisse und Schlussfolgerungen des Umsetzungsberichts und der Ergebnisse der Überwachung sollte die Kommission ~~frühestens drei Jahre~~ ***ein Jahr*** nach ihrem Inkrafttreten eine Bewertung dieser Verordnung vornehmen. Die Bewertung sollte sich auf die ~~fünf~~ ***sieben*** Kriterien Effizienz, ***Erforderlichkeit, Verhältnismäßigkeit,*** Wirksamkeit, Relevanz, Kohärenz und EU-Mehrwert stützen. Bewertet ~~wird~~ ***werden sollte*** die Funktionsweise der verschiedenen in der Verordnung vorgesehenen operativen und technischen Maßnahmen, einschließlich der Wirksamkeit von Maßnahmen zur Verbesserung der Erkennung, Ermittlung und Entfernung terroristischer Inhalte, der Wirksamkeit der Schutzvorkehrungen sowie der Auswirkungen auf potenziell beeinträchtigte ~~Rechte und~~ ***Grundrechte, darunter die Meinungsfreiheit, die Freiheit, Informationen zu erhalten und weiterzugeben, die Freiheit und der Pluralismus der Medien, die unternehmerische Freiheit und das Recht auf Privatsphäre und den Schutz personenbezogener Daten. Außerdem sollte die Kommission die Auswirkungen auf potenziell beeinträchtigte*** Interessen Dritter ***bewerten***, ~~darunter die~~ ***einschließlich einer*** Überprüfung der Verpflichtung zur Unterrichtung der Inhalteanbieter. **[Abänd. 40]**

(43) Da das Ziel dieser Verordnung, nämlich die Gewährleistung eines reibungslosen Funktionierens des digitalen Binnenmarkts durch die Verhinderung der Verbreitung terroristischer Online-Inhalte, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann und daher vielmehr wegen des Umfangs und der Wirkungen dieser Beschränkung auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das zur Erreichung dieses Ziels erforderliche Maß hinaus —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

ABSCHNITT I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Anwendungsbereich

(1) In dieser Verordnung werden ***gezielte*** einheitliche Vorschriften zur ~~Verhinderung~~ ***Bekämpfung*** des Missbrauchs von Hosting-Diensten zur ***öffentlichen*** Verbreitung terroristischer Online-Inhalte festgelegt. Insbesondere werden festgelegt: **[Abänd. 41]**

a) Vorschriften über ***angemessene und verhältnismäßige*** Sorgfaltspflichten, die von den Hostingdiensteanbietern anzuwenden sind, um die ***öffentliche*** Verbreitung terroristischer Inhalte durch ihre Dienste zu ~~verhindern~~ ***bekämpfen*** und erforderlichenfalls die rasche Entfernung solcher Inhalte zu gewährleisten; **[Abänd. 42]**

b) eine Reihe Maßnahmen, die von den Mitgliedstaaten umzusetzen sind, um terroristische Inhalte zu ermitteln, deren rasche Entfernung durch die Hostingdiensteanbieter ***im Einklang mit dem Unionsrecht unter Bereitstellung geeigneter Schutzvorkehrungen zur Wahrung der Meinungsfreiheit und der Freiheit, Informationen und Ideen in einer offenen und demokratischen Gesellschaft zu erhalten und weiterzugeben,*** zu ermöglichen und die Zusammenarbeit mit den zuständigen Behörden der anderen Mitgliedstaaten, Hostingdiensteanbietern und gegebenenfalls den zuständigen Einrichtungen der Union zu erleichtern. **[Abänd. 43]**

(2) Diese Verordnung gilt für Hostingdiensteanbieter, die ***der Öffentlichkeit*** unabhängig vom Ort ihrer Hauptniederlassung Dienstleistungen in der Union anbieten.
[Abänd. 44]

(2a) Diese Verordnung gilt weder für Inhalte, die für Zwecke der Bildung, Kunst, Presse oder Forschung oder für Zwecke der Sensibilisierung für terroristische Aktivitäten verbreitet werden, noch für Inhalte, durch die polemische oder kontroverse Ansichten im Rahmen der öffentlichen Debatte zum Ausdruck gebracht werden. **[Abänd. 45]**

(2b) Diese Verordnung berührt nicht die Pflicht, die in Artikel 6 des Vertrags über die Europäische Union verankerten Rechte, Freiheiten und Grundsätze zu achten, und gilt unbeschadet der im Unionsrecht und nationalen Recht verankerten Grundsätze der Redefreiheit, der Pressefreiheit sowie der Freiheit und des Pluralismus der Medien. **[Abänd. 46]**

(2c) Diese Verordnung lässt die Richtlinie 2000/31/EG unberührt. **[Abänd. 47]**

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

-1. „Dienste der Informationsgesellschaft“ Dienste im Sinne des Artikels 2 Buchstabe a der Richtlinie 2000/31/EG; **[Abänd. 48]**

1. „Hostingdiensteanbieter“ einen Anbieter von Diensten der Informationsgesellschaft, die darin bestehen, die durch einen Inhalteanbieter bereitgestellten Informationen im Auftrag des Inhalteanbieters zu speichern und die gespeicherten Informationen ~~Dritten~~ ***der Öffentlichkeit*** zur Verfügung zu stellen***. Dies gilt ausschließlich für Dienste, die der Öffentlichkeit auf der Anwendungsebene zur Verfügung gestellt werden. Anbieter von Cloud-Infrastruktur und Cloud-Anbieter gelten nicht als Hostingdiensteanbieter. Ausgenommen sind auch elektronische Kommunikationsdienste im Sinne der Richtlinie (EU) 2018/1972***; **[Abänd. 49]**

2. „Inhalteanbieter“ einen Nutzer, der Informationen bereitgestellt hat, die in seinem Auftrag von einem Hostingdiensteanbieter gespeichert ***und der Öffentlichkeit zur Verfügung gestellt*** wurden oder ~~gespeichert~~ werden; **[Abänd. 50]**

3. „in der Union Dienstleistungen anbieten“ die Befähigung von juristischen oder natürlichen Personen in einem oder mehreren Mitgliedstaaten zur Nutzung der Dienste des Hostingdiensteanbieters, der eine wesentliche Verbindung zu dem betreffenden Mitgliedstaat oder den Mitgliedstaaten hat, wie

   a) eine Niederlassung des Hostingdiensteanbieters in der Union;

   b) eine erhebliche Zahl von Nutzern in einem oder mehreren Mitgliedstaaten;

   c) die Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten;

~~4. „terroristische Straftaten“ Straftaten im Sinne des Artikels 3 Absatz 1 der Richtlinie (EU) 2017/541;~~ **[Abänd. 51]**

5. „terroristische Inhalte“ ~~eine oder mehrere der folgenden Informationen~~ ***wie folgt geartetes Material, einzeln oder in Kombination***:

   a) ~~der Aufruf zu oder die Befürwortung von terroristischen~~ ***Aufruf zur Begehung einer der in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten*** Straftaten, ~~auch durch ihre~~ ***wenn durch ein solches Verhalten direkt oder indirekt, z. B. durch*** Verherrlichung~~, mit der~~ ***terroristischer Handlungen***, ***die Begehung terroristischer Straftaten befürwortet wird und*** damit ~~einhergehenden~~ ***die*** Gefahr ***besteht***, dass ~~solche~~ ~~Taten~~ ***eine oder mehrere dieser Straftaten vorsätzlich*** begangen werden könnten; **[Abänd. 53]**

b) ~~die Ermutigung, an terroristischen~~ ***an eine andere Person oder Personengruppe gerichtete Aufforderung***, ***eine der in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten*** Straftaten ***zu begehen oder daran*** mitzuwirken***, mit der damit einhergehenden Gefahr, dass eine oder mehrere dieser Straftaten vorsätzlich begangen werden***; **[Abänd. 54]**

c) ~~die Förderung der Aktivitäten einer terroristischen Vereinigung, insbesondere durch Ermutigung zur Beteiligung~~ ***an eine andere Person oder Personengruppe gerichtete Aufforderung***, ***sich im Sinne von Artikel 4 der Richtlinie (EU) 2017/541 etwa durch Bereitstellung von Informationen oder materiellen Mitteln oder durch jegliche Art der Finanzierung ihrer Tätigkeit*** an ~~oder Unterstützung~~ ***den Handlungen*** einer terroristischen Vereinigung ~~im Sinne des Artikels 2 Absatz 3 der Richtlinie (EU) 2017/541~~ ***zu beteiligen, mit der damit einhergehenden Gefahr, dass eine oder mehrere dieser Straftaten vorsätzlich begangen werden***; **[Abänd. 55]**

d) ~~technische Anleitungen oder~~ ***Unterweisung in der Herstellung oder im Gebrauch von Sprengstoffen, Schuss- oder sonstigen Waffen oder schädlichen oder gefährlichen Stoffen beziehungsweise Unterweisung in anderen spezifischen*** Methoden ~~für das Begehen terroristischer Straftaten~~ ***oder Verfahren mit dem Ziel, eine in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführte terroristische Straftat zu begehen oder zu deren Begehung beizutragen***; **[Abänd. 56]**

da) Darstellung der Begehung einer oder mehrerer der in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten Straftaten, mit der damit einhergehenden Gefahr, dass eine oder mehrere dieser Straftaten vorsätzlich begangen werden; **[Abänd. 57]**

6. „Verbreitung terroristischer Inhalte“ die ***öffentliche*** Bereitstellung terroristischer Inhalte ~~für Dritte~~ durch die Dienste des Hostingdiensteanbieters; **[Abänd. 58]**

7. „Nutzungsbedingungen“ sämtliche Bestimmungen, Bedingungen und Klauseln, unabhängig von ihrer Bezeichnung oder Form, zur Regelung der vertraglichen Beziehungen zwischen dem Hostingdiensteanbieter und seinen Nutzern;

~~8. „Meldung“ eine von einer zuständigen Behörde oder gegebenenfalls einer zuständigen Einrichtung der Union an einen Hostingdiensteanbieter gerichtete Mitteilung in Bezug auf Informationen, die als terroristischer Inhalt erachtet werden können und vom Anbieter auf freiwilliger Basis auf ihre Vereinbarkeit mit seinen eigenen Nutzungsbedingungen zur Verhinderung der Verbreitung terroristischer Inhalte geprüft werden;~~ **[Abänd. 59]**

9. „Hauptniederlassung“ die Hauptverwaltung oder der eingetragene Sitz, wo die wichtigsten Finanzfunktionen und die betriebliche Kontrolle ausgeübt werden.

9a. ***„zuständige Behörde“ eine einzige benannte Justizbehörde oder funktional unabhängige Verwaltungsbehörde in dem Mitgliedstaat.*** **[Abänd. 60]**

ABSCHNITT II

MASSNAHMEN ZUR VERHINDERUNG DER VERBREITUNG TERRORISTISCHER ONLINE-INHALTE

Artikel 3

Sorgfaltspflichten

(1) Die Hostingdiensteanbieter ~~ergreifen geeignete, angemessene und verhältnismäßige Maßnahmen~~ ***handeln*** im Einklang mit dieser Verordnung, um die ~~Verbreitung terroristischer Inhalte zu verhindern und die~~ Nutzer vor terroristischen Inhalten zu schützen. Sie handeln dabei mit der gebotenen Sorgfalt, verhältnismäßig und ohne Diskriminierung sowie ***allen Umständen unter*** unter gebührender Berücksichtigung der Grundrechte der Nutzer und tragen der grundlegenden Bedeutung der ~~Meinungs- und Informationsfreiheit~~ ***Meinungsfreiheit und der Freiheit, Informationen und Ideen*** in einer offenen und demokratischen Gesellschaft ***zu erhalten und weiterzugeben,*** Rechnung***, um zu verhindern, dass Inhalte nicht terroristischer Art entfernt werden***. **[Abänd. 61]**

(1a) Diese Sorgfaltspflichten laufen weder auf eine allgemeine Verpflichtung der Hostingdiensteanbieter zur Überwachung der von ihnen übertragenen oder gespeicherten Informationen noch auf eine allgemeine Verpflichtung zur aktiven Suche nach Fakten oder Umständen, die auf illegale Aktivitäten hindeuten, hinaus. **[Abänd. 62]**

~~(2) Die Hostingdiensteanbieter nehmen in ihre Nutzungsbedingungen Bestimmungen zur Verhinderung der Verbreitung terroristischer Inhalte auf und wenden diese an.~~ **[Abänd. 63]**

(2a) Erhalten Hostingdiensteanbieter Kenntnis von terroristischen Inhalten im Rahmen ihrer Dienste oder werden sie dieser gewahr, so unterrichten sie die zuständigen Behörden über diese Inhalte und entfernen sie rasch. **[Abänd. 64]**

(2b) Hostingdiensteanbieter, die die Kriterien gemäß der Definition des Begriffs „Video-Sharing-Plattform-Anbieter“ in der Richtlinie (EU) 2018/1808 erfüllen, ergreifen im Einklang mit Artikel 28b Absatz 1 Buchstabe c und Absatz 3 der Richtlinie (EU) 2018/2018 geeignete Maßnahmen zur Bekämpfung der Verbreitung terroristischer Inhalte. **[Abänd. 65]**

Artikel 4

Entfernungsanordnungen

(1) Die zuständige Behörde ***des Mitgliedstaats, in dem sich die Hauptniederlassung des Hostingdiensteanbieters befindet,*** ist befugt, ~~Entscheidungen~~ ***Entfernungsanordnungen*** zu erlassen, mit denen Hostingdiensteanbieter verpflichtet werden, terroristische Inhalte zu entfernen oder ***in allen Mitgliedstaaten*** zu sperren. **[Abänd. 66]**

(1a) Die zuständige Behörde eines Mitgliedstaats, in dem der Hostingdiensteanbieter nicht seine Hauptniederlassung oder keinen gesetzlichen Vertreter hat, kann darum ersuchen, dass der Zugang zu terroristischen Inhalten gesperrt wird, und diese Aufforderung in seinem Hoheitsgebiet vollstrecken lassen. **[Abänd. 67]**

(1b) Wenn von der jeweils zuständigen Behörde zuvor noch keine Entfernungsanordnung an einen Hostingdiensteanbieter ergangen ist, nimmt sie mindestens 12 Stunden vor Ausstellung einer Entfernungsanordnung Kontakt zu dem Hostingdiensteanbieter auf und unterrichtet ihn über die Verfahrensweisen und die geltenden Fristen. **[Abänd. 68]**

(2) ~~Die Hostingdiensteanbieter entfernen die terroristischen Inhalte innerhalb~~ ***Innerhalb*** einer Stunde nach Erhalt der Entfernungsanordnung ***entfernen die Hostingdiensteanbieter die terroristischen Inhalte schnellstmöglich*** oder sperren den Zugang dazu. **[Abänd. 69]**

(3) Entfernungsanordnungen müssen folgende Angaben gemäß dem Formular in Anhang I enthalten:

a) ~~Bezeichnung~~ ***eine elektronische Signatur, die die Identifizierung*** der zuständigen Behörde, die die Entfernungsanordnung ausgestellt hat***,*** ***ermöglicht***, und die Authentifizierung der Entfernungsanordnung durch die zuständige Behörde; **[Abänd. 70]**

b) eine ***detaillierte*** Darlegung der Gründe, aus denen der Inhalt als terroristischer Inhalt erachtet wird, ~~zumindest durch~~ ***und eine spezifische*** Bezugnahme auf die in Artikel 2 Absatz 5 aufgeführten Kategorien terroristischer Inhalte; **[Abänd. 71]**

c) einen ***genauen*** Uniform Resource Locator (URL-Adresse) und gegebenenfalls weitere Angaben, die die Identifizierung der gemeldeten Inhalte ermöglichen; **[Abänd. 72]**

d) einen Verweis auf die vorliegende Verordnung als Rechtsgrundlage der Entfernungsanordnung;

e) Datum und Uhrzeit der Ausstellung;

f) ***leicht verständliche*** Informationen über Rechtsbehelfe, die dem Hostingdiensteanbieter und dem Inhalteanbieter zur Verfügung stehen***, einschließlich Rechtsbehelfen bei der zuständigen Behörde sowie der Möglichkeit der Befassung eines Gerichts, und über die für die Einlegung von Rechtsbehelfen geltenden Fristen***; **[Abänd. 73]**

g) ~~gegebenenfalls~~ ***sofern notwendig und verhältnismäßig,*** die Entscheidung nach Artikel 11, ***dass*** keine Informationen über die Entfernung oder die Sperrung terroristischer Inhalte ~~weiterzugeben~~ ***weitergegeben werden dürfen***. **[Abänd. 74]**

~~(4) Auf Antrag des Hostingdiensteanbieters oder des Inhalteanbieters legt die zuständige Behörde eine ausführliche Begründung vor, unbeschadet der Verpflichtung des Hostingdiensteanbieters, der Entfernungsanordnung innerhalb der in Absatz 2 genannten Frist nachzukommen.~~ **[Abänd. 75]**

(5) Die ~~zuständigen Behörden richten~~ ***zuständige Behörde richtet*** Entfernungsanordnungen an die Hauptniederlassung des Hostingdiensteanbieters oder an den vom Hostingdiensteanbieter nach Artikel 16 benannten gesetzlichen Vertreter und ~~übermitteln~~ ***übermittelt*** sie der in Artikel 14 Absatz 1 genannten Kontaktstelle. Diese Anordnungen werden durch elektronische Mittel versandt, die einen schriftlichen Nachweis unter Bedingungen ermöglichen, die die Authentifizierung des Absenders, einschließlich der Richtigkeit des Datums und der ~~Zeit~~ ***Uhrzeit*** der Absendung und des Eingangs der Anordnung, gestatten.
[Abänd. 76]

(6) Die Hostingdiensteanbieter ~~bestätigen den Eingang und~~ unterrichten die zuständige Behörde unverzüglich über die Entfernung oder die Sperrung der terroristischen Inhalte unter Verwendung des Formulars in Anhang II und geben dabei insbesondere den Zeitpunkt der Maßnahme an. **[Abänd. 77]**

(7) Kann der Hostingdiensteanbieter der Entfernungsanordnung wegen höherer Gewalt oder einer faktischen Unmöglichkeit, die dem Hostingdiensteanbieter nicht angelastet werden kann, ***einschließlich technischer oder betrieblicher Gründe,*** nicht nachkommen, so teilt er dies der zuständigen Behörde ***unverzüglich*** mit und legt unter Verwendung des Formulars in Anhang III die Gründe hierfür dar. Die in Absatz 2 genannte Frist findet Anwendung, sobald die angeführten Gründe nicht mehr vorliegen. **[Abänd. 78]**

(8) ~~Kann der~~ ***Der*** Hostingdiensteanbieter ~~der Entfernungsanordnung nicht nachkommen~~ ***kann sich weigern***, ~~weil~~ die Entfernungsanordnung ***auszuführen, wenn diese*** offensichtliche Fehler ~~oder unzureichende Informationen~~ enthält~~, um die Anordnung auszuführen, so~~***. Er*** teilt ~~er~~ dies der zuständigen Behörde mit und ersucht unter Verwendung des Formulars in Anhang III um die notwendige Klarstellung. Die in Absatz 2 genannte Frist findet Anwendung, sobald die Klarstellung erfolgt ist. **[Abänd. 79]**

(9) Die zuständige Behörde, die die Entfernungsanordnung ausgestellt hat, unterrichtet die für die Überwachung der Durchführung ~~proaktiver~~ ***spezifischer*** Maßnahmen nach Artikel 17 Absatz 1 Buchstabe c zuständige Behörde, wenn die Entfernungsanordnung rechtskräftig wird. Eine Entfernungsanordnung wird rechtskräftig, wenn innerhalb der nach anwendbarem nationalem Recht geltenden Frist kein Rechtsbehelf gegen sie eingelegt oder sie nach Einlegung eines Rechtsbehelfs bestätigt wurde. **[Abänd. 80]**

Artikel 4a

Konsultationsverfahren für Entfernungsanordnungen

(1) ***Die zuständige Behörde, die eine Entfernungsanordnung nach Artikel 4 Absatz 1a ausstellt, sendet gleichzeitig mit der Übermittlung der Entfernungsanordnung an den Hostingdiensteanbieter gemäß Artikel 4 Absatz 5 eine Kopie der Entfernungsanordnung an die zuständige Behörde nach Artikel 17 Absatz 1 Buchstabe a des Mitgliedstaats, in dem sich die Hauptniederlassung des Hostingdiensteanbieters befindet.***

(2) ***Wenn die zuständige Behörde des Mitgliedstaats, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat, berechtigten Grund zu der Annahme hat, dass sich die Entfernungsanordnung auf grundlegende Interessen dieses Mitgliedstaats auswirken könnte, unterrichtet sie die zuständige Anordnungsbehörde. Die Anordnungsbehörde berücksichtigt diese Umstände und zieht die Entfernungsanordnung erforderlichenfalls zurück oder passt sie entsprechend an.*** **[Abänd. 81]**

Artikel 4b

Kooperationsverfahren für die Ausstellung einer weiteren Entfernungsanordnung

(1) Hat eine zuständige Behörde eine Entfernungsanordnung gemäß Artikel 4 Absatz 1a ausgestellt, so kann diese Behörde Kontakt zu der zuständigen Behörde des Mitgliedstaats aufnehmen, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat, um sie aufzufordern, ebenfalls eine Entfernungsanordnung gemäß Artikel 4 Absatz 1 auszustellen.

(2) Schnellstmöglich, spätestens jedoch eine Stunde nach der Kontaktaufnahme gemäß Absatz 1, stellt die zuständige Behörde in dem Mitgliedstaat, in dem sich die Hauptniederlassung des Hostingdiensteanbieters befindet, entweder eine Entfernungsanordnung aus oder lehnt die Ausstellung einer Entfernungsanordnung ab und unterrichtet die zuständige Behörde, die die erste Anordnung ausgestellt hat, über ihre Entscheidung.

(3) In Fällen, in denen die zuständige Behörde in dem Mitgliedstaat, in dem sich die Hauptniederlassung befindet, mehr als eine Stunde benötigt, um eine eigene Bewertung des Inhalts vorzunehmen, übermittelt sie dem betreffenden Hostingdiensteanbieter eine Aufforderung, den Zugang zu dem Inhalt für bis zu 24 Stunden vorläufig zu sperren; während dieser Zeit nimmt die zuständige Behörde die Bewertung vor und übermittelt die Entfernungsanordnung oder zieht die Aufforderung zur Sperrung des Zugangs zurück. **[Abänd. 82]**

~~Artikel 5~~

~~Meldungen~~

~~(1) Die zuständige Behörde oder die zuständige Einrichtung der Union kann eine Meldung an einen Hostingdiensteanbieter richten.~~

~~(2) Die Hostingdiensteanbieter richten betriebliche und technische Maßnahmen ein, die eine rasche Beurteilung von Inhalten erleichtern, die von den zuständigen Behörden und gegebenenfalls den zuständigen Einrichtungen der Union zur freiwilligen Prüfung übermittelt wurden.~~

~~(3) Die Meldung wird an die Hauptniederlassung des Hostingdiensteanbieters oder an den vom Diensteanbieter nach Artikel 16 benannten gesetzlichen Vertreter gerichtet und der in Artikel 14 Absatz 1 genannten Kontaktstelle übermittelt. Diese Meldungen werden auf elektronischem Weg versandt.~~

~~(4) Die Meldung enthält ausreichend detaillierte Informationen, einschließlich der Gründe, warum der Inhalt als terroristischer Inhalt erachtet wird, eine URL und gegebenenfalls weitere Angaben, die die Identifizierung der gemeldeten terroristischen Inhalte ermöglichen.~~

~~(5) Der Hostingdiensteanbieter prüft vorrangig den gemeldeten Inhalt auf dessen Vereinbarkeit mit seinen eigenen Nutzungsbedingungen und entscheidet, ob der Inhalt entfernt oder gesperrt wird.~~

~~(6) Der Hostingdiensteanbieter unterrichtet die zuständige Behörde oder die zuständige Einrichtung der Union unverzüglich über das Ergebnis der Prüfung und den Zeitpunkt etwaiger aufgrund der Meldung ergriffener Maßnahmen.~~

~~(7) Ist der Hostingdiensteanbieter der Auffassung, dass die Meldung nicht genügend Informationen enthält, um die gemeldeten Inhalte prüfen zu können, so teilt er dies unverzüglich den zuständigen Behörden oder der zuständigen Einrichtung der Union mit und gibt an, welche weiteren Informationen oder Klarstellungen benötigt werden.~~ **[Abänd. 83]**

Artikel 6

~~Proaktive~~ ***Spezifische*** Maßnahmen

(1) ~~Die Hostingdiensteanbieter ergreifen gegebenenfalls proaktive~~ ***Unbeschadet der Richtlinie (EU) 2018/1808 und der Richtlinie 2000/31/EG können die Hostingdiensteanbieter spezifische*** Maßnahmen ***ergreifen***, um ihre Dienste vor der ***öffentlichen*** Verbreitung terroristischer Inhalte zu schützen. Die Maßnahmen müssen wirksam***, gezielt*** und verhältnismäßig sein, wobei dem Risiko und Ausmaß der möglichen Beeinflussung durch terroristische Inhalte, den Grundrechten der Nutzer sowie der grundlegenden Bedeutung ~~der Meinungs- und Informationsfreiheit~~ ***des Rechts auf freie Meinungsäußerung und der Freiheit, Informationen und Ideen*** in einer offenen und demokratischen Gesellschaft ***zu erhalten und weiterzugeben, in besonderem Maße*** Rechnung zu tragen ist. **[Abänd. 85]**

(2) Im Fall einer Unterrichtung nach Artikel 4 Absatz 9 fordert die in Artikel 17 Absatz 1 Buchstabe c genannte zuständige Behörde den Hostingdiensteanbieter auf, innerhalb von drei Monaten nach Eingang der Aufforderung und danach mindestens einmal jährlich einen Bericht über die von ihm ergriffenen spezifischen proaktiven Maßnahmen, einschließlich der Verwendung automatisierter Werkzeuge, vorzulegen, um

a) ein erneutes Hochladen von Inhalten, die zuvor entfernt oder gesperrt wurden, weil sie als terroristische Inhalte erachtet werden, zu verhindern;

b) terroristische Inhalte zu erkennen, zu ermitteln und unverzüglich zu entfernen oder zu sperren.

Diese Aufforderung wird an die Hauptniederlassung des Hostingdiensteanbieters oder an den vom Diensteanbieter benannten gesetzlichen Vertreter gerichtet.

~~Die Berichte müssen alle relevanten Angaben enthalten, die es der zuständigen Behörde nach Artikel 17 Absatz 1 Buchstabe c ermöglichen zu prüfen, ob die proaktiven Maßnahmen wirksam und verhältnismäßig sind; dies schließt auch eine Bewertung des Funktionierens gegebenenfalls verwendeter automatisierter Werkzeuge und Mechanismen der Aufsicht und Überprüfung durch Menschen ein.~~ **[Abänd. 86]**

~~(3) Ist die zuständige Behörde nach Artikel 17 Absatz 1 Buchstabe c der Auffassung, dass die ergriffenen und nach Absatz 2 gemeldeten proaktiven Maßnahmen nicht ausreichen, um das Risiko und das Ausmaß der möglichen Beeinflussung zu mindern und zu steuern, kann sie den Hostingdiensteanbieter auffordern, zusätzliche spezifische proaktive Maßnahmen zu ergreifen. Zu diesem Zweck arbeitet der Hostingdiensteanbieter mit der zuständigen Behörde nach Artikel 17 Absatz 1 Buchstabe c zusammen, um die von ihm zu ergreifenden spezifischen Maßnahmen zu ermitteln und Kernziele und Benchmarks sowie die Fristen für deren Umsetzung festzulegen.~~ **[Abänd. 87]**

(4) ~~Kann innerhalb der drei Monate nach der Aufforderung keine Einigung im Sinne von Absatz 3 erzielt werden~~ ***Nach der Feststellung, dass an einen Hostingdiensteanbieter Entfernungsanordnungen in großer Zahl ergangen sind***, ~~so~~ kann die zuständige Behörde nach Artikel 17 Absatz 1 Buchstabe c ~~eine Entscheidung erlassen, mit der~~ ***dem Hostingdiensteanbieter eine Aufforderung übermitteln***, ***notwendige, verhältnismäßige und wirksame zusätzliche*** spezifische ~~zusätzliche, notwendige und verhältnismäßige proaktive~~ Maßnahmen ~~auferlegt werden~~ ***zu ergreifen. Die zuständige Behörde erlegt weder eine allgemeine Überwachungspflicht noch die Verwendung automatischer Werkzeuge auf***. In der ~~Entscheidung~~ ***Aufforderung*** werden insbesondere die ***technische Umsetzbarkeit der Maßnahmen, die Größe und die*** wirtschaftliche Leistungsfähigkeit des Hostingdiensteanbieters und die Auswirkungen dieser Maßnahmen auf die Grundrechte der Nutzer und die grundlegende Bedeutung der ~~Meinungs- und Informationsfreiheit~~ ***Meinungsfreiheit und der Freiheit, Informationen und Ideen in einer offenen und demokratischen Gesellschaft zu erhalten und weiterzugeben,*** berücksichtigt. Diese ~~Entscheidung~~ ***Aufforderung*** wird an die Hauptniederlassung des Hostingdiensteanbieters oder an den von ihm benannten gesetzlichen Vertreter gerichtet. Der Hostingdiensteanbieter erstattet regelmäßig Bericht über die Durchführung der von der zuständigen Behörde nach Artikel 17 Absatz 1 Buchstabe c festgelegten Maßnahmen. **[Abänd. 88]**

(5) Ein Hostingdiensteanbieter kann die zuständige Behörde nach Artikel 17 Absatz 1 Buchstabe c jederzeit ersuchen, eine Aufforderung ~~oder Entscheidung~~ nach ~~den Absätzen 2, 3 bzw.~~ ***Absatz*** 4 zu überprüfen ~~oder~~ ***und*** gegebenenfalls zu widerrufen. Die zuständige Behörde trifft innerhalb einer angemessenen Frist nach Eingang des Ersuchens des Hostingdiensteanbieters eine mit Gründen versehene Entscheidung. **[Abänd. 89]**

Artikel 7

Aufbewahrung von Inhalten und zugehörigen Daten

(1) Die Hostingdiensteanbieter bewahren terroristische Inhalte, die infolge einer Entfernungsanordnung~~, einer Meldung~~ oder ~~proaktiver~~ ***spezifischer*** Maßnahmen nach den Artikeln 4, 5 und 6 entfernt oder gesperrt wurden, sowie zugehörige Daten, die infolge der Entfernung der terroristischen Inhalte entfernt wurden, zu folgenden Zwecken auf: **[Abänd. 90]**

a) Verfahren der behördlichen oder gerichtlichen Überprüfung ***oder des verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs***, **[Abänd. 91]**

b) Verhinderung, Erkennung, Untersuchung und Verfolgung von terroristischen Straftaten ***durch Strafverfolgungsbehörden***. **[Abänd. 92]**

(2) Die terroristischen Inhalte und zugehörigen Daten nach Absatz 1 ***Buchstabe a*** werden für einen Zeitraum von sechs Monaten aufbewahrt ***und anschließend gelöscht***. Auf Anordnung der zuständigen Behörde oder des zuständigen Gerichts werden die terroristischen Inhalte ***nur dann*** für einen ~~längeren~~ ***weiteren festgelegten*** Zeitraum aufbewahrt, wenn und solange dies für laufende Verfahren der behördlichen oder gerichtlichen Überprüfung ***oder verwaltungsrechtlicher oder gerichtlicher Rechtsbehelfe*** nach Absatz 1 Buchstabe a erforderlich ist. ***Die Hostingdiensteanbieter bewahren die terroristischen Inhalte und zugehörigen Daten nach Absatz 1 Buchstabe b auf, bis die Strafverfolgungsbehörde auf die Unterrichtung durch den Hostingdiensteanbieter gemäß Artikel 13 Absatz 4 reagiert, jedoch höchstens sechs Monate.*** **[Abänd. 93]**

(3) Die Hostingdiensteanbieter stellen sicher, dass die nach den Absätzen 1 und 2 aufbewahrten terroristischen Inhalte und zugehörigen Daten angemessenen technischen und organisatorischen Schutzvorkehrungen unterliegen.

Durch diese technischen und organisatorischen Schutzvorkehrungen wird sichergestellt, dass die aufbewahrten terroristischen Inhalte und zugehörigen Daten nur für die in Absatz 1 genannten Zwecke eingesehen und verarbeitet werden und ein hohes Maß an Sicherheit der betreffenden personenbezogenen Daten gewährleistet ist. Die Hostingdiensteanbieter überprüfen und aktualisieren diese Schutzvorkehrungen bei Bedarf.

ABSCHNITT III

SCHUTZVORKEHRUNGEN UND RECHENSCHAFTSPFLICHT

Artikel 8

Transparenzanforderungen ***an Hostingdiensteanbieter*** **[Abänd. 94]**

(1) ~~Die Hostingdiensteanbieter~~ ***Gegebenenfalls*** legen ***die Hostingdiensteanbieter*** in ihren Nutzungsbedingungen ***eindeutig*** ihre Strategie zur Verhinderung der Verbreitung terroristischer Inhalte dar, gegebenenfalls mit einer aussagekräftigen Erläuterung der Funktionsweise ~~proaktiver~~ ***spezifischer*** Maßnahmen~~, einschließlich der Verwendung automatisierter Werkzeuge~~. **[Abänd. 95]**

(2) ~~Die Hostingdiensteanbieter veröffentlichen~~ ***Hostingdiensteanbieter, die in dem betreffenden Jahr von einer Entfernungsanordnung betroffen sind oder waren, stellen*** jährliche Transparenzberichte über die gegen die Verbreitung terroristischer Inhalte ergriffenen Maßnahmen ***öffentlich zur Verfügung***. **[Abänd. 96]**

(3) Die Transparenzberichte enthalten mindestens folgende Angaben:

a) Informationen über die Maßnahmen des Hostingdiensteanbieters im Zusammenhang mit der Erkennung, Ermittlung und Entfernung terroristischer Inhalte;

b) Informationen über die Maßnahmen des Hostingdiensteanbieters zur Verhinderung eines erneuten Hochladens von Inhalten, die zuvor entfernt oder gesperrt wurden, weil sie als terroristische Inhalte erachtet werden***,*** ***insbesondere wenn automatisierte Technologie verwendet wurde***; **[Abänd. 97]**

c) Anzahl der nach Entfernungsanordnungen~~, Meldungen~~ oder ~~proaktiven~~ ***spezifischen*** Maßnahmen entfernten oder gesperrten Elemente mit terroristischem Inhalt ***und Anzahl der Fälle, in denen der Inhalt nach Anordnungen in Übereinstimmung mit Artikel 4 Absätze 7 und 8 nicht entfernt wurde, einschließlich der Gründe für die Ablehnung***; **[Abänd. 98]**

d) ~~Übersicht über~~ ***Anzahl und Ergebnis der*** Beschwerdeverfahren und ~~deren Ergebnis~~ ***Maßnahmen der gerichtlichen Überprüfung, einschließlich der Anzahl der Fälle, in denen Inhalte fälschlicherweise als terroristische Inhalte identifiziert wurden***. **[Abänd. 99]**

Artikel 8a

Transparenzanforderungen an die zuständigen Behörden

(1) Die zuständigen Behörden veröffentlichen jährliche Transparenzberichte, die mindestens folgende Angaben enthalten:

a) Anzahl der ausgestellten Entfernungsanordnungen und Anzahl der abgelehnten oder nicht beachteten Entfernungsanordnungen;

b) Anzahl der Fälle, in denen terroristische Inhalte erkannt wurden, die Untersuchungen und eine Strafverfolgung nach sich zogen, und die Anzahl der Fälle, in denen Inhalte fälschlicherweise als terroristische Inhalte identifiziert wurden;

c) eine Beschreibung der von der zuständigen Behörde gemäß Artikel 6 Absatz 4 geforderten Maßnahmen. **[Abänd. 100]**

Artikel 9

Schutzvorkehrungen in Bezug auf die Anwendung und Durchführung ~~proaktiver~~ ***spezifischer*** Maßnahmen **[Abänd. 101]**

(1) Verwenden Hostingdiensteanbieter ~~nach dieser Verordnung~~ automatisierte Werkzeuge für die von ihnen gespeicherten Inhalte, so treffen sie wirksame und geeignete Schutzvorkehrungen, um sicherzustellen, dass Entscheidungen, die diese Inhalte betreffen, insbesondere Entscheidungen zur Entfernung oder Sperrung ~~von~~ ***des Zugangs zu*** Inhalten, die als terroristische Inhalte erachtet werden, zutreffend und fundiert sind. **[Abänd. 102]**

(2) Die Schutzvorkehrungen bestehen~~, soweit angemessen,~~ insbesondere in ~~einer~~ ***der*** Aufsicht und Überprüfung ~~durch Menschen, aber in jedem Fall immer dann, wenn eine eingehende Beurteilung des betreffenden Kontexts erforderlich ist, um feststellen zu können, ob ein Inhalt als terroristischer Inhalt zu erachten ist~~ ***der Angemessenheit der Entscheidung***, ***Inhalte zu entfernen oder den Zugang zu ihnen zu sperren, durch Menschen***, ***wobei insbesondere das Recht auf freie Meinungsäußerung und die Freiheit***, ***Informationen und Ideen in einer offenen und demokratischen Gesellschaft zu erhalten und weiterzugeben, zu berücksichtigen sind***. **[Abänd. 103]**

Artikel 9a

Wirksame Rechtsbehelfe

(1) Inhalteanbieter, deren Inhalte infolge einer Entfernungsanordnung entfernt oder gesperrt wurden, und Hostingdiensteanbieter, die eine Entfernungsanordnung erhalten haben, haben ein Recht auf einen wirksamen Rechtsbehelf. Die Mitgliedstaaten schaffen wirksame Verfahren für die Ausübung dieses Rechts.
[Abänd. 104]

Artikel 10

Beschwerdemechanismen

(1) Die Hostingdiensteanbieter richten ~~wirksame~~ ***einen wirksamen*** und ~~zugängliche Mechanismen~~ ***zugänglichen Mechanismus*** ein, ~~die~~ ***der*** Inhalteanbietern, deren Inhalte aufgrund ~~einer Entfernungsanordnung nach Artikel 5 oder proaktiver~~ ***spezifischer*** Maßnahmen nach Artikel 6 entfernt oder gesperrt wurden, die Möglichkeit ~~geben~~ ***gibt***, Beschwerde gegen die Maßnahme des Hostingdiensteanbieters einzulegen und die Reaktivierung des Inhalts zu verlangen.
[Abänd. 105]

(2) Die Hostingdiensteanbieter prüfen umgehend jede eingehende Beschwerde und reaktivieren den Inhalt unverzüglich, wenn dessen Entfernung oder Sperrung nicht gerechtfertigt war. Sie setzen den Beschwerdeführer ~~über das~~ ***innerhalb von zwei Wochen nach Eingang der Beschwerde von dem*** Ergebnis der Prüfung in Kenntnis ***und fügen eine Erklärung bei, falls der Hostingdiensteanbieter beschließt, den Inhalt nicht wiederherzustellen. Eine Wiederherstellung der Inhalte steht weiteren gerichtlichen Maßnahmen gegen die Entscheidung des Hostingdiensteanbieters oder der zuständigen Behörde nicht entgegen***. **[Abänd. 106]**

Artikel 11

Unterrichtung der Inhalteanbieter

(1) Entfernen oder sperren Hostingdiensteanbieter terroristische Inhalte, so stellen sie dem Inhalteanbieter ***umfassende und präzise*** Informationen über die Entfernung oder Sperrung der terroristischen Inhalte ***und über die Möglichkeiten, die Entscheidung anzufechten,*** zur Verfügung ***und übermitteln ihm auf Verlangen eine Kopie der nach Artikel 4 ausgestellten Entfernungsanordnung***. **[Abänd. 107]**

~~(2) Auf Anfrage des Inhalteanbieters teilt der Hostingdiensteanbieter dem Inhalteanbieter die Gründe für die Entfernung oder Sperrung sowie die Möglichkeiten zur Anfechtung der Entscheidung mit.~~ **[Abänd. 108]**

(3) Die Verpflichtung nach ~~den Absätzen~~ ***Absatz*** 1 ~~und 2~~ gilt nicht, wenn die zuständige Behörde ***auf der Grundlage objektiver Beweise und unter Berücksichtigung der Verhältnismäßigkeit und Notwendigkeit einer solchen Entscheidung*** entscheidet, dass aus Gründen der öffentlichen Sicherheit wie der Verhinderung, Untersuchung, Erkennung und Verfolgung terroristischer Straftaten so lange wie erforderlich, längstens jedoch ~~[vier]~~ ***vier*** Wochen ab dieser Entscheidung, keine Informationen weitergegeben ***werden*** dürfen. In diesem Fall gibt der Hostingdiensteanbieter keine Informationen über die Entfernung oder Sperrung terroristischer Inhalte weiter. **[Abänd. 109]**

ABSCHNITT IV

Zusammenarbeit zwischen zuständigen Behörden, Einrichtungen der Union und Hostingdiensteanbietern

Artikel 12

Kapazitäten der zuständigen Behörden

Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden über die nötigen Kapazitäten und ausreichende Mittel verfügen, um die Ziele dieser Verordnung zu erreichen und ihren sich daraus ergebenden Verpflichtungen nachkommen zu können***, wobei ihre Unabhängigkeit umfassend gewährleistet ist***. **[Abänd. 110]**

Artikel 13

Zusammenarbeit zwischen Hostingdiensteanbietern, zuständigen Behörden und gegebenenfalls zuständigen Einrichtungen der Union

(1) In Bezug auf Entfernungsanordnungen ~~und Meldungen~~ unterrichten die zuständigen Behörden der Mitgliedstaaten ~~und gegebenenfalls die zuständigen Einrichtungen der Union wie~~ ***einander, stimmen sich ab und arbeiten zusammen und unterrichten gegebenenfalls*** Europol ***bzw.*** ~~einander,~~ stimmen sich ***mit Europol*** ab und arbeiten ***mit Europol*** zusammen, um Doppelarbeit zu vermeiden, die Koordinierung zu ~~verstärken~~ ***verbessern*** und Überschneidungen ~~mit~~ ***von*** Untersuchungen in verschiedenen Mitgliedstaaten zu vermeiden. **[Abänd. 112]**

(2) In Bezug auf Maßnahmen nach Artikel 6 und Durchsetzungsmaßnahmen nach Artikel 18 unterrichten die zuständigen Behörden der Mitgliedstaaten die zuständige Behörde nach Artikel 17 Absatz 1 Buchstaben c und d, stimmen sich mit ihr ab und arbeiten mit ihr zusammen. Die Mitgliedstaaten stellen sicher, dass die zuständige Behörde nach Artikel 17 Absatz 1 Buchstaben c und d im Besitz aller einschlägigen Informationen ist. Zu diesem Zweck sehen die Mitgliedstaaten geeignete ***und sichere*** Kommunikationskanäle oder Mechanismen vor, um sicherzustellen, dass die relevanten Informationen rechtzeitig übermittelt werden. **[Abänd. 113]**

(3) Die Mitgliedstaaten ~~und Hostingdiensteanbieter~~ können ~~sich für die Verwendung spezieller~~ ***spezielle*** Werkzeuge ~~entscheiden, gegebenenfalls auch~~ ***einschließlich*** der von ~~den zuständigen Einrichtungen der Union wie~~ Europol eingeführten Werkzeuge ***nutzen***, um insbesondere Folgendes zu erleichtern: **[Abänd. 114]**

a) die Bearbeitung von Entfernungsanordnungen nach Artikel 4 und diesbezügliche Rückmeldungen;

~~b) die Bearbeitung von Meldungen nach Artikel 5 und diesbezügliche Rückmeldungen;~~ **[Abänd. 115]**

c) die Zusammenarbeit zur Ermittlung und Durchführung ~~proaktiver~~ ***spezifischer*** Maßnahmen nach Artikel 6. **[Abänd. 116]**

(4) ~~Verfügen~~ ***Werden*** Hostingdiensteanbieter ~~über Nachweise für terroristische Straftaten~~ ***terroristischer Inhalte gewahr***, so unterrichten sie unverzüglich die für die Untersuchung und Verfolgung von Straftaten in dem betreffenden Mitgliedstaat zuständigen Behörden***. Kann der betreffende Mitgliedstaat nicht ausgemacht werden, benachrichtigt der Hostingdiensteanbieter*** ~~oder~~ die Kontaktstelle nach Artikel ~~14~~ ***17*** Absatz 2 in dem Mitgliedstaat, in dem ~~sie ihre~~ ***er seine*** Hauptniederlassung ~~haben~~ ***hat*** oder über einen gesetzlichen Vertreter ~~verfügen. Im Zweifelsfall können die Hostingdiensteanbieter~~ ***verfügt, und übermittelt*** diese Informationen ***auch*** an Europol zur weiteren Bearbeitung ~~übermitteln~~. **[Abänd. 117]**

(4a) Die Hostingdiensteanbieter arbeiten mit den zuständigen Behörden zusammen. **[Abänd. 118]**

Artikel 14

Kontaktstellen

(1) ~~Die~~ Hostingdiensteanbieter***, die zuvor eine oder mehrere Entfernungsanordnungen erhalten haben,*** richten eine Kontaktstelle ein, die den Erhalt von Entfernungsanordnungen ~~und Meldungen~~ auf elektronischem Weg ermöglicht und ~~deren zügige~~ ***eine rasche*** Bearbeitung nach ~~den Artikeln~~ ***Artikel*** 4 ~~und 5~~ sicherstellt. Sie sorgen dafür, dass diese Informationen öffentlich zugänglich gemacht werden. **[Abänd. 119]**

(2) In den Informationen nach Absatz 1 sind die Amtssprachen der Union gemäß der Verordnung Nr. 1/58 anzugeben, in denen ~~die~~ ***eine Kontaktaufnahme mit der*** Kontaktstelle ~~angeschrieben werden kann~~ ***möglich ist*** und in denen der weitere Austausch im Zusammenhang mit Entfernungsanordnungen ~~und Meldungen~~ nach ~~den~~ ~~Artikeln~~ ***Artikel*** 4 ~~und 5~~ stattfindet. ~~Zu ihnen~~ ***Hierzu*** gehört mindestens eine der Amtssprachen des Mitgliedstaats, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder sein gesetzlicher Vertreter nach Artikel 16 ansässig oder niedergelassen ist. **[Abänd. 120]**

~~(3) Die Mitgliedstaaten richten eine Kontaktstelle für die Behandlung von Ersuchen um Klarstellung und Rückmeldungen im Zusammenhang mit den von ihnen ausgestellten Entfernungsanordnungen und Meldungen ein. Informationen über die Kontaktstelle werden öffentlich zugänglich gemacht.~~ **[Abänd. 121]**

ABSCHNITT V

ANWENDUNG UND DURCHSETZUNG

Artikel 15

Gerichtsbarkeit

(1) Die Gerichtsbarkeit für die Zwecke der Artikel 6, 18 und 21 liegt bei dem Mitgliedstaat, in dem sich die Hauptniederlassung des Hostingdiensteanbieters befindet. Hostingdiensteanbieter, deren Hauptniederlassung sich nicht in einem der Mitgliedstaaten befindet, gelten als der Gerichtsbarkeit des Mitgliedstaats unterworfen, in dem der gesetzliche Vertreter nach Artikel 16 ansässig oder niedergelassen ist.

(2) Hat ein Hostingdiensteanbieter***, dessen Hauptniederlassung sich nicht in einem der Mitgliedstaaten befindet,*** keinen gesetzlichen Vertreter benannt, so liegt die Gerichtsbarkeit bei allen Mitgliedstaaten. ***Entscheidet ein Mitgliedstaat, diese Gerichtsbarkeit auszuüben, so setzt er alle anderen Mitgliedstaaten hiervon in Kenntnis.*** **[Abänd. 122]**

~~(3) Hat die Behörde eines anderen Mitgliedstaats eine Entfernungsanordnung nach Artikel 4 Absatz 1 ausgestellt, so hat dieser Mitgliedstaat die Gerichtsbarkeit über Zwangsmaßnahmen nach nationalem Recht, um die Entfernungsanordnung durchzusetzen.~~ **[Abänd. 123]**

Artikel 16

Gesetzlicher Vertreter

(1) Hostingdiensteanbieter, die keine Niederlassung in der Union haben, aber Dienstleistungen in der Union anbieten, benennen schriftlich eine juristische oder natürliche Person ~~zu ihrem~~ ***als ihren*** gesetzlichen Vertreter in der Union***, der*** für die Entgegennahme, Einhaltung und Durchsetzung von Entfernungsanordnungen~~,~~ ~~Meldungen, Anträgen und Entscheidungen~~ ***und Aufforderungen zuständig ist***, die von den zuständigen Behörden auf Grundlage dieser Verordnung ausgestellt werden. Der gesetzliche Vertreter muss in einem der Mitgliedstaaten, in denen der Hostingdiensteanbieter die Dienste anbietet, ansässig oder niedergelassen sein. **[Abänd. 124]**

(2) Der Hostingdiensteanbieter betraut den gesetzlichen Vertreter mit der Entgegennahme, Einhaltung und Durchsetzung der Entfernungsanordnungen~~,~~ ~~Meldungen, Anträge~~ und ~~Entscheidungen~~ ***Aufforderungen*** nach Absatz 1 im Namen des betreffenden Hostingdiensteanbieters. Die Hostingdiensteanbieter statten ihren gesetzlichen Vertreter mit den notwendigen Befugnissen und Ressourcen aus, damit dieser mit den zuständigen Behörden zusammenarbeiten und den betreffenden Entscheidungen und Anordnungen nachkommen kann. **[Abänd. 125]**

(3) Der benannte gesetzliche Vertreter kann für Verstöße gegen Pflichten aus dieser Verordnung haftbar gemacht werden; die Haftung und die rechtlichen Schritte, die gegen den Hostingdiensteanbieter eingeleitet werden können, bleiben hiervon unberührt.

(4) Der Hostingdiensteanbieter setzt die zuständige Behörde nach Artikel 17 Absatz 1 Buchstabe d in dem Mitgliedstaat, in dem der gesetzliche Vertreter ansässig oder niedergelassen ist, über die Benennung in Kenntnis. Informationen über den gesetzlichen Vertreter werden öffentlich zugänglich gemacht.

ABSCHNITT VI

SCHLUSSBESTIMMUNGEN

Artikel 17

Benennung der zuständigen Behörden

(1) Jeder Mitgliedstaat benennt ~~die Behörde~~ ***eine Justizbehörde*** oder ~~die Behörden~~ ***eine funktional unabhängige Verwaltungsbehörde***, die dafür zuständig ~~sind~~ ***ist***, **[Abänd. 126]**

a) Entfernungsanordnungen nach Artikel 4 auszustellen;

~~b) terroristische Inhalte zu erkennen, zu ermitteln und den Hostingdiensteanbietern nach Artikel 5 zu melden;~~ **[Abänd. 127]**

c) die Durchführung ~~proaktiver~~ ***spezifischer*** Maßnahmen nach Artikel 6 zu überwachen; **[Abänd. 128]**

d) die Verpflichtungen aus dieser Verordnung mittels Sanktionen nach Artikel 18 durchzusetzen.

(1a) ***Die Mitgliedstaaten benennen eine bei der zuständigen Behörde angesiedelte Kontaktstelle für die Bearbeitung von Ersuchen um Klarstellung und Rückmeldungen im Zusammenhang mit den von ihnen ausgestellten Entfernungsanordnungen. Angaben zur Kontaktstelle werden öffentlich zugänglich gemacht.*** **[Abänd. 129]**

(2) Die Mitgliedstaaten ~~teilen~~ ***melden*** der Kommission die in Absatz 1 genannten zuständigen Behörden bis zum [sechs Monate nach Inkrafttreten dieser Verordnung] ~~mit~~. ***Die Kommission erstellt ein Online-Register, in dem alle zuständigen Behörden mit ihrer jeweiligen Kontaktstelle aufgeführt sind.*** Die Kommission veröffentlicht die Mitteilung und eventuelle Änderungen derselben im Amtsblatt der Europäischen Union. **[Abänd. 130]**

Artikel 18

Sanktionen

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei ***systematischen und ständigen*** Verstößen der Hostingdiensteanbieter gegen die Verpflichtungen ~~aus~~ ***gemäß*** dieser Verordnung zu verhängen sind, und treffen alle ~~für die Anwendung der~~ ***erforderlichen Maßnahmen, um sicherzustellen, dass die*** Sanktionen ~~erforderlichen Maßnahmen~~ ***angewandt werden***. Diese Sanktionen beschränken sich auf Verstöße gegen die Verpflichtungen aus **[Abänd. 131]**

~~a) Artikel 3 Absatz 2 (Nutzungsbedingungen von Hostingdiensteanbietern);~~ **[Abänd. 132]**

b) Artikel 4 Absätze 2 und 6 (Ausführung von Entfernungsanordnungen und diesbezügliche Rückmeldungen);

~~c) Artikel 5 Absätze 5 und 6 (Prüfung von Meldungen und diesbezügliche Rückmeldungen);~~ **[Abänd. 133]**

d) Artikel 6 ~~Absätze~~ ***Absatz*** ~~2 und~~ 4 (Berichte über ~~proaktive~~ ***spezifische*** Maßnahmen und ***die*** Ergreifung von Maßnahmen aufgrund einer ~~Entscheidung zur Auferlegung spezifischer proaktiver~~ ***Aufforderung, durch die zusätzliche spezifische*** Maßnahmen ***auferlegt wurden***); **[Abänd. 134]**

e) Artikel 7 (Aufbewahrung von Daten);

f) Artikel 8 (~~Transparenz~~ ***Transparenzanforderungen an Hostingdiensteanbieter***); **[Abänd. 135]**

g) Artikel 9 (Schutzvorkehrungen in Bezug auf ~~proaktive~~ ***die Anwendung und Durchführung spezifischer*** Maßnahmen); **[Abänd. 136]**

h) Artikel 10 (Beschwerdeverfahren);

i) Artikel 11 (Unterrichtung der Inhalteanbieter);

j) Artikel 13 Absatz 4 (Informationen über ~~Nachweise für~~ terroristische ~~Straftaten~~ ***Inhalte***); **[Abänd. 137]**

k) Artikel 14 Absatz 1 (Kontaktstellen);

l) Artikel 16 (Benennung eines gesetzlichen Vertreters).

(2) Die Sanktionen ***gemäß Absatz 1*** müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen spätestens bis [sechs Monate nach Inkrafttreten dieser Verordnung] mit und melden ihr unverzüglich alle diesbezüglichen Änderungen. **[Abänd. 138]**

(3) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Festlegung von Art und Höhe der Sanktionen alle relevanten Umstände berücksichtigen, darunter

a) Art, Schwere und Dauer des Verstoßes;

b) die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde;

c) frühere Verstöße der haftbaren juristischen Person;

d) die Finanzkraft der haftbaren juristischen Person;

e) die Bereitschaft des Hostingdiensteanbieters, mit den zuständigen Behörden zusammenzuarbeiten~~.~~***;*** **[Abänd. 139]**

(ea) die Art und Größe des Hostingdiensteanbieters, insbesondere bei Kleinst- und Kleinunternehmen im Sinne der Empfehlung 2003/361/EG[13] der Kommission. **[Abänd. 140]**

(4) Die Mitgliedstaaten stellen sicher, dass bei einem systematischen ***und ständigen*** Verstoß gegen die Verpflichtungen aus Artikel 4 Absatz 2 finanzielle Sanktionen in Höhe von bis zu 4 % des ~~weltweiten Jahresumsatzes des Hostingdiensteanbieters~~ ***vom Hostingdiensteanbieter*** im vorangegangenen Geschäftsjahr ***erwirtschafteten weltweiten Jahresumsatzes*** verhängt werden. **[Abänd. 141]**

Artikel 19

Technische Anforderungen***, Kriterien für die Bewertung der Signifikanz*** und Änderungen der Formulare für Entfernungsanordnungen **[Abänd. 142]**

(1) Der Kommission wird die Befugnis übertragen, ~~nach~~ ***gemäß*** Artikel 20 delegierte Rechtsakte zu erlassen, um diese Verordnung durch ***notwendige*** technische Anforderungen an die von den zuständigen Behörden für die Übermittlung von Entfernungsanordnungen zu verwendenden elektronischen Mittel zu ergänzen. **[Abänd. 143]**

---

13 Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

(1a) Der Kommission wird die Befugnis übertragen, gemäß Artikel 20 delegierte Rechtsakte zu erlassen, um diese Verordnung durch Kriterien und Zahlen zu ergänzen, anhand derer die zuständigen Behörden festlegen, was unter einer großen Zahl unbestrittener Entfernungsanordnungen im Sinne dieser Verordnung zu verstehen ist. **[Abänd. 144]**

(2) Der Kommission wird die Befugnis übertragen, solche delegierten Rechtsakte zur Änderung der Anhänge I, II und III zu erlassen, um einem etwaigen Verbesserungsbedarf hinsichtlich des Inhalts der Entfernungsanordnungsformulare sowie der Formulare für die Übermittlung von Informationen über die Unmöglichkeit der Ausführung der Entfernungsanordnung wirksam zu entsprechen.

Artikel 20

Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte nach Artikel 19 wird der Kommission auf unbestimmte Zeit ab dem [Datum des Anwendungsbeginns dieser Verordnung] übertragen.

(3) Die Befugnisübertragung nach Artikel 19 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Der Beschluss tritt am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem späteren, in dem Beschluss festgelegten Zeitpunkt in Kraft. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung über bessere Rechtsetzung vom 13. April 2016 festgelegten Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der nach Artikel 19 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 21
Monitoring

(1) Die Mitgliedstaaten erheben von ihren zuständigen Behörden und den ihrer Gerichtsbarkeit unterstehenden Hostingdiensteanbietern Informationen über die Maßnahmen, die von diesen aufgrund dieser Verordnung ergriffen wurden, und übermitteln sie der Kommission spätestens bis zum [31. März] jeden Jahres. Diese Informationen umfassen:

a) Informationen über die Anzahl der ausgestellten Entfernungsanordnungen ~~und Meldungen~~ nach Artikel 4 ~~und Artikel 5~~, die Anzahl der entfernten oder gesperrten Elemente mit terroristischem Inhalt, einschließlich der zugehörigen Fristen ***nach Artikel 4, sowie Informationen über die Anzahl der entsprechenden Fälle erfolgreicher Aufdeckung, Ermittlung und Verfolgung terroristischer Straftaten***; **[Abänd. 145]**

b) Informationen über die spezifischen proaktiven Maßnahmen nach Artikel 6, einschließlich des Umfangs der entfernten oder gesperrten terroristischen Inhalte und der zugehörigen Fristen;

ba) Informationen über die Anzahl der von den zuständigen Behörden angeforderten Zugriffe auf von Hostingdiensteanbietern nach Artikel 7 aufbewahrte Inhalte; **[Abänd. 146]**

c) Informationen über die Anzahl der eingeleiteten Beschwerdeverfahren und der von Hostingdiensteanbietern unternommenen Maßnahmen nach Artikel 10;

d) Informationen über die Anzahl der eingeleiteten Rechtsbehelfsverfahren und der von der zuständigen Behörde nach nationalem Recht erlassenen Entscheidungen.

(2) Die Kommission erstellt spätestens [ein Jahr nach Anwendungsbeginn dieser Verordnung] ein ausführliches Programm für das Monitoring der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung. In dem Monitoring-Programm werden die Indikatoren und Instrumente benannt, mit denen Daten und sonstige erforderliche Nachweise zu erfassen sind, und die Zeitabstände der Erfassung angegeben. Darin wird auch festgelegt, welche Maßnahmen die Kommission und die Mitgliedstaaten bei der Erfassung und Auswertung der Daten und sonstigen Nachweise im Hinblick auf die Überwachung der Fortschritte und die Evaluierung der Verordnung nach Artikel 23 zu ergreifen haben.

Artikel 22

Bericht über die Anwendung

Die Kommission erstattet dem Europäischen Parlament und dem Rat bis zum [zwei Jahre nach Inkrafttreten dieser Verordnung] Bericht über die Anwendung dieser Verordnung. In dem Bericht der Kommission werden Informationen über das Monitoring nach Artikel 21 und die sich aus den Transparenzanforderungen nach Artikel 8 ergebenden Informationen berücksichtigt. Die Mitgliedstaaten übermitteln der Kommission die für die Ausarbeitung des Berichts erforderlichen Informationen.

Artikel 23

Evaluierung

~~Frühestens [drei Jahre~~ ***Ein Jahr*** nach Anwendungsbeginn dieser Verordnung~~]~~ führt die Kommission eine Evaluierung dieser Verordnung durch und legt dem Europäischen Parlament und dem Rat einen Bericht über die Anwendung der Verordnung und das Funktionieren und die Wirksamkeit der Schutzvorkehrungen ***sowie über die Auswirkungen auf die Grundrechte und insbesondere auf das Recht auf freie Meinungsäußerung, die Freiheit, Informationen zu erhalten und weiterzugeben, und das Recht auf Achtung der Privatsphäre*** vor. ***Im Rahmen dieser Evaluierung erstattet die Kommission außerdem Bericht über die Notwendigkeit, Durchführbarkeit und Wirksamkeit der Einrichtung einer europäischen Plattform für terroristische Online-Inhalte, die allen Mitgliedstaaten die Verwendung eines einzigen sicheren Kommunikationskanals zur Übermittlung von Entfernungsanordnungen betreffend terroristische Inhalte an Hostingdiensteanbieter gestatten würde.*** Gegebenenfalls wird der Bericht um Legislativvorschläge ergänzt. Die Mitgliedstaaten übermitteln der Kommission die für die Ausarbeitung des Berichts erforderlichen Informationen. **[Abänd. 147]**

Artikel 24

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

Sie gilt ab dem [~~sechs~~ ***zwölf*** Monate nach ihrem Inkrafttreten]. **[Abänd. 148]**

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu ... am …

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*

ANHANG I

ENTFERNUNGSANORDNUNG FÜR TERRORISTISCHE INHALTE (Artikel 4 der Verordnung (EU) xxx)

Nach Artikel 4 der Verordnung (EU) …[1] muss der Empfänger der Entfernungsanordnung terroristische Inhalte innerhalb einer Stunde nach Erhalt dieser Anordnung von der zuständigen Behörde entfernen oder den Zugang dazu sperren.
Nach Artikel 7 der Verordnung (EU) …[2] sind die Empfänger verpflichtet, die entfernten oder gesperrten Inhalte und zugehörigen Daten für einen Zeitraum von sechs Monaten oder auf Anordnung der zuständigen Behörden oder Gerichte für einen längeren Zeitraum aufzubewahren.
Die Entfernungsanordnung ist in einer der vom Empfänger gemäß Artikel 14 Absatz 2 angegebenen Sprachen zu übermitteln.

ABSCHNITT A:
Ausstellender Mitgliedstaat:
…….
Hinweis: Angaben zur ausstellenden Behörde sind am Ende des Dokuments (Abschnitte E und F) zu machen
Empfänger (gesetzlicher Vertreter):
…….
Empfänger (Kontaktstelle):
…….
Mitgliedstaat, unter dessen Gerichtsbarkeit der Empfänger fällt [falls abweichend vom ausstellenden Staat]:
…….
Uhrzeit und Datum der Ausstellung der Entfernungsanordnung:
…….
Referenznummer der Entfernungsanordnung:
…….

[1] Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte (*ABl. L ...*).
[2] Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte (*ABl. L ...*).

ABSCHNITT B: ~~Innerhalb einer Stunde~~ ***Unverzüglich*** zu entfernender oder zu sperrender Inhalt: **[Abänd. 162]**

Eine URL und alle weiteren Informationen, die die Identifizierung und die genaue Lokalisierung der gemeldeten Inhalte ermöglichen:

……

Gründe, aus denen hervorgeht, warum der Inhalt gemäß Artikel 2 Absatz 5 der Verordnung (EU) xxx als terroristischer Inhalt anzusehen ist. Der Inhalt (Zutreffendes bitte ankreuzen):

□ ~~ruft~~ ***enthält den Aufruf*** zur Begehung ~~terroristischer Straftaten auf oder befürwortet oder verherrlicht diese~~ ***einer in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten terroristischen Straftat*** (Artikel 2 Absatz 5 Buchstabe a) **[Abänd. 149]**

□ ~~ermutigt~~ ***enthält die an eine andere Person oder Personengruppe gerichtete Aufforderung*** zur ~~Beteiligung an~~ ***Begehung einer in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten*** terroristischen ~~Straftaten~~ ***Straftat oder zur Mitwirkung daran*** (Artikel 2 Absatz 5 Buchstabe b) **[Abänd. 150]**

□ ~~fördert~~ ***enthält*** die ~~Aktivitäten einer terroristischen Vereinigung, ermutigt~~ ***an eine andere Person oder Personengruppe gerichtete Aufforderung*** zur Beteiligung an ~~oder Unterstützung~~ ***den in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten Handlungen*** einer terroristischen Vereinigung (Artikel 2 Absatz 5 Buchstabe c) **[Abänd. 151]**

□ enthält technische Anleitungen oder Methoden für ~~das Begehen terroristischer Straftaten~~ ***die Herstellung oder den Gebrauch von Sprengstoffen, Schuss- oder sonstigen Waffen oder schädlichen oder gefährlichen Stoffen beziehungsweise Unterweisungen in anderen spezifischen Methoden oder Verfahren mit dem Ziel, eine in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführte terroristische Straftat zu begehen*** (Artikel 2 Absatz 5 Buchstabe d) **[Abänd. 152]**

□ ***enthält die Darstellung der Begehung einer in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten Straftat dar (Artikel 2 Absatz 5 Buchstabe e)*** **[Abänd. 153]**

Zusätzliche Angaben zu den Gründen, aus denen der Inhalt als terroristischer Inhalt angesehen wird (fakultativ):

……

……

……

ABSCHNITT C: Unterrichtung des Inhalteanbieters

Bitte beachten Sie, dass (bitte ankreuzen, falls zutreffend):

□ der Empfänger aus Gründen der öffentlichen Sicherheit **den Inhalteanbieter**, dessen Inhalt entfernt oder gesperrt wurde, **nicht informieren darf**.

Hinweis: zu Einzelheiten über die Möglichkeiten, die Entfernungsanordnung im ausstellenden Mitgliedstaat (der dem Inhalteanbieter auf Anfrage mitgeteilt werden kann) nach nationalem Recht anzufechten siehe Abschnitt G

ABSCHNITT D: Unterrichtung des Mitgliedstaats der gerichtlichen Zuständigkeit

□ bitte ankreuzen, sofern der Staat der gerichtlichen Zuständigkeit nicht der ausstellende Mitgliedstaat ist

□ eine Kopie der Entfernungsanordnung wird der zuständigen Behörde des Staates der gerichtlichen Zuständigkeit übermittelt

ABSCHNITT E: Angaben zur Behörde, die die Entfernungsanordnung ausgestellt hat

Art der Behörde, die die Entfernungsanordnung ausgestellt hat (Zutreffendes bitte ankreuzen):

□ Richter, Gericht oder Ermittlungsrichter

□ Strafverfolgungsbehörde

□ andere zuständige Behörde → bitte auch Abschnitt F ausfüllen

Angaben zur ausstellenden Behörde und/oder zu ihrem gesetzlichen Vertreter, die/der die Genauigkeit und Richtigkeit der Entfernungsanordnung bescheinigt:

Name der Behörde:

……

Name ihres Vertreters:

……

Funktion (Titel/Amtsbezeichnung):

……

Aktenzeichen: ……

Anschrift: ……

Telefonnummer (Ländervorwahl) (Gebiets-/Ortsvorwahl):.....

Fax (Ländervorwahl) (Gebiets-/Ortsvorwahl):.....

E-Mail:……

Datum:

……

Dienststempel (falls vorhanden) und Unterschrift[3]:

……

[3] Eine Unterschrift ist nicht erforderlich, wenn die Übermittlung über authentifizierte Übertragungskanäle erfolgt.

ABSCHNITT F: Kontaktangaben für Folgemaßnahmen

Kontaktangaben der ausstellenden Behörde zum Erhalt einer Rückmeldung über den Zeitpunkt der Entfernung oder Sperrung des Zugangs oder zur Klärung weiterer Fragen:

……..…….

Kontaktangaben der Behörde des Staates, unter dessen Gerichtsbarkeit der Empfänger fällt (falls abweichend vom ausstellenden Mitgliedstaat):

……..…….

ABSCHNITT G: Information über verfügbare Rechtsbehelfe

Informationen über zuständige Stellen oder Gerichte, Fristen und Verfahren für die Anfechtung der Entfernungsanordnung***, einschließlich Formvorschriften***: **[Abänd. 154]**

Zuständige Stelle oder Gericht zur Anfechtung der Entfernungsanordnung:

……..…….

Frist für die Anfechtung der Entscheidung:

XXX Monate ab dem xxxx

Link zu den Bestimmungen der nationalen Rechtsvorschriften:

……..…….

ANHANG II

FORMULAR FÜR RÜCKMELDUNGEN NACH DER ENTFERNUNG ODER SPERRUNG TERRORISTISCHER INHALTE (Artikel 4 Absatz 5 der Verordnung (EU) xxx)

ABSCHNITT A:
Empfänger der Entfernungsanordnung:
……
Behörde, die die Entfernungsanordnung ausgestellt hat:
……
Aktenzeichen der ausstellenden Behörde:
……
Aktenzeichen des Empfängers:
……
Uhrzeit und Datum des Erhalts der Entfernungsanordnung:
……

ABSCHNITT B:
Terroristischer Inhalt/Zugang zu terroristischen Inhalten, der Gegenstand der Entfernungsanordnung war (Zutreffendes bitte ankreuzen):

- □ entfernt
- □ gesperrt

Uhrzeit und Datum der Entfernung oder der Sperrung des Zugangs:
.....

ABSCHNITT C: Angaben zum Empfänger

Name des Hostingdiensteanbieters/des gesetzlichen Vertreters:

…….

Mitgliedstaat der Hauptniederlassung oder Niederlassung des gesetzlichen Vertreters:

…….

Name der bevollmächtigten Person:

…….

Angaben zur Kontaktstelle (E-Mail):

…….

Datum:

…….

ANHANG III

Informationen über die Unmöglichkeit der Ausführung der Entfernungsanordnung (Artikel 4 Absätze 6 und 7 der Verordnung (EU) xxx)

ABSCHNITT A:
Empfänger der Entfernungsanordnung:
……
Behörde, die die Entfernungsanordnung ausgestellt hat:
……
Aktenzeichen der ausstellenden Behörde:
……
Aktenzeichen des Empfängers:
……
Uhrzeit und Datum des Erhalts der Entfernungsanordnung:
……

ABSCHNITT B: Gründe für die Unmöglichkeit der Ausführung
i) Der Entfernungsanordnung kann aus folgenden Gründen nicht oder nicht innerhalb der gesetzten Frist nachgekommen werden:

□ höhere Gewalt oder eine faktische Unmöglichkeit, die dem Empfänger oder dem Diensteanbieter nicht angelastet werden kann***, einschließlich technischer und betrieblicher Gründe*** **[Abänd. 155]**

□ die Entfernungsanordnung enthält offensichtliche Fehler

□ die Entfernungsanordnung enthält unzureichende Informationen

ii) Bitte machen Sie nähere Angaben zu den Gründen für die Unmöglichkeit der Ausführung:
……
iii) Falls die Entfernungsanordnung offensichtliche Fehler und/oder unzureichende Informationen enthält, geben Sie bitte an, um welche Fehler es sich handelt und welche weiteren Informationen oder Klarstellungen erforderlich sind:
……

ABSCHNITT H: Angaben zum Diensteanbieter/zu seinem gesetzlichen Vertreter:
Name des Diensteanbieters/des gesetzlichen Vertreters:
……
Name der bevollmächtigten Person:
……
Kontaktangaben (E-Mail):
……
Unterschrift:
……
Uhrzeit und Datum:
……