Rat der
Europäischen Union

Brüssel, den 7. Dezember 2018
(OR. en)

15336/18

Interinstitutionelles Dossier:
2018/0331(COD)

CT 198
ENFOPOL 605
JAI 1264
COTER 175
CYBER 313
TELECOM 461
FREMP 222
AUDIO 121
DROIPEN 199
CODEC 2270

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	6. Dezember 2018
Empfänger:	Delegationen
Nr. Vordok.:	14978/18 + COR 1
Nr. Komm.dok.:	12129/18 + ADD 1-3
Betr.:	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte – allgemeine Ausrichtung

Der Rat hat sich auf seiner Tagung vom 6. Dezember 2018 auf die in der Anlage enthaltene allgemeine Ausrichtung geeinigt.

Änderungen gegenüber dem Kommissionsvorschlag sind durch ***Fett- und Kursivdruck***, Streichungen durch […] gekennzeichnet.

[…]

[...] ***Entwurf*** einer

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Verhinderung der Verbreitung terroristischer Online-Inhalte

[...]

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,

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 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 freie Meinungsäußerung und die Informationsfreiheit erhöht werden.

[1] ABl. C ...vom ..., S. .

(2) Hostingdiensteanbieter, die im Internet aktiv sind, spielen in der digitalen Wirtschaft eine zentrale Rolle, indem sie Unternehmen und Bürger miteinander verbinden 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.

(3) Das Vorhandensein terroristischer Online-Inhalte hat schwerwiegende negative Folgen für die Nutzer, die Bürger und die Gesellschaft insgesamt sowie 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 mit ihrem Diensteangebot verbundenen technologischen Mittel 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 Dienste verbreitet werden, zu helfen.

(4) Die 2015 begonnenen 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 und dem sich rasch verändernden Problem gerecht zu werden. Dieser Rechtsrahmen soll auf den freiwilligen Bemühungen aufbauen, die durch die Empfehlung (EU) 2018/334[2] der Kommission verstärkt wurden, und entspricht der Forderung des Europäischen Parlaments, die Maßnahmen zur Bekämpfung illegaler und schädlicher Inhalte zu intensivieren, sowie des Europäischen Rats, die automatische Erkennung und Entfernung von zu terroristischen Handlungen anstiftenden Inhalten zu verbessern.

---

[2] 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 unberührt lassen.[3] 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. ***Diese Verordnung gilt nicht für Tätigkeiten im Zusammenhang mit der nationalen Sicherheit, die weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fallen.***

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

---

[3] 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 zum Schutz der öffentlichen Sicherheit bei und enthält gleichzeitig angemessene und solide Vorkehrungen zum Schutz der betreffenden Grundrechte. 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 einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sind, wobei der besonderen Bedeutung der Meinungs- und Informationsfreiheit ***sowie der Freiheit der Presse und der Pluralität der Medien,*** die die wesentlichen Grundlagen einer pluralistischen, demokratischen Gesellschaft und einen der grundlegenden Werte der Union darstellen, Rechnung zu tragen ist. Maßnahmen, die sich auf die Meinungs- und Informationsfreiheit auswirken, sollten in dem Sinne streng zielgerichtet sein, dass sie dazu dienen müssen, die Verbreitung terroristischer Inhalte zu verhindern, ohne dadurch das Recht auf den rechtmäßigen Erhalt und die rechtmäßige Weitergabe von Informationen zu beeinträchtigen, wobei der zentralen Rolle der Hostingdiensteanbieter, öffentliche Debatten sowie die Verbreitung und den Erhalt von Informationen, Meinungen und Ideen nach geltendem Recht zu erleichtern, zu berücksichtigen ist.

(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***, und die Möglichkeit der Hostingdiensteanbieter, Entscheidungen über die Auferlegung von proaktiven Maßnahmen oder von Sanktionen vor dem Gericht des Mitgliedstaats, in dem sie niedergelassen sind oder einen gesetzlichen Vertreter haben, anzufechten***.

(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, sollte in dieser Verordnung aufbauend auf der Definition terroristischer Straftatbestände in der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates der Begriff "terroristische Inhalte" präventiv definiert werden.[4] In Anbetracht der Notwendigkeit, besonders schädliche terroristische Online-Propaganda zu bekämpfen, sollten in der Definition Materialien [...] erfasst werden, die zur Begehung terroristischer Straftaten oder zu einem Betrag zu diesen Straftaten anstiften, diese(n) fördern oder befürworten [...] oder für die Beteiligung an Handlungen einer terroristischen Vereinigung werben. […] ***Unter die Definition fallen Inhalte, die zum Zweck der Begehung terroristischer Straftaten Anleitungen zur Herstellung oder Verwendung von Sprengstoffen, Schusswaffen oder anderen Waffen oder schädlichen oder gefährlichen Stoffen sowie CBRN-Stoffen oder zu anderen Methoden oder Verfahren, einschließlich der Auswahl von Anschlagszielen, enthalten.*** Bei solchen […] ***Materialien*** 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 Zwecke der Bildung, [...] ***Gegennarrativen*** oder der Forschung verbreitet werden, sollten angemessen geschützt werden***, wobei ein angemessenes Gleichgewicht zwischen den Grundrechten, darunter insbesondere die Meinungs- und Informationsfreiheit, und den Erfordernissen der öffentlichen Sicherheit erreicht werden muss***. ***Wenn die Veröffentlichung des verbreiteten Materials der redaktionellen Verantwortung des Inhalteanbieters unterliegt, sollte bei Entscheidungen über die Entfernung solcher Inhalte den journalistischen Standards, die in dem Unionsrecht entsprechenden Presse- und Medienvorschriften festgelegt sind, sowie dem Recht auf freie Meinungsäußerung und der Freiheit der Medien und ihrer Pluralität gemäß Artikel 11 der Charta der Grundrechte Rechnung getragen werden.*** Ferner sollte die Formulierung radikaler, polemischer oder kontroverser Ansichten zu sensiblen politischen Fragen in der öffentlichen Debatte nicht als terroristischer Inhalt betrachtet werden.

---

[4] 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).

(10) Zur Erfassung 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 ***und Materialien*** in seinem Auftrag speichern und die gespeicherten Informationen ***und Materialien*** Dritten zur Verfügung zu stellen, unabhängig davon, ob diese Tätigkeit rein technischer, automatischer und passiver Art ist. [...]***Inhalte zu speichern bedeutet, Daten im Speicher eines physischen oder virtuellen Servers aufzubewahren; dies schließt Anbieter reiner Durchleitungsdienste und andere elektronische Kommunikationsdienste in der Definition des [Europäischen Kodex für die Elektronische Kommunikation] sowie Anbieter von Cachingdiensten vom Anwendungsbereich aus, sowie andere Dienstleistungen, die auf anderen Ebenen der Internet-Infrastruktur erbracht werden, wie Register oder Registrierungsstellen, DNS (Domain-Namen-Systeme) oder verwandte Dienstleistungen, wie Zahlungsdienste oder DDoS-Schutzdienstleister (DDoS = Distributed Denial of Service). Des Weiteren muss die Information im Auftrag des Inhalteanbieters gespeichert werden; es fallen nur die Dienstleistungen in den Anwendungsbereich, deren direkter Empfänger der Inhalteanbieter ist. Ferner gilt, dass die gespeicherten Informationen Dritten bereitgestellt werden, wobei Dritte alle Nutzer bezeichnet, die nicht der Inhalteanbieter sind. Interpersonelle Kommunikationsdienste, die den direkten interpersonellen und interaktiven Informationsaustausch zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind, fallen nicht in den Anwendungsbereich.*** Beispiele für solche ***Hostingdienste***anbieter [...] sind Plattformen sozialer Medien, Videostreamingdienste, Video-, Bild- und Audio-Sharing-Dienste, File-Sharing- und andere Cloud- ***und Speicher***dienste [...]. ***Diese Verordnung gilt für die Tätigkeit, Hostingdienste anzubieten, und nicht für den Anbieter selbst oder seine Haupttätigkeit, bei der möglicherweise Hostingdienste mit anderen Dienstleistungen verbunden werden, die nicht in den Anwendungsbereich der Verordnung fallen.***

(10a) 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.

(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 der Existenz einer erheblichen Zahl von Nutzern in einem oder mehreren Mitgliedstaaten oder der Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten beurteilt 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 auf einen oder mehrere Mitgliedstaaten ausrichtet[5]. Andererseits kann die Erbringung der Dienstleistung zum Zwecke der bloßen Einhaltung des in der Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates[6] festgelegten Verbots der Diskriminierung nicht allein aus diesem Grund als Ausrichtung von Tätigkeiten auf ein bestimmtes Gebiet innerhalb der Union betrachtet werden.

---

5 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).

6 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 Verbreitung terroristischer Inhalte über ihre Dienste zu verhindern. Diese Sorgfaltspflichten sollten nicht auf eine allgemeine Überwachungspflicht 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 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 erfolgen.

(13) Das Verfahren und die Verpflichtungen, die sich nach einer Beurteilung durch die zuständigen Behörden aus den gesetzmäßigen Anordnungen an die Hostingdiensteanbieter, 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 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. ***Unbeschadet der Anforderung gemäß Artikel 7 [oder gemäß dem Gesetzgebungsentwurf zu elektronischen Beweismitteln],*** Daten aufzubewahren, obliegt es den Hostingdiensteanbietern, zu entscheiden, ob sie die betreffenden Inhalte entfernen oder den Zugang zu den Inhalten für Nutzer in der Union sperren. ***Dies sollte dazu führen, dass Internetnutzer, die ihre Dienste nutzen, daran gehindert werden, oder dass es ihnen zumindest erschwert wird und sie ernsthaft davon abgeschreckt werden, auf Inhalte zuzugreifen, zu denen der Zugang gesperrt wurde.***

(13a) Die Entfernungsanordnung sollte eine Klassifizierung des betreffenden Inhalts als terroristischer Inhalt sowie ausreichende Informationen zur Fundstelle des Inhalts enthalten – es sollte die URL-Adresse sowie weitere Angaben zur Verfügung gestellt werden, zum Beispiel ein Screenshot des betreffenden Inhalts. Wenn sie dazu aufgefordert wird, sollte die zuständige Behörde eine zusätzliche Begründung einreichen, warum der Inhalt als terroristischer Inhalt eingestuft wird. Die eingereichten Gründe müssen keine sensiblen Informationen enthalten, die Ermittlungen gefährden könnten. Die Begründung sollte es allerdings den Hostingdiensteanbietern und letztendlich auch den Inhalteanbietern ermöglichen, ihr Recht auf wirksamen Rechtsbehelf effektiv wahrzunehmen.

(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 der Absendung und des Eingangs der Anordnung, gestatten (z. B. über ein gesichertes E-Mail-System und 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 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 erfüllt werden[7].

[7] 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) [...] ***D***ieser ***Meldem***echanismus, mit dem Hostingdiensteanbieter auf Informationen ***und Materialien*** aufmerksam gemacht werden, die als terroristische Inhalte angesehen werden können und deren Vereinbarkeit mit ihren Nutzungsbedingungen sie somit freiwillig prüfen können, [...] ***stellt eine besonders effektive, rasche und verhältnismäßige Möglichkeit dar, um Hostingdiensteanbieter auf spezielle Inhalte in ihren Diensten aufmerksam zu machen***. 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[8] festgelegte Mandat von Europol bleibt von der Durchführung dieser Verordnung im Hinblick auf die Meldungen unberührt.

(16) Angesichts des Umfangs und der Schnelligkeit, die für eine wirksame Erkennung und Entfernung terroristischer Inhalte erforderlich sind, sind verhältnismäßige proaktive 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 prüfen, ob es in Abhängigkeit von Risiko und Ausmaß der möglichen Beeinflussung durch terroristische Inhalte sowie von den Auswirkungen auf die Rechte Dritter und auf das öffentliche Informationsinteresse angemessen ist, proaktive Maßnahmen zu ergreifen. Aus diesem Grund sollten Hostingdiensteanbieter festlegen, welche geeigneten, wirksamen und verhältnismäßigen proaktiven Maßnahmen ergriffen werden sollten. Diese Anforderung sollte nicht mit einer allgemeinen Überwachungspflicht verbunden sein. Im Rahmen dieser Prüfung ist das Fehlen von an einen Hostingdiensteanbieter gerichteten Entfernungsanordnungen ein Hinweis auf ein geringes ***Risiko und*** eine geringe Beeinflussung durch terroristische Inhalte.

---

8 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).

(17) Bei der Durchführung proaktiver Maßnahmen sollten die Hostingdiensteanbieter dafür sorgen, dass das Recht der Nutzer auf Meinungs- und Informationsfreiheit – darunter das Recht, Informationen frei zu empfangen und zu weitergeben – gewahrt bleibt. 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 Aufsicht und Überprüfung, 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.

(18) Um sicherzustellen, dass Hostingdiensteanbieter, die terroristischen Inhalten ausgesetzt sind, geeignete Maßnahmen ergreifen, um den Missbrauch ihrer Dienste zu verhindern, sollten die zuständigen Behörden die Hostingdiensteanbieter, die eine rechtskräftig gewordene Entfernungsanordnung erhalten haben, ersuchen, über die ergriffenen proaktiven 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 Instrumente 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 Instrumente. Der Diensteanbieter sollte über die spezifischen proaktiven Maßnahmen Bericht erstatten, damit die zuständige Behörde beurteilen kann, ob die Maßnahmen 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 und Verhältnismäßigkeit der Maßnahmen sollten die zuständigen Behörden die einschlägigen Parameter berücksichtigen, einschließlich der Anzahl der an den Anbieter gerichteten Entfernungsanordnungen und Meldungen, seiner wirtschaftlichen Leistungsfähigkeit und der Wirkung seines Dienstes bei der Verbreitung terroristischer Inhalte (z. B. unter Berücksichtigung der Zahl der Nutzer in der Union).

(19) Nach dem Ersuchen sollte die zuständige Behörde mit dem Hostingdiensteanbieter einen Dialog über die erforderlichen proaktiven Maßnahmen aufnehmen. Falls erforderlich, sollte die zuständige Behörde geeignete, wirksame und verhältnismäßige proaktive Maßnahmen auferlegen, wenn sie der Auffassung ist, dass die getroffenen Maßnahmen den Risiken nicht hinreichend gerecht werden. Die Entscheidung, 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.

(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, ***sowie "Transaktionsdaten"*** 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 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 die Reaktivierung dieses Inhalts in seiner vor der Entfernung bestehenden Form sichergestellt werden. Die Verpflichtung zur Aufbewahrung der Inhalte für Ermittlungs- und Strafverfolgungszwecke ist notwendig und gerechtfertigt, da dieses Material zur Störung oder Verhinderung terroristischer Aktivitäten wertvoll sein könnte. Wenn Unternehmen, insbesondere durch ihre eigenen proaktiven Maßnahmen, Material entfernen oder den Zugang dazu sperren, und die zuständige Behörde nicht 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 Aufbewahrung von Inhalten zu Zwecken der Verhinderung, Erkennung, Ermittlung und Verfolgung terroristischer Straftaten ebenfalls gerechtfertigt. Aus diesen Gründen 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.

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

(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. Hostingdiensteanbieter***, die terroristischen Inhalten ausgesetzt sind,*** sollten jährliche Transparenzberichte mit aussagekräftigen Informationen über ihre Maßnahmen im Zusammenhang mit der Erkennung, Ermittlung und Entfernung terroristischer Inhalte veröffentlichen***, soweit dies nicht dem Zweck der umgesetzten Maßnahmen zuwiderläuft***.

(25) Beschwerdeverfahren stellen eine notwendige Schutzvorkehrung gegen die irrtümliche Entfernung von Inhalten dar, ***die aufgrund von Maßnahmen gemäß den Nutzungsbedingungen der Hostingdiensteanbieter gelöscht wurden*** und die im Rahmen der Meinungs- und Informationsfreiheit geschützt sind. Die Hostingdiensteanbieter sollten daher nutzerfreundliche Beschwerdeverfahren einrichten und dafür sorgen, dass Beschwerden unverzüglich und in voller 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. ***Zudem sollten Inhalteanbieter, deren Inhalte aufgrund einer Entfernungsanordnung entfernt wurden, das Recht auf einen wirksamen Rechtsbehelf gemäß Artikel 19 EUV und Artikel 47 der Charta der Grundrechte der Europäischen Union haben.***

(26) ***Generell*** setzen wirksame Rechtsbehelfe nach Artikel 19 EUV und Artikel 47 der Charta der Grundrechte der Europäischen Union 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 aussagekräftige Informationen zur Verfügung stellen, die dem Inhalteanbieter die Anfechtung der Entscheidung ermöglichen. Dies erfordert jedoch nicht notwendigerweise eine Benachrichtigung des Inhalteanbieters. Je nach den Umständen 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.

(27) Zur Vermeidung von Doppelarbeit und einer gegenseitigen Behinderung bei (nationalen) Ermittlungen sollten die zuständigen Behörden einander informieren und sich untereinander sowie gegebenenfalls mit Europol abstimmen und kooperieren, ***bevor sie*** Entfernungsanordnungen erteilen oder ***wenn sie*** Meldungen an die Hostingdiensteanbieter ***senden***. [...]***Wenn sie über die Erteilung einer der Entfernungsanordnung entscheidet, sollte die zuständige Behörde Benachrichtigungen zu konfligierenden Ermittlungsinteressen gebührend berücksichtigen ("Konfliktvermeidung"). Wenn eine zuständige Behörde von der zuständigen Behörde eines anderen Mitgliedstaats über eine bereits erteilte Entfernungsanordnung informiert wird, sollte keine zweite Anordnung erteilt werden.*** Bei der Umsetzung der Bestimmungen dieser Verordnung könnte Europol im Einklang mit seinem derzeitigen Mandat und bestehenden Rechtsrahmen Unterstützung leisten.

(28) Um die wirksame und ausreichend kohärente Durchführung proaktiver Maßnahmen zu gewährleisten, sollten die zuständigen Behörden der Mitgliedstaaten in Bezug auf die Gespräche, die sie mit den Hostingdiensteanbietern führen, zusammenarbeiten, um spezifische proaktive Maßnahmen zu ermitteln, umzusetzen und zu bewerten. In ähnlicher Weise ist eine solche Zusammenarbeit auch hinsichtlich der Annahme von Vorschriften über Sanktionen sowie der Um- und Durchsetzung von Sanktionen erforderlich. ***Die Kommission sollte diese Abstimmung und Zusammenarbeit erleichtern.***

(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 jeweils zuständigen Behörde informiert ist. Zu diesem Zweck sollten die Mitgliedstaaten geeignete Kommunikationskanäle oder -mechanismen vorsehen, die die rechtzeitige Übermittlung der relevanten Informationen ermöglichen.

(30) Um den raschen Austausch zwischen den zuständigen Behörden untereinander und mit den Hostingdiensteanbietern zu erleichtern und Doppelarbeit zu vermeiden, ***werden*** die Mitgliedstaaten ***aufgefordert, die speziell dafür*** von Europol entwickelten Instrumente wie die aktuelle Verwaltungsanwendung für die Meldung von Internetinhalten (Internet Referral Management application, IRMa) oder deren Nachfolgeinstrumente ***zu*** 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.[9]

(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 ***– internen oder ausgelagerten –*** Einrichtung bestehen, die die elektronische Übermittlung von Entfernungsanordnungen und Meldungen ermöglicht, sowie technisch ***oder*** personell so ausgestattet ist, dass eine zügige 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 [...] Hostingdiensteanbieter***, die terroristischen Inhalten ausgesetzt sind, was durch den Eingang einer endgültigen Entfernungsanordnung belegt wurde,*** 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. 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.

(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. ***Um eine wirksame Umsetzung zu gewährleisten sowie aus Gründen der Dringlichkeit und der Wahrung öffentlicher Interessen sollte die Gerichtsbarkeit für Entfernungsanordnungen und Meldungen bei den Mitgliedstaaten liegen.***

---

[9] COM(2018) 225 final.

(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 jeden bestehenden gesetzlichen Vertreter einschalten, wenn dieser in der Lage ist, seine Aufgaben wie in dieser Verordnung dargelegt auszuführen.***

(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 benennen. Aus der Anforderung, zuständige Behörden zu benennen, folgt nicht notwendigerweise die Einrichtung neuer Behörden, sondern es kann sich um bereits bestehende Stellen handeln, die mit den in dieser Verordnung festgelegten Aufgaben betraut werden. Diese Verordnung schreibt die Benennung der Behörden vor, die für die Erteilung von Entfernungsanordnungen und Meldungen sowie die Aufsicht über proaktive Maßnahmen und die Verhängung von Sanktionen zuständig sind. Es ist Sache der Mitgliedstaaten zu entscheiden, wie viele Behörden sie für diese Aufgaben benennen wollen.

(38) Sanktionen sind erforderlich, damit gewährleistet ist, dass die Hostingdiensteanbieter die ihnen aus dieser Verordnung erwachsenden Verpflichtungen wirksam umsetzen. Die Mitgliedstaaten sollten für Sanktionen***, bei denen es sich um verwaltungs- oder strafrechtliche Sanktionen handeln kann,*** Regeln, gegebenenfalls auch Leitlinien für die Verhängung von Geldbußen, erlassen. Besonders schwere Sanktionen werden für den Fall festgelegt, 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 Verordnung festgelegt werden, in welchem Umfang die einschlägigen Verpflichtungen mit Sanktionen belegt werden können. Sanktionen für Verstöße gegen Artikel 6 sollten nur im Zusammenhang mit der Berichtspflicht nach Artikel 6 Absatz 2 oder einer Entscheidung zur Auferlegung zusätzlicher proaktiver Maßnahmen nach Artikel 6 Absatz 4 verhängt werden. ***Wenn die Art des Verstoßes bewertet und über die Anwendung von Sanktionen entschieden wird, sollten Grundrechte wie die Meinungsfreiheit uneingeschränkt geachtet werden.*** Bei der Entscheidung, ob finanzielle Sanktionen verhängt werden sollen, sollten die finanziellen Mittel des Anbieters gebührend berücksichtigt werden. Die Mitgliedstaaten stellen sicher, dass Sanktionen nicht dazu führen, dass nicht terroristische Inhalte entfernt werden.

(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 niedergelegt wurden.[10] 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.

(41) Die Mitgliedstaaten sollten Informationen über die Umsetzung der Rechtsvorschriften sammeln. ***Die Mitgliedstaaten können die Transparenzberichte der Hostingdiensteanbieter nutzen und diese, wo notwendig, durch ausführlichere Informationen ergänzen.*** Es sollte ein detailliertes Programm zur Überwachung der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung erstellt werden, um die Bewertung zu erleichtern.

---

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

(42) Anhand der Ergebnisse und Schlussfolgerungen des Umsetzungsberichts und der Ergebnisse der Überwachung sollte die Kommission frühestens drei Jahre nach ihrem Inkrafttreten eine Bewertung dieser Verordnung vornehmen. Die Bewertung sollte sich auf die fünf Kriterien Effizienz, Wirksamkeit, Relevanz, Kohärenz und EU-Mehrwert stützen. Bewertet wird 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 Interessen Dritter, darunter die Überprüfung der Verpflichtung zur Unterrichtung der Inhalteanbieter.

(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 einheitliche Vorschriften zur Verhinderung des Missbrauchs von Hosting-Diensten zur Verbreitung terroristischer Online-Inhalte festgelegt. Insbesondere werden festgelegt:

(a) Vorschriften über Sorgfaltspflichten, die von den Hostingdiensteanbietern anzuwenden sind, um die Verbreitung terroristischer Inhalte durch ihre Dienste zu verhindern und erforderlichenfalls die rasche Entfernung solcher Inhalte zu gewährleisten;

(b) eine Reihe Maßnahmen, die von den Mitgliedstaaten umzusetzen sind, um terroristische Inhalte zu ermitteln, deren rasche Entfernung durch die Hostingdiensteanbieter zu ermöglichen und die Zusammenarbeit mit den zuständigen Behörden der anderen Mitgliedstaaten, Hostingdiensteanbietern und gegebenenfalls den zuständigen Einrichtungen der Union zu erleichtern.

(2) Diese Verordnung gilt für Hostingdiensteanbieter, die unabhängig vom Ort ihrer Hauptniederlassung Dienstleistungen in der Union anbieten.

(3) ***Diese Verordnung berührt nicht die Pflicht, die Grundrechte und die allgemeinen Rechtsgrundsätze, wie sie in Artikel 6 des Vertrags über die Europäische Union niedergelegt sind, zu achten.***

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

(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 zur Verfügung zu stellen;

(2) "Inhalteanbieter" einen Nutzer, der Informationen bereitgestellt hat, die in seinem Auftrag von einem Hostingdiensteanbieter gespeichert wurden oder gespeichert werden;

(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 die Niederlassung des Hostingdiensteanbieters in der Union;

mangels einer solchen Niederlassung wird die Bewertung einer wesentlichen Verbindung anhand spezifischer faktengestützter Kriterien vorgenommen, wie

(a) ***eine*** erhebliche Zahl von Nutzern in einem oder mehreren Mitgliedstaaten;

(b) ***oder*** die Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten.

(4) "terroristische Straftaten" ***eine der in*** Artikel 3 Absatz 1 der Richtlinie (EU) 2017/541 ***aufgeführten vorsätzlichen Handlungen***;

(5) "terroristische Inhalte" [...] ***Material, das dazu beitragen kann, dass die in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten vorsätzlichen Handlungen begangen werden, durch:***

aa) die Drohung, eine terroristischen Straftat zu begehen;

(a) ***den*** Aufruf zu oder die Befürwortung von terroristischen Straftaten, ***beispielsweise*** durch ***die*** Verherrlichung *terroristischer* Handlungen, mit der damit einhergehenden Gefahr, dass solche Taten begangen werden könnten;

(b) ***die Gewinnung von Personen oder einer Gruppe von Personen für die Begehung von oder*** Mitwirkung an terroristischen Straftaten [...];

(c) die Förderung der Aktivitäten einer terroristischen Vereinigung, insbesondere durch [...] ***die Gewinnung von Personen oder einer Gruppe von Personen für die*** Beteiligung an oder Unterstützung von kriminellen Tätigkeiten einer terroristischen Vereinigung im Sinne des Artikels 2 Absatz 3 der Richtlinie (EU) 2017/541;

technische Anleitungen oder Methoden für das Begehen terroristischer Straftaten.

(6) "Verbreitung terroristischer Inhalte" die Bereitstellung terroristischer Inhalte für Dritte durch die Dienste des Hostingdiensteanbieters;

(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;

(9) "Hauptniederlassung" die Hauptverwaltung oder der eingetragene Sitz, wo ***in der Union*** die wichtigsten Finanzfunktionen und die betriebliche Kontrolle ausgeübt werden.

ABSCHNITT II

MAßNAHMEN ZUR VERHINDERUNG DER VERBREITUNG TERRORISTISCHER ONLINE-INHALTE

Artikel 3

Sorgfaltspflichten

(1) Die Hostingdiensteanbieter ergreifen geeignete, angemessene und verhältnismäßige Maßnahmen 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 unter gebührender Berücksichtigung der Grundrechte der Nutzer und tragen der grundlegenden Bedeutung der Meinungs- und Informationsfreiheit in einer offenen und demokratischen Gesellschaft Rechnung.

(2) Die Hostingdiensteanbieter nehmen in ihre Nutzungsbedingungen Bestimmungen auf, ***dass sie keine terroristischen Inhalte speichern***, und wenden Bestimmungen zur Verhinderung der Verbreitung terroristischer Inhalte an.

Artikel 4

Entfernungsanordnungen

(1) Die zuständige Behörde ist befugt, ***Entfernungsanordnungen*** zu erlassen, mit denen Hostingdiensteanbieter verpflichtet werden, terroristische Inhalte zu entfernen oder zu sperren.

(2) Die Hostingdiensteanbieter entfernen die terroristischen Inhalte innerhalb einer Stunde nach Eingang der Entfernungsanordnung oder sperren den Zugang dazu.

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

(a) die Bezeichnung der zuständigen Behörde, die die Entfernungsanordnung ausgestellt hat, und die Authentifizierung der Entfernungsanordnung durch die zuständige Behörde; [...] ***eine Bewertung des Inhalts***, [...] zumindest durch Bezugnahme auf die ***betreffenden*** in Artikel 2 Absatz 5 aufgeführten Kategorien terroristischer Inhalte;

(b) einen Uniform Resource Locator (URL-Adresse) und gegebenenfalls weitere Angaben, die die Identifizierung der gemeldeten Inhalte ermöglichen;

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

(d) Datum und Uhrzeit der Ausstellung;

(e) Informationen über Rechtsbehelfe, die dem Hostingdiensteanbieter und dem Inhalteanbieter zur Verfügung stehen;

(f) gegebenenfalls die Entscheidung nach Artikel 11, keine Informationen über die Entfernung oder die Sperrung terroristischer Inhalte weiterzugeben.

(4) Auf Antrag des Hostingdiensteanbieters oder des Inhalteanbieters legt die zuständige Behörde eine ***ergänzende*** Begründung vor, ***mit der erläutert wird, warum der Inhalt als terroristischer Inhalt erachtet wird,*** unbeschadet der Verpflichtung des Hostingdiensteanbieters, der Entfernungsanordnung innerhalb der in Absatz 2 genannten Frist nachzukommen.

(5) Die zuständigen Behörden richten Entfernungsanordnungen an die Hauptniederlassung des Hostingdiensteanbieters oder an den vom Hostingdiensteanbieter nach Artikel 16 benannten gesetzlichen Vertreter und übermitteln 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 der Absendung und des Eingangs der Anordnung, gestatten.

(6) Die Hostingdiensteanbieter bestätigen ***unverzüglich*** den Eingang und unterrichten die zuständige Behörde [...] 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.

(7) Kann der Hostingdiensteanbieter der Entfernungsanordnung wegen höherer Gewalt oder einer faktischen Unmöglichkeit, die dem Hostingdiensteanbieter nicht angelastet werden kann, nicht nachkommen, so teilt er dies der zuständigen Behörde 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.

(8) Kann der Hostingdiensteanbieter der Entfernungsanordnung nicht nachkommen, weil die Entfernungsanordnung offensichtliche Fehler oder unzureichende Informationen enthält, um die Anordnung auszuführen, so 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.

(9) Die zuständige Behörde, die die Entfernungsanordnung ausgestellt hat, unterrichtet die für die Überwachung der Durchführung proaktiver 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.

Artikel 4a

Konsultationsverfahren für Entfernungsanordnungen

(1) Zeitgleich mit der Übermittlung einer Entfernungsanordnung an den Hostingdiensteanbieter gemäß Artikel 4 Absatz 5 legt die Anordnungsbehörde der gemäß Artikel 17 Absatz 1 zuständigen Behörde des Mitgliedstaats, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat, eine Kopie dieser Entfernungsanordnung vor.

(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.

(3) Die Anordnungsbehörde berücksichtigt diese Umstände und zieht die Entfernungsanordnung erforderlichenfalls zurück oder passt sie entsprechend an.

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 [...] Informationen [...] ***über die*** Gründe, aus denen der Inhalt als terroristischer Inhalt erachtet wird, ***gibt*** eine URL ***an*** und enthält 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 ***unverzüglich*** die zuständige Behörde oder die zuständige Einrichtung der Union [...] 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.

Artikel 6

Proaktive Maßnahmen

(1) Die Hostingdiensteanbieter ergreifen ***je nach Risiko und Ausmaß der möglichen Beeinflussung durch terroristische Inhalte*** [...] proaktive Maßnahmen, um ihre Dienste vor der Verbreitung terroristischer Inhalte zu schützen. Die Maßnahmen müssen wirksam 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 in einer offenen und demokratischen Gesellschaft Rechnung zu tragen ist.

(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 Instrumente, vorzulegen, um

(a) [...] ***wirksam gegen ein erneutes Auftauchen von Inhalten vorzugehen***, die zuvor entfernt oder gesperrt wurden, weil sie als terroristische Inhalte erachtet werden [...];

(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 Instrumente sowie Mechanismen der Aufsicht und Überprüfung durch Menschen ein.

(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.

(4) Kann innerhalb der drei Monate nach der Aufforderung keine Einigung im Sinne von Absatz 3 erzielt werden, so kann die zuständige Behörde nach Artikel 17 Absatz 1 Buchstabe c eine Entscheidung erlassen, mit der spezifische zusätzliche, notwendige und verhältnismäßige proaktive Maßnahmen auferlegt werden. In der Entscheidung werden insbesondere die wirtschaftliche Leistungsfähigkeit des Hostingdiensteanbieters und die Auswirkungen dieser Maßnahmen auf die Grundrechte der Nutzer und die grundlegende Bedeutung der Meinungs- und Informationsfreiheit berücksichtigt. ***Es liegt in der Verantwortung der zuständigen Behörde nach Artikel 17 Absatz 1 Buchstabe c, im Einklang mit dem Ziel dieser Verordnung über die Art und den Umfang der proaktiven Maßnahmen zu entscheiden.*** Diese Entscheidung 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.

(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. 4 zu überprüfen oder gegebenenfalls zu widerrufen. Die zuständige Behörde trifft innerhalb einer angemessenen Frist nach Eingang des Ersuchens des Hostingdiensteanbieters eine mit Gründen versehene Entscheidung.

Artikel 7

Aufbewahrung von Inhalten und zugehörigen Daten

(1) Die Hostingdiensteanbieter bewahren terroristische Inhalte, die infolge einer Entfernungsanordnung, einer Meldung oder proaktiver 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:

(a) Verfahren der behördlichen oder gerichtlichen Überprüfung,

(b) Verhinderung, Erkennung, Untersuchung und Verfolgung von terroristischen Straftaten.

(2) Die terroristischen Inhalte und zugehörigen Daten nach Absatz 1 werden für einen Zeitraum von sechs Monaten aufbewahrt. Auf Anordnung der zuständigen Behörde oder des zuständigen Gerichts werden die terroristischen Inhalte für einen längeren Zeitraum aufbewahrt, wenn und solange dies für laufende Verfahren der behördlichen oder gerichtlichen Überprüfung nach Absatz 1 Buchstabe a erforderlich ist.

(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

(1) Die Hostingdiensteanbieter legen in ihren Nutzungsbedingungen ihre Strategie zur Verhinderung der Verbreitung terroristischer Inhalte dar, gegebenenfalls mit einer aussagekräftigen Erläuterung der Funktionsweise proaktiver Maßnahmen, einschließlich der Verwendung automatisierter Instrumente.

(2) Die Hostingdiensteanbieter, [...] ***die terroristischen Inhalten ausgesetzt sind,*** veröffentlichen jährliche Transparenzberichte über die gegen die Verbreitung terroristischer Inhalte ergriffenen Maßnahmen.

(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, ***die der*** Hostingdiensteanbieter ***trifft, um wirksam gegen*** ein erneutes Auftauchen von Inhalten ***vorzugehen***, die zuvor entfernt oder gesperrt wurden, weil sie als terroristische Inhalte erachtet werden;

(c) Anzahl der nach Entfernungsanordnungen, Meldungen oder proaktiven Maßnahmen entfernten oder gesperrten Elemente mit terroristischem Inhalt;

(d) Übersicht über Beschwerdeverfahren und deren Ergebnis.

Artikel 9

Schutzvorkehrungen in Bezug auf die Anwendung und Durchführung proaktiver Maßnahmen

(1) Verwenden Hostingdiensteanbieter nach dieser Verordnung automatisierte Instrumente 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 Inhalten, die als terroristische Inhalte erachtet werden, zutreffend und fundiert sind.

(2) Die Schutzvorkehrungen bestehen, soweit angemessen, insbesondere in einer 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.

Artikel 10

Beschwerdemechanismen

(1) Die Hostingdiensteanbieter richten wirksame und zugängliche Mechanismen ein, die Inhalteanbietern, deren Inhalte aufgrund einer Entfernungsanordnung nach Artikel 5 oder proaktiver Maßnahmen nach Artikel 6 entfernt oder gesperrt wurden, die Möglichkeit geben, Beschwerde gegen die Maßnahme des Hostingdiensteanbieters einzulegen und die Reaktivierung des Inhalts zu verlangen.

(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 Ergebnis der Prüfung in Kenntnis.

Artikel 11

Unterrichtung der Inhalteanbieter

(1) Entfernen oder sperren Hostingdiensteanbieter terroristische Inhalte, so stellen sie dem Inhalteanbieter Informationen über die Entfernung oder Sperrung der terroristischen Inhalte zur Verfügung.

(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.

(3) Die Verpflichtung nach den Absätzen 1 und 2 gilt nicht, wenn die zuständige Behörde entscheidet, dass aus Gründen der öffentlichen Sicherheit wie der Verhinderung, Untersuchung, Erkennung und Verfolgung terroristischer Straftaten so lange wie erforderlich, längstens jedoch ***sechs*** Wochen ab dieser Entscheidung, keine Informationen weitergegeben dürfen. ***Falls gerechtfertigt, kann dieser Zeitraum einmal um weitere sechs Wochen verlängert werden.*** In diesem Fall gibt der Hostingdiensteanbieter keine Informationen über die Entfernung oder Sperrung terroristischer Inhalte weiter.

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.

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 Europol einander, stimmen sich ab und arbeiten zusammen, um Doppelarbeit zu vermeiden, die Koordinierung zu verstärken und Überschneidungen mit Untersuchungen in verschiedenen Mitgliedstaaten zu vermeiden.

(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 Kommunikationskanäle oder Mechanismen vor, um sicherzustellen, dass die relevanten Informationen rechtzeitig übermittelt werden.

(3) ***Für die wirksame Umsetzung dieser Verordnung sowie um Doppelarbeit zu vermeiden,*** können sich die Mitgliedstaaten und Hostingdiensteanbieter für die Verwendung spezieller Instrumente entscheiden, [...] auch der von den zuständigen Einrichtungen der Union wie Europol eingerichteten Instrumente, um insbesondere Folgendes zu erleichtern:

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

(b) die Bearbeitung von Meldungen nach Artikel 5 und diesbezügliche Rückmeldungen;

(c) die Zusammenarbeit zur Ermittlung und Durchführung proaktiver Maßnahmen nach Artikel 6.

(4) Verfügen Hostingdiensteanbieter über Nachweise für terroristische Straftaten, so unterrichten sie unverzüglich die für die Untersuchung und Verfolgung von Straftaten in dem oder den betreffenden Mitgliedstaat(en) zuständigen Behörden [...]. ***Ist es nicht möglich, den(die) betreffenden Mitgliedstaat(en) festzustellen, benachrichtigen*** die Hostingdiensteanbieter ***die Kontaktstelle nach Artikel 14 Absatz 3 in dem Mitgliedstaat, in dem sie ihre Hauptniederlassung haben oder über einen gesetzlichen Vertreter verfügen und übermitteln*** diese Informationen zur weiteren Bearbeitung an Europol [...].

Artikel 14

Kontaktstellen

(1) Die Hostingdiensteanbieter richten eine Kontaktstelle ein, die den Erhalt von Entfernungsanordnungen und Meldungen auf elektronischem Weg ermöglicht und deren zügige Bearbeitung nach den Artikeln 4 und 5 sicherstellt. Sie sorgen dafür, dass diese Informationen öffentlich zugänglich gemacht werden.

(2) In den Informationen nach Absatz 1 sind die Amtssprachen der Union gemäß der Verordnung Nr. 1/58 anzugeben, in denen die Kontaktstelle angeschrieben werden kann und in denen der weitere Austausch im Zusammenhang mit Entfernungsanordnungen und Meldungen nach den Artikeln 4 und 5 stattfindet. Zu ihnen 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.

(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.

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. ***Jeder Mitgliedstaat ist für die Zwecke im Sinne der Artikel 4 und 5 zuständig, unabhängig davon, wo der Hostingdiensteanbieter seine Hauptniederlassung oder einen gesetzlichen Vertreter benannt hat.***

(2) Hat ein Hostingdiensteanbieter keinen gesetzlichen Vertreter benannt, so liegt die Gerichtsbarkeit bei allen Mitgliedstaaten. ***Entscheidet ein Mitgliedstaat, die Gerichtsbarkeit auszuüben, unterrichtet er hiervon alle anderen Mitgliedstaaten.***

[…] […]

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 gesetzlichen Vertreter in der Union für die Entgegennahme, Einhaltung und Durchsetzung von Entfernungsanordnungen, Meldungen, Anträgen und Entscheidungen, 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.

(2) Der Hostingdiensteanbieter betraut den gesetzlichen Vertreter mit der Entgegennahme, Einhaltung und Durchsetzung der Entfernungsanordnungen, Meldungen, Anträge und Entscheidungen 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.

(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 oder die Behörden, die dafür zuständig sind,

(a) Entfernungsanordnungen nach Artikel 4 auszustellen;

(b) terroristische Inhalte zu erkennen, zu ermitteln und den Hostingdiensteanbietern nach Artikel 5 zu melden;

(c) die Durchführung proaktiver Maßnahmen nach Artikel 6 zu überwachen;

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

(2) Die Mitgliedstaaten teilen der Kommission die in Absatz 1 genannte ***zuständige Behörde oder*** zuständigen Behörden bis zum [***zwölf*** *Monate nach Inkrafttreten dieser Verordnung*] mit. Die Kommission veröffentlicht die Mitteilung und eventuelle Änderungen derselben im *Amtsblatt der Europäischen Union*.

Artikel 18

Sanktionen

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen der Hostingdiensteanbieter gegen die Verpflichtungen aus dieser Verordnung zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Diese Sanktionen beschränken sich auf Verstöße gegen die Verpflichtungen aus

(a) Artikel 3 Absatz 2 (Nutzungsbedingungen von Hostingdiensteanbietern);

(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);

(d) Artikel 6 Absätze 2 und 4 (Berichte über proaktive Maßnahmen und Ergreifung von Maßnahmen aufgrund einer Entscheidung zur Auferlegung spezifischer proaktiver Maßnahmen);

(e) Artikel 7 (Aufbewahrung von Daten);

(f) Artikel 8 (Transparenz);

(g) Artikel 9 (Schutzvorkehrungen in Bezug auf proaktive Maßnahmen);

(h) Artikel 10 (Beschwerdeverfahren);

(i) Artikel 11 (Unterrichtung der Inhalteanbieter);

(j) Artikel 13 Absatz 4 (Informationen über Nachweise für terroristische Straftaten);

(k) Artikel 14 Absatz 1 (Kontaktstellen);

(l) Artikel 16 (Benennung eines gesetzlichen Vertreters).

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

(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 ***oder natürlichen*** Person;

(d) die Finanzkraft der haftbaren juristischen ***oder natürlichen*** Person;

(e) die Bereitschaft des Hostingdiensteanbieters, mit den zuständigen Behörden zusammenzuarbeiten.

(4) Die Mitgliedstaaten stellen sicher, dass bei einem systematischen Verstoß gegen die Verpflichtungen aus Artikel 4 Absatz 2 finanzielle Sanktionen in Höhe von bis zu 4 % des weltweiten Jahresumsatzes des Hostingdiensteanbieters im vorangegangenen Geschäftsjahr verhängt werden.

Artikel 19

Technische Anforderungen und Änderungen der Formulare für Entfernungsanordnungen

(1) Der Kommission wird die Befugnis übertragen, nach Artikel 20 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.

(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 ergangenen Entfernungsanordnungen und Meldungen nach Artikel 4 und Artikel 5, die Anzahl der entfernten oder gesperrten Elemente mit terroristischem Inhalt, einschließlich der zugehörigen Fristen;

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

(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 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 vor. Gegebenenfalls wird der Bericht um Legislativvorschläge ergänzt. Die Mitgliedstaaten übermitteln der Kommission die für die Ausarbeitung des Berichts erforderlichen Informationen.

Artikel 24

Inkrafttreten

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

Sie gilt ab dem [***12*** [...] Monate nach ihrem Inkrafttreten].

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

Geschehen zu Brüssel am […]

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