EUROPÄISCHE
KOMMISSION

Brüssel, den 12.9.2018
COM(2018) 640 final

2018/0331 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Verhinderung der Verbreitung terroristischer Online-Inhalte

Ein Beitrag der Europäischen Kommission zur Tagung der Staats- und Regierungschefs vom 19.–20. September 2018 in Salzburg

{SEC(2018) 397 final} - {SWD(2018) 408 final} - {SWD(2018) 409 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

1.1. Gründe und Ziele des Vorschlags

Die Allgegenwart des Internets ermöglicht es Nutzern, mit Hunderten von Millionen von Menschen auf der ganzen Welt zu kommunizieren und zu arbeiten, Kontakte zu pflegen sowie Informationen zu erstellen, zu erhalten und zu teilen. Internetplattformen sind in der gesamten Union und darüber hinaus für ihre Nutzer im Hinblick auf deren wirtschaftliches und gesellschaftliches Wohlergehen von großem Nutzen. Die Möglichkeit, so viele Adressaten zu minimalen Kosten zu erreichen, bietet jedoch auch Kriminellen einen Anreiz, das Internet für illegale Zwecke zu missbrauchen. Die jüngsten Terroranschläge in der EU haben deutlich gemacht, wie Terroristen dabei vorgehen – sie nutzen das Internet, um Kontakt zu ihren Unterstützern zu halten und neue Unterstützer zu gewinnen, terroristische Aktivitäten vorzubereiten und zu erleichtern, ihre Gräueltaten zu verherrlichen, andere aufzufordern, ihrem Beispiel zu folgen, und um in der breiten Öffentlichkeit Angst zu schüren.

Terroristische Inhalte, die für diese Zwecke im Internet geteilt werden, werden durch die Anbieter von Hosting-Diensten, die das Hochladen von Inhalten Dritter erlauben, weiterverbreitet. Bei mehreren Terroranschlägen, die Europa in jüngster Zeit erschütterten, haben terroristische Inhalte im Internet nachweislich eine entscheidende Rolle dabei gespielt, sogenannte „einsame Wölfe“ zu radikalisieren und ihnen den Anstoß zu Anschlägen zu geben. Solche Inhalte sind nicht nur von erheblichem Nachteil für Einzelne und die Gesellschaft insgesamt, sondern führen auch dazu, dass Nutzer weniger Vertrauen in das Internet haben sowie Geschäftsmodelle und der Ruf der betroffenen Unternehmen geschädigt werden. Terroristen haben nicht nur große Social-Media-Plattformen missbraucht, sondern zunehmend auch kleinere Anbieter, die unterschiedliche Arten von Hosting-Diensten weltweit anbieten. Dieser Missbrauch des Internets macht die besondere gesellschaftliche Verantwortung der Internetplattformen deutlich, die ihre Nutzer vor den terroristischen Inhalten schützen müssen, sowie die ernsten Sicherheitsrisiken, die diese Inhalte für die Gesellschaft insgesamt darstellen.

Auf entsprechende Aufforderungen der Behörden hin haben Anbieter von Hosting-Diensten Maßnahmen zur Bekämpfung terroristischer Inhalte in ihren Diensten ergriffen. Mit freiwilligen Maßnahmen und Partnerschaften wie dem EU-Internetforum, das im Dezember 2015 im Rahmen der Europäischen Sicherheitsagenda gegründet wurde, wurden bereits Fortschritte erzielt. Das EU-Internetforum hat die freiwillige Zusammenarbeit zwischen den Mitgliedstaaten und den Anbietern von Hosting-Diensten gefördert und Maßnahmen unterstützt, die die Zugänglichkeit terroristischer Online-Inhalte verringern und die Zivilgesellschaft darin bestärken, den Umfang schlagkräftiger, alternativer Diskurse im Internet zu erhöhen. Diese Anstrengungen haben dazu beigetragen, die Zusammenarbeit zu vertiefen, die Reaktion der Unternehmen auf die Meldungen nationaler Behörden und der Europol-Meldestelle für Internetinhalte zu verbessern, den Einsatz freiwilliger proaktiver Maßnahmen zur Verbesserung der automatischen Erkennung terroristischer Inhalte zu fördern, die Zusammenarbeit innerhalb der Branche zu stärken – auch durch die Entwicklung der „Hash-Datenbank“, mit der das Hochladen terroristischer Inhalte auf verbundenen Plattformen unterbunden werden soll – und die Transparenz bei diesen Anstrengungen zu erhöhen. Die Zusammenarbeit im Rahmen des EU-Internetforums dürfte in Zukunft zwar fortgesetzt werden, doch wurde auch deutlich, wo die Grenzen der freiwilligen Vereinbarungen liegen. Zum einen haben sich nicht alle betroffenen Anbieter von Hosting-Diensten in dem Forum engagiert, zum anderen reichen Umfang und Tempo der bei den

Hosting-Anbietern erzielten Fortschritte insgesamt nicht aus, um das Problem wirksam anzugehen.

Dies macht nur zu deutlich, wie notwendig verschärfte Maßnahmen seitens der Europäischen Union zur Bekämpfung terroristischer Online-Inhalte sind. Am 1. März 2018 verabschiedete die Kommission eine Empfehlung für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten, die sich auf die Mitteilung der Kommission vom September[1] sowie auf die Arbeiten des EU-Internetforums stützt. Die Empfehlung hat ein Kapitel allein den Maßnahmen gewidmet, mit denen sich das Hochladen und Teilen terroristischer Online-Propaganda wirksam eindämmen lässt – etwa durch ein verbessertes Meldeverfahren, ein Zeitfenster von einer Stunde zwischen Meldung und Reaktion, eine verstärkt proaktive Erkennung, wirksame Entfernung und ausreichende Schutzvorkehrungen zur genauen Bewertung terroristischer Inhalte[2].

Wie wichtig es ist, die Maßnahmen im Zusammenhang mit terroristischen Online-Inhalten zu verstärken, zeigt sich auch an den Forderungen der EU-Mitgliedstaaten, von denen einige bereits rechtliche Vorschriften erlassen oder eine entsprechende Absicht bekundet haben. Nach den Terroranschlägen in der EU und angesichts der Tatsache, dass terroristische Online-Inhalte nach wie vor leicht zugänglich sind, hat der Europäische Rat auf seiner Tagung vom 22. und 23. Juni 2017 die Branche aufgefordert, neue Techniken und Werkzeuge zu entwickeln, um die automatische Erkennung und Entfernung von zu terroristischen Handlungen anstiftenden Inhalten zu verbessern. Dies sollte erforderlichenfalls durch einschlägige Gesetzgebungsmaßnahmen auf EU-Ebene ergänzt werden. Am 28. Juni 2018 begrüßte der Europäische Rat die Absicht der Kommission, einen Gesetzgebungsvorschlag zur Verbesserung der Erkennung und Entfernung von Inhalten, die Hass schüren und zu terroristischen Handlungen anstiften, zu unterbreiten. Zudem richtete das Europäische Parlament in seiner Entschließung zu Online-Plattformen und zum digitalen Binnenmarkt vom 15. Juni 2017 an die betroffenen Plattformen die dringende Aufforderung, die Maßnahmen zum Umgang mit illegalen und schädlichen Inhalten zu verstärken, und an die Kommission die Forderung, Vorschläge zur Bewältigung dieser Probleme vorzulegen.

Zur Bewältigung dieser Herausforderungen und als Reaktion auf die Forderungen der Mitgliedstaaten und des Europäischen Parlaments war es der Kommission ein Anliegen, mit ihrem Vorschlag einen klaren und abgestimmten Rechtsrahmen zu schaffen, mit dem der Missbrauch von Hosting-Diensten für die Verbreitung terroristischer Online-Inhalte verhindert und gewährleistet werden kann, dass der digitale Binnenmarkt reibungslos funktioniert und Vertrauen und Sicherheit gewahrt werden. Mit dieser Verordnung soll klargestellt werden, dass Anbieter von Hosting-Diensten dafür zuständig sind, alle angemessenen, sinnvollen und verhältnismäßigen Maßnahmen zu ergreifen, die zur Gewährleistung der Sicherheit ihrer Dienste und für eine rasche und wirksame Erkennung und Entfernung terroristischer Online-Inhalte notwendig sind, wobei der grundlegenden Bedeutung der Meinungs- und Informationsfreiheit in einer offenen und demokratischen Gesellschaft Rechnung getragen wird. Zudem werden einige notwendige Schutzvorkehrungen für die uneingeschränkte Wahrung der Grundrechte eingeführt, wie der Meinungs- und Informationsfreiheit in einer demokratischen Gesellschaft, sowie die Möglichkeit von Rechtsbehelfen, wie sie durch den in Artikel 19 EUV und in Artikel 47 der EU-Grundrechtecharta verankerten wirksamen Rechtsschutz garantiert wird.

---

1 Mitteilung (COM(2017) 555 final) über den Umgang mit illegalen Online-Inhalten.

2 Empfehlung (C(2018) 1177 final) vom 1. März 2018 für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten.

Ziel des Vorschlags ist es, die Wirksamkeit der laufenden Maßnahmen zur Erkennung, Identifizierung und Entfernung terroristischer Inhalte zu erhöhen, ohne Grundrechte, wie die Meinungs- und Informationsfreiheit einzuschränken, indem den Anbietern von Hosting-Diensten ein Minimum an Sorgfaltspflichten, etwa bestimmte Regeln, auferlegt werden und auch die Mitgliedstaaten bestimmten Pflichten nachkommen müssen. Ein derart harmonisierter Rechtsrahmen wird die Bereitstellung von Online-Diensten im gesamten digitalen Binnenmarkt erleichtern, gleiche Wettbewerbsbedingungen für alle Anbieter von Hosting-Diensten schaffen, die ihre Dienste auf die Europäische Union ausrichten, und – flankiert durch angemessene Vorkehrungen zum Schutz der Grundrechte– einen soliden Rechtsrahmen für die Erkennung und Entfernung terroristischer Inhalte darstellen. So werden die Transparenzpflichten das Vertrauen der Bürgerinnen und Bürger und insbesondere der Internetnutzer stärken und die Rechenschaftspflicht sowie die Transparenz der Maßnahmen der Unternehmen, auch gegenüber den Behörden, verbessern. Der Vorschlag sieht zudem die Verpflichtung vor, Rechtsbehelfs- und Beschwerdemechanismen einzuführen, damit Nutzer die Entfernung ihrer Inhalte anfechten können. Die den Mitgliedstaaten auferlegten Verpflichtungen werden zu diesen Zielen beitragen und die einschlägigen Behörden besser in die Lage versetzen, geeignete Maßnahmen gegen terroristische Online-Inhalte und zur Verbrechensbekämpfung zu ergreifen. Kommen Anbieter von Hosting-Diensten ihren Pflichten aus dieser Verordnung nicht nach, können Mitgliedstaaten Sanktionen auferlegen.

1.2. Kohärenz mit den bestehenden Vorschriften in diesem Bereich

Dieser Vorschlag steht mit dem EU-Recht zum digitalen Binnenmarkt, insbesondere mit der Richtlinie über den elektronischen Geschäftsverkehr in Einklang. Keine Maßnahme, auch keine proaktive Maßnahme, die ein Anbieter von Hosting-Diensten auf der Grundlage dieser Verordnung ergreift, sollte für sich genommen dazu führen, dass der Diensteanbieter den Anspruch auf Haftungsausschluss verliert, der unter bestimmten Bedingungen nach Artikel 14 der Richtlinie über den elektronischen Geschäftsverkehr gewährt wird. Ein Beschluss nationaler Behörden zur Auferlegung verhältnismäßiger und konkreter proaktiver Maßnahmen sollte grundsätzlich nicht dazu führen, dass die Mitgliedstaaten eine allgemeine Überwachungspflicht nach Artikel 15 Absatz 1 der Richtlinie 2000/31/EG auferlegen. Angesichts der besonders großen Gefahren, die von der Verbreitung terroristischer Inhalte ausgehen, können die auf der Grundlage dieser Verordnung erlassenen Beschlüsse in Ausnahmefällen von diesem im EU-Recht festgelegten Grundsatz abweichen. Vor Annahme solcher Beschlüsse sollte die zuständige Behörde darauf achten, dass die Anforderungen an die öffentliche Sicherheit und die betreffenden Interessen und Grundrechte, wie vor allem die Meinungs- und Informationsfreiheit, die unternehmerische Freiheit sowie der Schutz personenbezogener Daten und der Privatsphäre in einem ausgewogenen Verhältnis stehen. Die Sorgfaltspflichten der Anbieter von Hosting-Diensten sollten dieser Ausgewogenheit Rechnung tragen, wie dies auch in der Richtlinie über den elektronischen Geschäftsverkehr zum Ausdruck gebracht wird.

Der Vorschlag steht darüber hinaus im Einklang mit der Richtlinie (EU) 2017/541 zur Terrorismusbekämpfung und ist auch an diese Richtlinie eng angelehnt, deren Ziel es ist, das einzelstaatliche Recht der Mitgliedstaaten dahingehend zu harmonisieren, dass terroristische Straftatbestände einheitlich definiert werden. Nach Artikel 21 dieser Richtlinie sind die Mitgliedstaaten verpflichtet, Maßnahmen zu ergreifen, um sicherzustellen, dass Online-Inhalte, die eine öffentliche Aufforderung zur Begehung einer Straftat darstellen, unverzüglich entfernt werden, wobei den Mitgliedstaaten die Art der Maßnahmen überlassen bleibt. Aufgrund ihres präventiven Charakters erstreckt sich diese Verordnung nicht nur auf zu Terrorismus anstiftendes Material, sondern auch auf Material für Rekrutierungs- und Schulungszwecke, und damit auch auf sonstige Straftaten im Zusammenhang mit

terroristischen Aktivitäten, die ebenfalls unter die Richtlinie (EU) 2017/541 fallen. Mit dieser Verordnung wird den Anbietern von Hosting-Diensten unmittelbar die Pflicht auferlegt, Sorgfalt walten zu lassen und terroristische Inhalte zu entfernen. Zudem werden die Verfahren für die Entfernungsanordnungen mit dem Ziel vereinheitlicht, die Zugänglichkeit terroristischer Online-Inhalte zu verringern.

Die Verordnung ergänzt mit ihrem im Hinblick auf Zielgruppe und Inhalt größeren Anwendungsbereich die in der künftigen Richtlinie über audiovisuelle Mediendienste festgelegten Vorschriften. Sie deckt nicht nur Videoplattformen, sondern unterschiedlichste Anbieter von Hosting-Diensten ab. Zudem gilt sie nicht nur für Videos, sondern auch für Bilder und Text. Außerdem geht die vorliegende Verordnung mit ihren materiellen Bestimmungen über die Richtlinie hinaus, indem die Vorschriften für Anordnungen zur Entfernung terroristischer Inhalte sowie proaktive Maßnahmen vereinheitlicht werden.

Die vorgeschlagene Verordnung baut auf der Empfehlung der Kommission[3] über den Umgang mit illegalen Inhalten vom März 2018 auf. Die Empfehlung bleibt nach wie vor in Kraft, so dass alle, die an der Verringerung der Zugänglichkeit illegaler Inhalte – auch terroristischer Inhalte – mitwirken, ihre Bemühungen mit den in der Verordnung genannten Maßnahmen auch fortsetzen und miteinander abstimmen sollten.

1.3. Zusammenfassung der vorgeschlagenen Verordnung

Zur Zielgruppe des Verordnungsvorschlags zählen die Anbieter von Hosting-Diensten, die ihre Dienste – unabhängig von deren Niederlassungsort oder ihrer Größe – in der Union anbieten. Mit dem vorgeschlagenen Rechtsakt werden Maßnahmen eingeführt, mit denen der Missbrauch von Hosting-Diensten für die Verbreitung terroristischer Online-Inhalte unterbunden und so gewährleistet werden soll, dass der digitale Binnenmarkt reibungslos funktioniert und Vertrauen und Sicherheit gewahrt werden. Die Begriffsbestimmung illegaler terroristischer Inhalte als Informationen, die zur Anstiftung und Verherrlichung terroristischer Straftaten sowie zur Aufforderung, einen Beitrag zu diesen Straftaten zu leisten, eingesetzt werden und die Anweisungen für das Begehen terroristischer Straftaten enthalten oder für die Beteiligung an terroristischen Vereinigungen werben, folgt der in der Richtlinie (EU) 2017/541 festgelegten Definition terroristischer Straftaten.

Damit sichergestellt ist, dass illegale terroristische Inhalte tatsächlich entfernt werden, wird mit der Verordnung die Entfernungsanordnung eingeführt, die durch Verwaltungs- oder Gerichtsentscheidung von einer zuständigen Behörde in einem Mitgliedstaat ausgestellt werden kann. In diesem Fall ist der Anbieter von Hosting-Diensten verpflichtet, innerhalb einer Stunde den Inhalt zu entfernen oder den Zugang zu diesem Inhalt zu desaktivieren. Darüber hinaus werden mit der Verordnung die Mindestanforderungen für die Meldungen festgelegt, die von den zuständigen Behörden der Mitgliedstaaten und Einrichtungen der Union (wie Europol) den Anbietern von Hosting-Diensten zur Überprüfung anhand ihrer jeweiligen Geschäftsbedingungen übermittelt werden. Schließlich sind die Anbieter von Hosting-Diensten nach der Verordnung verpflichtet, gegebenenfalls proaktive, im Verhältnis zum Risiko stehende Maßnahmen zu ergreifen und terroristisches Material aus ihren Diensten auch mit Hilfe automatischer Erkennungswerkzeuge zu entfernen.

Flankiert werden die Maßnahmen zur Verringerung terroristischer Online-Inhalte durch Vorkehrungen, mit denen der uneingeschränkte Schutz der Grundrechte gewährleistet werden soll. Zum Schutz nicht terroristischer Inhalte vor einer irrtümlichen Entfernung enthält der

[3] Empfehlung (C(2018) 1177 final) vom 1. März 2018 für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten.

Vorschlag Auflagen zur Festlegung von Rechtsbehelfen und Beschwerdemechanismen, mit denen sichergestellt werden soll, dass Nutzer die Entfernung ihre Inhalte anfechten können. Außerdem werden mit der Verordnung Transparenzpflichten für die Maßnahmen eingeführt, die die Anbieter von Hosting-Diensten gegen terroristische Inhalte ergreifen, womit die Rechenschaftspflicht gegenüber den Nutzern, Bürgern und Behörden gewahrt wird.

Zudem müssen die Mitgliedstaaten nach der Verordnung dafür sorgen, dass ihre zuständigen Behörden über die notwendigen Kapazitäten verfügen, um gegen terroristische Online-Inhalte vorgehen zu können. Darüber hinaus sind die Mitgliedstaaten verpflichtet, sich gegenseitig zu informieren und zu kooperieren, und können die von Europol eingerichteten Kanäle nutzen, um sicherzugehen, dass Entfernungsanordnungen und Meldungen koordiniert werden. Zudem sieht die Verordnung die Verpflichtung für Anbieter von Hosting-Diensten vor, Berichte mit Einzelheiten zu den von ihnen ergriffenen Maßnahmen vorzulegen und die Strafverfolgungsbehörden zu unterrichten, sobald sie auf Inhalte stoßen, die eine Gefahr für Leben oder Sicherheit darstellen. Schließlich sind die Anbieter von Hosting-Diensten verpflichtet, den von ihnen entfernten Inhalt aufzubewahren – als Sicherheit bei irrtümlicher Entfernung und als potenzielles Beweismaterial für Prävention, Erkennung, Ermittlung und die Strafverfolgung bei terroristischen Straftaten.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄSSIGKEIT

2.1. Rechtsgrundlage

Rechtsgrundlage ist Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, der die Festlegung von Maßnahmen zur Gewährleistung der Funktionsweise des Binnenmarkts vorsieht.

Artikel 114 ist die geeignete Rechtsgrundlage, um die Bedingungen für Anbieter von Hosting-Diensten im digitalen Binnenmarkt grenzübergreifend zu harmonisieren und um das Problem der unterschiedlichen einzelstaatlichen Bestimmungen, die sonst die Funktionsweise des Binnenmarkts beeinträchtigt hätten, zu lösen. Zudem wird so verhindert, dass in Zukunft die Wirtschaftstätigkeit aufgrund möglicherweise unterschiedlicher Entwicklungen nationaler Gesetze beeinträchtigt wird.

Auf der Grundlage von Artikel 114 AEUV können auch Diensteanbietern mit Sitz außerhalb der EU Pflichten auferlegt werden, sofern sich die Bereitstellung ihres Dienstes auf den Binnenmarkt auswirkt, denn nur so kann das gewünschte Binnenmarktziel erreicht werden.

2.2. Wahl des Instruments

Artikel 114 AEUV gibt dem Gesetzgeber der Union die Möglichkeit, Verordnungen und Richtlinien zu erlassen.

Da vorgesehen ist, Diensteanbietern, die in der Regel ihre Dienste in mehreren Mitgliedstaaten anbieten, Verpflichtungen aufzuerlegen, würde eine unterschiedliche Anwendung dieser Vorschriften die in mehreren Mitgliedstaaten tätigen Anbieter in der Erbringung ihrer Dienste behindern. Bei einer Verordnung kann eine Verpflichtung unionsweit einheitlich auferlegt werden, sie ist unmittelbar anwendbar, schafft Klarheit und größere Rechtssicherheit und vermeidet eine unterschiedliche Umsetzung in den Mitgliedstaaten. Aus diesen Gründen wird eine Verordnung als die am besten geeignete Form für dieses Instrument angesehen.

2.3. Subsidiarität

Angesicht der grenzüberschreitenden Dimension der hier behandelten Probleme müssen die in den Vorschlag aufgenommenen Maßnahmen auf Unionsebene erlassen werden, um die Ziele zu erreichen. Das Internet ist seinem Wesen nach grenzübergreifend, auf in einem Mitgliedstaat gehostete Inhalte kann in der Regel von einem anderen Mitgliedstaat aus zugegriffen werden.

Nach und nach zeichnet sich ein Flickenteppich einzelstaatlicher Vorschriften zum Umgang mit terroristischen Online-Inhalten ab, wodurch auch die Risiken zunehmen. Für die Unternehmen wäre die Einhaltung abweichender Vorschriften eine Belastung, auch entstünden ungleiche Wettbewerbsbedingungen und Sicherheitslücken.

Daher erhöht eine Maßnahme auf EU-Ebene die Rechtssicherheit und die Wirksamkeit der Maßnahmen, die die Anbieter von Hosting-Diensten gegen terroristische Online-Inhalte ergreifen. So können noch mehr Unternehmen tätig werden, auch solche mit Sitz außerhalb der Europäischen Union, und die Integrität des digitalen Binnenmarkts würde gestärkt.

Dies belegt die Notwendigkeit einer EU-Maßnahme, zumal der Europäische Rat im Juni 2018 in seinen Schlussfolgerungen die Kommission aufgefordert hatte, einen Legislativvorschlag zu diesem Bereich vorzulegen.

2.4. Verhältnismäßigkeit

Nach dem Vorschlag sind die Anbieter von Hosting-Diensten verpflichtet, Maßnahmen anzuwenden, mit denen terroristische Inhalte unverzüglich aus ihren Diensten entfernt werden. Mit Kernmerkmalen beschränkt sich der Vorschlag auf das zur Erreichung der Ziele unbedingt Notwendige.

Der Vorschlag berücksichtigt den Aufwand für Anbieter von Hosting-Diensten sowie Vorkehrungen, etwa zum Schutz der Meinungs- und Informationsfreiheit sowie anderer Grundrechte. Das Zeitfenster von einer Stunde für die Entfernung von Inhalten gilt nur für Anweisungen zur Entfernung von Inhalten, deren Illegalität eine zuständige Behörde in einer gerichtlich überprüften Entscheidung festgestellt hat. Für den Umgang mit Meldungen besteht die Pflicht, Maßnahmen vorzusehen, die eine unverzügliche Bewertung terroristischer Inhalte ermöglichen, wobei hier weder eine Pflicht zur Entfernung noch absolute Fristen auferlegt werden. Die endgültige Entscheidung liegt beim Anbieter von Hosting-Diensten. Der Aufwand, der den Unternehmen für die Bewertung von Inhalten entsteht, wird dadurch verringert, dass die zuständigen Behörden der Mitgliedstaaten und die Einrichtungen der Union erläutern müssen, warum sie den Inhalt als terroristischen Inhalt einstufen. Anbieter von Hosting- Diensten müssen gegebenenfalls proaktive Maßnahmen ergreifen, um ihre Dienste vor der Verbreitung terroristischer Inhalte zu schützen. Die konkreten Pflichten im Zusammenhang mit proaktiven Maßnahmen beschränken sich auf solche Anbieter von Hosting- Diensten, die terroristischen Inhalten ausgesetzt sind, was durch den Eingang einer endgültigen Entfernungsanweisung belegt wurde, wobei diese Maßnahmen im Verhältnis zum Risikoniveau sowie zu den Ressourcen des Unternehmens stehen sollten. Die Aufbewahrung der entfernten Inhalte und der entsprechenden Daten ist auf einen Zeitraum beschränkt, der im Verhältnis zu dem Ziel steht, Verwaltungs- oder Gerichtsverfahren zu ermöglichen, sowie zu dem Ziel, Terroranschläge zu verhindern, zu erkennen, zu untersuchen und strafrechtlich zu verfolgen.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

3.1. Konsultation der Interessenträger

Bei der Vorbereitung des vorgeschlagenen Rechtsakts konsultierte die Kommission alle einschlägigen Interessenträger, um deren Ansichten einzuholen und sich eine Meinung über etwaige weitere Schritte zu bilden. Die Kommission führte eine offene Konsultation zu den Maßnahmen durch, mit denen die Wirksamkeit im Umgang mit illegalen Inhalten verbessert werden kann. Sie erhielt 8961 Antworten, davon 8749 von Privatpersonen, 172 von Organisationen, 10 von öffentlichen Verwaltungen und 30 Antworten von sonstigen Stellen. Gleichzeitig wurde eine Eurobarometer-Umfrage mit einer zufälligen Auswahl von 33 500 Personen mit Wohnsitz in der EU zu illegalen Online-Inhalten durchgeführt. Zudem konsultierte die Kommission in den Monaten Mai und Juni 2018 die Behörden der Mitgliedstaaten sowie Anbieter von Hosting-Diensten zu konkreten Maßnahmen im Umgang mit terroristischen Online-Inhalten.

Im Großen und Ganzen brachten die Interessenträger zum Ausdruck, dass terroristische Online-Inhalte ein ernstes gesellschaftliches Problem darstellen, das die Internetnutzer sowie die Geschäftsmodelle der Anbieter von Hosting-Diensten schädigt. Ganz allgemein vertraten 65 % der Teilnehmer an der Eurobarometer[4]-Umfrage die Auffassung, dass das Internet für seine Nutzer nicht sicher ist und 90 % der Teilnehmer hielten es für wichtig, die Verbreitung illegaler Online-Inhalte einzudämmen. Die Konsultation mit den Mitgliedstaaten zeigten, dass freiwillige Vereinbarungen zwar Ergebnisse hervorbringen, doch viele trotzdem bei terroristischen Inhalten verbindliche Vorgaben für notwendig erachten – eine Auffassung, die auch der Europäische Rat in seinen Schlussfolgerungen vom Juni 2018 vertreten hatte. Zwar sprachen sich die Anbieter von Hosting-Diensten für eine Fortsetzung der freiwilligen Maßnahmen aus, doch verwiesen sie auch auf die potenziell negativen Auswirkungen des rechtlichen Flickenteppichs, der sich in der Union abzeichnet.

Viele Interessenträger verwiesen auch auf die Notwendigkeit, dass jeglichen Regulierungsmaßnahmen zur Entfernung von Inhalten, vor allem proaktiven Maßnahmen und strengen Zeitfenstern, Vorkehrungen zum Schutz der Grundrechte, vor allem der Redefreiheit, gegenüberstehen müssen. Die Interessenträger verwiesen auf die notwendigen Maßnahmen im Zusammenhang mit Transparenz, Rechenschaftspflicht und einer manuellen Überprüfung beim Einsatz automatisierter Werkzeuge.

3.2. Folgenabschätzung

Der Ausschuss für Regulierungskontrolle gab eine befürwortende Stellungnahme mit Vorbehalten zur Folgenabschätzung ab und unterbreitete verschiedene Verbesserungsvorschläge[5]. Auf der Grundlage dieser Stellungnahme wurde der Bericht über die Folgenabschätzung geändert, um den wichtigsten Anmerkungen des Ausschusses Rechnung zu tragen, indem das Hauptaugenmerk speziell auf terroristische Inhalte ausgerichtet wurde und auf die Folgen für die Funktionsweise des digitalen Binnenmarkts sowie die Auswirkungen auf die Grundrechte und die Funktionsweise der in den Optionen vorgeschlagenen Schutzvorkehrungen stärker eingegangen wurde.

Werden keine zusätzlichen Maßnahmen getroffen, dürften die freiwilligen Maßnahmen des Ausgangsszenarios weiterlaufen und sich in gewissem Umfang auf die Reduzierung

4 Eurobarometer 469, Illegale Online-Inhalte, Juni 2018.

5 Link zur Stellungnahme des Ausschusses für Regierungskontrolle zur Verordnung.

terroristischer Online-Inhalte auswirken. Allerdings ist nicht davon auszugehen, dass alle Anbieter von Hosting-Diensten, die solchen Inhalten ausgesetzt sind, freiwillige Maßnahmen ergreifen, zudem ist mit einer weiteren rechtlichen Fragmentierung zu rechnen, bei der immer neue Hemmnisse für die grenzüberschreitende Erbringung von Dienstleistungen eingeführt werden. Neben dem Ausgangsszenario wurden drei in ihrer Wirksamkeit abgestufte Hauptoptionen geprüft, die im Hinblick auf die in der Folgenabschätzung genannten Ziele und das übergeordnete Ziel der Reduzierung terroristischer Online-Inhalte in Frage kamen.

Der Anwendungsbereich dieser Pflichten war in allen drei Optionen auf alle Anbieter von Hosting-Diensten ausgerichtet (zielgruppenspezifischer Anwendungsbereich), die ihren Sitz in der EU und in Drittländern haben – sofern sie ihre Dienste in der Union anbieten (geografischer Anwendungsbereich). Angesichts der Art des Problems und der Notwendigkeit, den Missbrauch kleinerer Plattformen zu unterbinden, ist bei keiner Option eine Ausnahmeregelung für KMU vorgesehen. Alle Optionen sehen vor, dass die Anbieter von Hosting-Diensten einen rechtlichen Vertreter in der EU benennen - dies gilt auch für Unternehmen mit Sitz außerhalb der EU – um die Durchsetzbarkeit des EU-Rechts zu gewährleisten. Alle Optionen sehen zudem vor, dass die Mitgliedstaaten Sanktionsmechanismen entwickeln.

Bei allen Optionen ist die Schaffung eines neuen und harmonisierten Systems rechtlicher Anordnungen zur Entfernung terroristischer Online-Inhalte geplant, die von nationalen Behörden ausgestellt und den Anbietern von Hosting-Diensten mit der Aufforderung übermittelt werden, den entsprechenden Inhalt innerhalb einer Stunde zu entfernen. Diese Anordnungen erfordern nicht unbedingt eine Bewertung seitens des Anbieters von Hosting-Diensten, zudem können gegen sie Rechtsmittel eingelegt werden.

Schutzvorkehrungen, vor allem Beschwerdeverfahren und wirksame Rechtsmittel, einschließlich Rechtsbehelfe sowie sonstige Bestimmungen zur Vermeidung eines irrtümlichen Entfernens von nicht terroristischen Inhalten sind – unter Wahrung der Grundrechte – allen drei Optionen gemein. Zudem beinhalten alle Optionen Berichtspflichten in Form öffentlicher Transparenz und Berichten an die Mitgliedstaaten und die Kommission sowie an Behörden bei vermuteten Straftaten. Zudem ist die Pflicht zur Zusammenarbeit zwischen nationalen Behörden, Anbietern von Hosting-Diensten und gegebenenfalls mit Europol vorgesehen.

Die Unterschiede zwischen den drei Optionen bestehen vor allem im Umfang der Begriffsbestimmung terroristischer Inhalte, im Harmonisierungsniveau der Meldungen, im Umfang der proaktiven Maßnahmen, in den Koordinierungspflichten der Mitgliedstaaten sowie in den Vorschriften zur Aufbewahrung von Daten. Option 1 begrenzt den materiellen Anwendungsbereich auf die Verbreitung von Inhalten, die unmittelbar zu terroristischen Handlungen anstiften, und verfolgt damit eine enge Auslegung, während die Optionen 2 und 3 einen umfassenderen Ansatz vorsehen, der auch Material für die Rekrutierung und Schulung einschließt. Bei Option 1 müssten Anbieter von Hosting-Diensten, die terroristischen Inhalten ausgesetzt sind, eine Risikoabschätzung vornehmen, proaktive Maßnahmen zur Eindämmung des Risikos würden jedoch freiwillig bleiben. Nach Option 2 müssen Anbieter von Hosting-Diensten einen Aktionsplan ausarbeiten, der den Einsatz automatisierter Werkzeuge vorsehen kann, mit denen das Wiederhochladen bereits entfernter Inhalte unterbunden wird. Option 3 beinhaltet umfassendere proaktive Maßnahmen, mit denen die Diensteanbieter, die terroristischen Inhalten ausgesetzt sind, auch neues Material identifizieren müssen. Bei allen Optionen stehen die Anforderungen an proaktive Maßnahmen im Verhältnis zum Umfang, in dem der Diensteanbieter terroristischem Material ausgesetzt ist, sowie zu dessen wirtschaftlicher Leistungsfähigkeit. Im Hinblick auf die Meldungen würde Option 1 das

Meldekonzept nicht harmonisieren, während Option 2 dies für Europol erreichen würde und Option 3 auch die Meldungen von Mitgliedstaaten einbezieht. Nach den Optionen 2 und 3 wären die Mitgliedstaaten zur gegenseitigen Information, Koordination und Kooperation verpflichtet und nach Option 3 müssten sie zusätzlich gewährleisten, dass ihre zuständigen Behörden in der Lage sind, terroristische Inhalte aufzuspüren und zu melden. Schließlich umfasst Option 3 auch die Anforderung, zum Schutz vor der irrtümlichen Entfernung von Inhalten und zur Erleichterung strafrechtlicher Untersuchungen Daten aufzubewahren.

Abgesehen von den rechtlichen Bestimmungen sehen alle Optionen eine Reihe flankierender Unterstützungsmaßnahmen vor, mit denen insbesondere die Zusammenarbeit zwischen den nationalen Behörden und Europol sowie mit den Anbietern von Hosting-Diensten erleichtert und Forschung, Entwicklung und Innovation bei der Entwicklung und Einführung technischer Lösungen unterstützt werden sollen. Nach Verabschiedung des Rechtsinstruments könnten zusätzliche Sensibilisierungs- und Unterstützungsmaßnahmen für KMU eingesetzt werden.

Die Folgenabschätzung kam zu dem Schluss, dass eine Reihe von Maßnahmen zur Erreichung der politischen Ziele notwendig ist. Die umfassende Begriffsbestimmung terroristischer Inhalte, die auch besonders schädliches Material einschließt, ist einer engen Definition der Inhalte vorzuziehen (Option 1). Proaktive Pflichten, die sich auf die Unterbindung des Wiederhochladens terroristischer Inhalte beschränken (Option 2) wären im Vergleich zur Verpflichtung, auch neue terroristische Inhalte zu erkennen (Option 3), weniger wirksam. Die Meldebestimmungen sollten sowohl Meldungen von Europol als auch der Mitgliedstaaten umfassen (Option 3) und nicht allein auf Meldungen von Europol beschränkt sein (Option 2), da Meldungen von Mitgliedstaaten einen wichtigen Beitrag im Rahmen der Bemühungen insgesamt darstellen, die Zugänglichkeit terroristischer Online-Inhalte zu erschweren. Solche Maßnahmen müssten zusätzlich zu den allen Optionen gemeinsamen Maßnahmen umgesetzt werden, wozu auch solide Schutzvorkehrungen gegen die irrtümliche Entfernung von Inhalten gehören.

3.3. Grundrechte

Terroristische Online-Propaganda dient dem Zweck, Menschen zu Terroranschlägen anzustiften, indem sie beispielsweise mit detaillierten Anweisungen, wie größtmöglicher Schaden angerichtet werden kann, versorgt werden. Weitere Propaganda wird in der Regel veröffentlicht, nachdem solche Gräueltaten begangen wurden, wobei diese Taten dann verherrlicht und andere aufgefordert werden, diesem Beispiel zu folgen. Diese Verordnung leistet einen Beitrag zum Schutz der öffentlichen Sicherheit, indem die Zugänglichkeit terroristischer Inhalte, die zur Verletzung der Grundrechte auffordern, verringert wird.

Der Vorschlag könnte sich potenziell auf eine Reihe von Grundrechten auswirken:

(a) Rechte des Inhalteanbieters: das Recht auf freie Meinungsäußerung; das Recht auf den Schutz personenbezogener Daten; das Recht auf Wahrung der Privatsphäre und des Familienlebens, den Grundsatz der Nichtdiskriminierung und das Recht auf einen wirksamen Rechtsbehelf;

(b) Rechte des Diensteanbieters: das Recht auf unternehmerische Freiheit; das Recht auf einen wirksamen Rechtsbehelf;

(c) Rechte aller Bürger: Recht auf Meinungs- und Informationsfreiheit.

Im Hinblick auf das einschlägige EU-Recht wurden in den Verordnungsvorschlag angemessene und solide Vorkehrungen aufgenommen, um die Rechte dieser Personen zu schützen.

Hierzu wurde in die Verordnung eine Begriffsbestimmung terroristischer Online-Inhalte aufgenommen, die der Definition terroristischer Straftaten der Richtlinie (EU) 2017/541 entspricht. Diese Definition gilt für Entfernungsanordnungen und Meldungen sowie für proaktive Maßnahmen. Sie gewährleistet, dass nur illegale Inhalte, die der unionweiten Begriffsbestimmung zusammenhängender Straftatbestände genügen, entfernt werden. Darüber hinaus werden mit der Verordnung den Anbietern von Hosting-Diensten allgemeine Sorgfaltspflichten auferlegt, d. h. sie sind verpflichtet, im Umgang mit den von ihnen gespeicherten Inhalten, vor allem bei der Anwendung ihrer eigenen Geschäftsbedingungen und im Hinblick auf die Vermeidung der Entfernung nicht terroristischer Inhalte, mit Sorgfalt und nach den Geboten der Verhältnismäßigkeit und Nichtdiskriminierung vorzugehen.

Konkret ist die Verordnung so ausgelegt, dass die Verhältnismäßigkeit der Maßnahmen mit Blick auf die Wahrung der Grundrechte sichergestellt wird. Hinsichtlich der Entfernungsanordnungen rechtfertigt die Bewertung des Inhalts (einschließlich gegebenenfalls rechtlicher Überprüfungen) durch eine zuständige Behörde das Zeitlimit von einer Stunde für diese Maßnahme. Zudem sind die Meldebestimmungen der Verordnung auf solche Meldungen beschränkt, die von den zuständigen Behörden und den Einrichtungen der Union übermittelt werden und Erläuterungen enthalten, warum der Inhalt als terroristischer Inhalt angesehen werden kann. Für die Entfernung der in einer Meldung genannten Inhalte ist zwar nach wie vor der Anbieter von Hosting-Diensten verantwortlich, doch wird ihm die Entscheidung durch die vorgenannte Bewertung erleichtert.

Bei den proaktiven Maßnahmen sind die Anbieter von Hosting-Diensten für die Identifizierung, Bewertung und Entfernung von Inhalten verantwortlich, die Schutzvorkehrungen, auch manuelle Überprüfungen, vor allem wenn ein größerer Zusammenhang berücksichtigt werden muss, einrichten müssen, damit Inhalte nicht irrtümlich entfernt werden. Anders als beim Ausgangsszenario, bei dem die am stärksten betroffenen Unternehmen automatisierte Werkzeuge ohne öffentliche Aufsicht einsetzen, unterliegt das die Ausgestaltung der Maßnahmen und deren Umsetzung zudem der Berichterstattung an die zuständigen Behörden der Mitgliedstaaten. Diese Pflicht verringert das Risiko irrtümlicher Entfernungen sowohl für Unternehmen, die neue Werkzeuge einsetzen, als auch für die Unternehmen, die diese bereits nutzen. Darüber hinaus sind die Anbieter von Hosting- Diensten verpflichtet, nutzerfreundliche Beschwerdemechanismen einzuführen, damit Inhalteanbieter die Entscheidung zur Entfernung ihrer Inhalte anfechten können, und der breiten Öffentlichkeit Transparenzberichte vorzulegen.

Schließlich sind Anbieter von Hosting-Diensten verpflichtet, Inhalte und damit zusammenhängende Daten für eine Dauer von sechs Monaten aufzubewahren, damit trotz dieser Schutzvorkehrungen irrtümlich entfernte Inhalte wiederhergestellt werden können und die Wirksamkeit von Beschwerde- und Überprüfungsverfahren im Hinblick auf den Schutz der Meinungs- und Informationsfreiheit gewährleistet ist. Auch dient die Aufbewahrung auch Zwecken der Strafverfolgung. Anbieter von Hosting-Diensten müssen technische und organisatorische Vorkehrungen treffen, damit die Daten nicht für andere Zwecke verwendet werden.

Die insbesondere zu Entfernungsanordnungen, Meldungen, proaktiven Maßnahmen und die Aufbewahrung von Daten vorgeschlagenen Maßnahmen sollen nicht nur dazu dienen, die Internetnutzer gegen terroristische Inhalte, sondern auch das Leben der Bürgerinnen und Bürger zu schützen, indem die Zugänglichkeit terroristischer Inhalte verringert wird.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Der Legislativvorschlag für eine Verordnung hat keine Auswirkungen auf den Haushalt der Union.

5. WEITERE ANGABEN

5.1. Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten

Die Kommission wird [innerhalb eines Jahres ab dem Zeitpunkt der Anwendung dieser Verordnung] ein detailliertes Programm für das Monitoring der Ergebnisse und Auswirkungen dieser Verordnung vorlegen. In dem Monitoringprogramm wird festgelegt, mit welchen Indikatoren und Mitteln sowie in welchen Zeitabständen die Daten und sonstigen erforderlichen Nachweise erhoben werden. Es enthält Angaben dazu, welche Maßnahmen von der Kommission und den Mitgliedstaaten für die Erhebung und Auswertung der Daten und anderer Nachweise zur Überwachung der Fortschritte und zur Bewertung dieser Verordnung zu ergreifen sind.

Auf der Grundlage des festgelegten Monitoringprogramms wird die Kommission zwei Jahre nach Inkrafttreten dieser Verordnung einen Bericht über die Durchführung dieser Verordnung vorlegen, der sich auf die von den Unternehmen veröffentlichten Transparenzberichte sowie auf die Informationen der Mitgliedstaaten stützt. Die Kommission wird frühestens vier Jahre nach Inkrafttreten der Verordnung eine Bewertung vornehmen.

Abhängig von den Ergebnissen dieser Bewertung, bei der auch festgestellt wird, ob noch Lücken oder Schwachstellen bestehen, sowie unter Berücksichtigung der technischen Entwicklung wird die Kommission bewerten, ob der Anwendungsbereich der Verordnung erweitert werden muss. Im Bedarfsfall wird die Kommission Vorschläge unterbreiten, um die Verordnung anzupassen.

Die Kommission unterstützt die Durchführung, das Monitoring und die Bewertung der Verordnung durch eine Sachverständigengruppe der Kommission. Die Gruppe wird auch die Zusammenarbeit zwischen den Anbietern von Hosting-Diensten, den Strafverfolgungsbehörden und Europol erleichtern, den Austausch und Verfahrensweisen für die Erkennung und Entfernung terroristischer Inhalte fördern, ihren Sachverstand zur Entwicklung terroristischer Online-Vorgehensweise zur Verfügung stellen sowie gegebenenfalls mit Rat und Orientierungshilfen die Durchführung der Bestimmungen unterstützen.

Die Durchführung der vorgeschlagenen Verordnung kann durch verschiedene Unterstützungsmaßnahmen erleichtert werden – etwa durch die Entwicklung einer Plattform bei Europol für die Koordinierung von Meldungen von Entfernungsanordnungen. Von der EU geförderte Forschungsarbeiten zur Entwicklung der Vorgehensweisen von Terroristen liefern Erkenntnisse und stärken das Bewusstsein aller einschlägigen Interessenträger. Zudem werden mit Horizont 2020 Forschungsarbeiten zur Entwicklung neuer Techniken unterstützt, mit denen beispielsweise das Hochladen terroristischer Inhalte automatisch unterbunden werden kann. Zudem wird die Kommission auch in Zukunft prüfen, wie die zuständigen Behörden und die Anbieter von Hosting-Diensten bei der Durchführung dieser Verordnung mit Finanzierungsinstrumenten der EU unterstützt werden könnten.

5.2. Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags

Artikel 1 enthält den Gegenstand und verweist darauf, dass die Verordnung Vorschriften zur Vermeidung des Missbrauchs von Hosting-Diensten für die Verbreitung terroristischer Online-Inhalte festlegt, worunter auch Sorgfaltspflichten von Anbietern von Hosting-Diensten sowie von den Mitgliedstaaten zu ergreifende Maßnahmen fallen. Er enthält auch Angaben zum geografischen Anwendungsbereich, der sich unabhängig vom Ort ihrer Niederlassung auf die Anbieter von Hosting-Diensten, die ihre Dienste in der Union anbieten, erstreckt.

Artikel 2 enthält die Definition der im Vorschlag verwendeten Begriffe. Er legt auch den Begriff terroristischer Inhalte für präventive Zwecke fest und stützt sich dabei auf die Richtlinie zur Terrorismusbekämpfung, sodass auch Material und Informationen, die zur Begehung terroristischer Straftaten oder zu einem Beitrag zu diesen Straftaten anstiften, diese(n) fördern oder befürworten, die Anweisungen für das Begehen dieser Straftaten enthalten oder die Teilnahme an den Handlungen einer terroristischen Vereinigung fördern, erfasst werden.

Mit Artikel 3 werden den Anbietern von Hosting-Diensten Sorgfaltspflichten auferlegt, denen sie nachkommen müssen, wenn sie unter gebührender Berücksichtigung der betroffenen Grundrechte Maßnahmen auf der Grundlage dieser Verordnung ergreifen. So haben die Anbieter von Hosting-Diensten in ihre Geschäftsbedingungen entsprechende Bestimmungen aufzunehmen und anschließend sicherzustellen, dass sie auch angewandt werden.

Artikel 4 erlegt den Mitgliedstaaten die Pflicht auf, die zuständigen Behörden in die Lage zu versetzen, Entfernungsanordnungen auszustellen. Zudem enthält dieser Artikel die Bestimmung, dass die Anbieter von Hosting-Diensten Inhalte innerhalb einer Stunde nach Eingang einer entsprechenden Anordnung entfernen müssen. Außerdem enthält er die Mindestangaben, die eine Entfernungsanordnung enthalten sollte, sowie Verfahren, nach denen die Anbieter von Hosting-Diensten den ausstellenden Behörden eine Rückmeldung geben bzw. ihnen mitteilen können, wenn sie der Anordnung nicht nachkommen können oder sie weiteren Klärungsbedarf haben. Zudem sind die ausstellenden Behörden nach diesem Artikel verpflichtet, die Behörde, die die Aufsicht über die proaktiven Maßnahmen ausübt, darüber zu informieren, unter die Gerichtsbarkeit welchen Mitgliedstaats der Anbieter der Hosting-Dienste fällt.

Nach Artikel 5 sind die Anbieter von Hosting-Diensten verpflichtet, Maßnahmen festzulegen, die eine unverzügliche Bewertung von Inhalten ermöglichen, die von einer zuständigen Behörde eines Mitgliedstaats oder einer Einrichtung der Union gemeldet wurden, ohne jedoch die Entfernung des gemeldeten Inhalts oder bestimmte Fristen für ein Tätigwerden vorzuschreiben. Außerdem enthält er die Mindestangaben, die Meldungen enthalten sollten, sowie Verfahren, nach denen die Anbieter von Hosting-Diensten den ausstellenden Behörden eine Rückmeldung geben bzw. der Behörde, die die Inhalte gemeldet hatte, mitteilen können, wenn sie weiteren Klärungsbedarf haben.

Nach Artikel 6 sind die Anbieter von Hosting-Diensten verpflichtet, gegebenenfalls wirksame und verhältnismäßige proaktive Maßnahmen zu treffen. In ihm ist ein Verfahren festgelegt, mit dem sichergestellt werden soll, dass bestimmte Anbieter von Hosting-Diensten (z. B. solche, die eine endgültige Entfernungsanordnung erhalten haben) in Abhängigkeit von den auf ihren Diensten exponierten terroristischen Inhalten zusätzliche proaktive Maßnahmen erforderlichenfalls ergreifen, um Risiken abzumildern. Die Anbieter von Hosting-Diensten

sollten mit den zuständigen Behörden mit Blick auf die notwendigen Maßnahmen kooperieren, wobei die zuständigen Behörden dem Diensteanbieter Maßnahmen auferlegen können, sollte keine Einigung zustande kommen. Der Artikel sieht auch ein Überprüfungsverfahren der Verwaltungsentscheidung vor.

Nach Artikel 7 sind die Anbieter von Hosting-Diensten verpflichtet, entfernte Inhalte und damit zusammenhängende Daten sechs Monate lang für Überprüfungsverfahren und Ermittlungszwecke aufzubewahren. Diese Frist kann verlängert werden, damit eine Überprüfung abgeschlossen werden kann. Zudem sind die Anbieter von Hosting-Diensten nach diesem Artikel gehalten, Vorkehrungen zu treffen, damit die aufbewahrten Inhalte und damit zusammenhängende Daten vor einem Zugriff oder einer Weiterverarbeitung für andere Zwecke geschützt werden.

Artikel 8 enthält die Verpflichtung für Anbieter von Hosting-Diensten, ihre Strategien im Umgang mit terroristischen Inhalten zu erläutern und jährlich Transparenzberichte zu den von ihnen in diesem Zusammenhang ergriffenen Maßnahmen zu veröffentlichen.

Artikel 9 sieht konkrete Vorkehrungen für die Nutzung und Umsetzung proaktiver Maßnahmen vor, bei denen automatisierte Werkzeuge eingesetzt werden, damit die Entscheidungen präzise und gut begründet sind.

Artikel 10 verpflichtet die Anbieter von Hosting-Diensten zur Einrichtung von Beschwerdemechanismen für Entfernungen, Meldungen und proaktive Maßnahmen sowie zur umgehenden Prüfung jeder Beschwerde.

Artikel 11 verpflichtet die Anbieter von Hosting-Diensten, den Inhalteanbieter über die Entfernung seiner Inhalte zu informieren, sofern die zuständige Behörde nicht aus Gründen der öffentlichen Sicherheit eine Nichtoffenlegung fordert.

Nach Artikel 12 müssen die Mitgliederstaaten dafür sorgen, dass die zuständigen Behörden über ausreichende Fähigkeiten und Ressourcen verfügen, damit sie ihren in dieser Verordnung festgelegten Zuständigkeiten nachkommen können.

Nach Artikel 13 sind die Mitgliedstaaten verpflichtet, miteinander und gegebenenfalls mit Europol zu kooperieren, um Überschneidungen und Einflussnahmen in laufende Ermittlungen zu vermeiden. Der Artikel eröffnet Mitgliedstaaten und Anbietern von Hosting-Diensten auch die Möglichkeit, spezielle Werkzeuge, auch die von Europol, für die Verarbeitung von und Rückmeldungen zu Entfernungsanordnungen und Meldungen zu nutzen und bei proaktiven Maßnahmen zusammenzuarbeiten. Zudem sind Mitgliedstaaten aufgefordert, geeignete Kommunikationskanäle einzurichten, damit der zeitnahe Austausch von Informationen bei der Durchführung und Durchsetzung der Bestimmungen dieser Verordnung gewährleistet ist. Nach dem Artikel sind Anbieter von Hosting-Diensten zudem verpflichtet, die jeweiligen Behörden zu unterrichten, wenn sie auf Belege für terroristische Straftaten im Sinne von Artikel 3 der Richtlinie (EU) 2017/541 zur Terrorismusbekämpfung stoßen.

Artikel 14 sieht die Einrichtung von Anlaufstellen sowohl durch Anbieter von Hosting-Diensten als auch durch die Mitgliedstaaten vor, um insbesondere bei Meldungen und Entfernungsanordnungen die Kommunikation zwischen ihnen zu erleichtern.

Nach Artikel 15 legen die Mitgliedstaaten den Gerichtsstand für die Zwecke der Aufsicht über die proaktiven Maßnahmen, die Festsetzung von Sanktionen und das Monitoring fest.

Nach Artikel 16 müssen Anbieter von Hosting-Diensten, die keinen Sitz in einem Mitgliedstaat haben, aber Dienste in der Union anbieten, einen rechtlichen Vertreter in der Union benennen.

Nach Artikel 17 müssen Mitgliedstaaten die Behörden festlegen, die für die Ausstellung der Entfernungsanordnungen, die Meldung terroristischer Inhalte, die Aufsicht über die Durchführung der proaktiven Maßnahmen und die Durchsetzung der Verordnung zuständig sind.

In Artikel 18 ist festgelegt, dass die Mitgliedstaaten Sanktionsvorschriften für die Nichteinhaltung sowie die Kriterien festlegen sollen, anhand derer die Mitgliedstaaten die Art und die Höhe der Sanktionen bestimmen. Da es äußerst wichtig ist, die in einer Entfernungsanordnung genannten terroristischen Inhalte unverzüglich zu entfernen, sollten für die systematische Verletzung dieser Anforderung spezielle Vorschriften für die Verhängung finanzieller Sanktionen festgelegt werden.

Artikel 19 ermöglicht ein schnelleres und flexibleres Verfahren mittels delegierter Rechtsakte für die Änderung der Formblätter für die Entfernungsanordnungen sowie die Authentifizierung von Übermittlungskanälen.

In Artikel 20 sind die Bedingungen festgelegt, unter denen die Kommission befugt ist, delegierte Rechtsakte für die notwendigen Änderungen der Formblätter und technischen Anforderungen für Entfernungsanordnungen zu erlassen.

Nach Artikel 21 sind die Mitgliedstaaten verpflichtet, spezifische Angaben im Zusammenhang mit der Anwendung der Verordnung zur Unterstützung der Kommission bei der Wahrnehmung ihrer Aufgaben nach Artikel 23 zu übermitteln. Die Kommission erstellt ein detailliertes Programm zur Überwachung der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung.

Nach Artikel 22 berichtet die Kommission zwei Jahre nach Inkrafttreten der Verordnung über deren Durchführung.

Nach Artikel 23 legt die Kommission frühestens drei Jahre nach Inkrafttreten der Verordnung einen Bewertungsbericht vor.

Nach Artikel 24 tritt die vorgeschlagene Verordnung am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt in Kraft und findet sechs Monate nach ihrem Inkrafttreten Anwendung. Diese Frist wird angesichts der Notwendigkeit der Festlegung von Durchführungsmaßnahmen, aber auch der Dringlichkeit der vollständigen Anwendung der Vorschriften dieser Verordnung vorgeschlagen. Die Frist von sechs Monaten geht von der Annahme aus, dass die Verhandlungen rasch zum Abschluss gebracht werden.

2018/0331 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Verhinderung der Verbreitung terroristischer Online-Inhalte

Ein Beitrag der Europäischen Kommission zur Tagung der Staats- und Regierungschefs vom 19.–20. September 2018 in Salzburg

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[6],

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.

(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.

[6] ABl. C xxx vom xx.xx.xxxx, S. .

(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 der Kommission[7] 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.

(5) Die Anwendung dieser Verordnung sollte die Anwendung des Artikels 14 der Richtlinie 2000/31/EG[8] 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.

(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.

(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

---

[7] 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).

[8] 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).

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, die eine der wesentlichen Grundlagen einer pluralistischen, demokratischen Gesellschaft und einen der grundlegenden Werte der Union darstellt, 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.

(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[9] der Begriff „terroristische Inhalte“ präventiv definiert werden. In Anbetracht der Notwendigkeit, besonders schädliche terroristische Online-Propaganda zu bekämpfen, sollten in der Definition Materialien und Informationen erfasst werden, die zur Begehung terroristischer Straftaten oder zu einem Betrag zu diesen Straftaten anstiften, diese(n) fördern oder befürworten, die Anweisungen für die Begehung solcher Straftaten enthalten oder für die Beteiligung an Handlungen einer terroristischen Vereinigung werben. 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 verbreitet werden, sollten angemessen geschützt werden. Ferner sollte die Formulierung radikaler, polemischer oder kontroverser Ansichten zu sensiblen politischen Fragen in der öffentlichen Debatte nicht als terroristischer Inhalt betrachtet werden.

[9] 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 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 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 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.

(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[10] auf einen oder mehrere Mitgliedstaaten ausrichtet. Andererseits kann die Erbringung der Dienstleistung zum Zwecke der bloßen Einhaltung des in der Verordnung

[10] 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).

(EU) 2018/302 des Europäischen Parlaments und des Rates[11] festgelegten Verbots der Diskriminierung nicht allein aus diesem Grund als Ausrichtung von Tätigkeiten auf ein bestimmtes Gebiet innerhalb der Union betrachtet werden.

(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. Es obliegt den Hostingdiensteanbietern zu entscheiden, ob sie die betreffenden Inhalte entfernen oder den Zugang zu den Inhalten für Nutzer in der Union sperren.

(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[12] erfüllt werden.

(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

---

[11] 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] 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).

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[13] 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 eine geringe Beeinflussung durch terroristische Inhalte.

(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

[13] 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).

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 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 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, 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. Die Hostingdiensteanbieter sollten jährliche Transparenzberichte mit aussagekräftigen Informationen über ihre Maßnahmen im Zusammenhang mit der Erkennung, Ermittlung und Entfernung terroristischer Inhalte veröffentlichen.

(25) Beschwerdeverfahren stellen eine notwendige Schutzvorkehrung gegen die irrtümliche Entfernung von Inhalten dar, 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.

(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 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 bei der Erteilung von Entfernungsanordnungen oder bei Meldungen an die Hostingdiensteanbieter sich gegenseitig informieren und miteinander sowie gegebenenfalls mit Europol koordinieren und kooperieren. 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.

(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, 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[14].

(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 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. 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. 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.

(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.

[14] COM(2018) 225 final.

(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 Regeln für Sanktionen, 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. 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[15] 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.

(41) Die Mitgliedstaaten sollten Informationen über die Umsetzung der Rechtsvorschriften sammeln. Es sollte ein detailliertes Programm zur Überwachung der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung erstellt werden, um die Bewertung zu erleichtern.

(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:

[15] ABl. L 123 vom 12.5.2016, S. 1.

(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.

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

(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;

(5) „terroristische Inhalte“ eine oder mehrere der folgenden Informationen:

(a) der Aufruf zu oder die Befürwortung von terroristischen Straftaten, auch durch ihre Verherrlichung, mit der damit einhergehenden Gefahr, dass solche Taten begangen werden könnten;

(b) die Ermutigung, an terroristischen Straftaten mitzuwirken;

(c) die Förderung der Aktivitäten einer terroristischen Vereinigung, insbesondere durch Ermutigung zur Beteiligung an oder Unterstützung einer terroristischen Vereinigung im Sinne des Artikels 2 Absatz 3 der Richtlinie (EU) 2017/541;

(d) 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 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 zur Verhinderung der Verbreitung terroristischer Inhalte auf und wenden diese an.

Artikel 4
Entfernungsanordnungen

1. Die zuständige Behörde ist befugt, Entscheidungen 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 Erhalt 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;

   (b) eine Darlegung der Gründe, aus denen der Inhalt als terroristischer Inhalt erachtet wird, zumindest durch Bezugnahme auf die in Artikel 2 Absatz 5 aufgeführten Kategorien terroristischer Inhalte;

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

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

(e) Datum und Uhrzeit der Ausstellung;

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

(g) 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 ausführliche Begründung vor, 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 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.

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 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.

Artikel 6
Proaktive Maßnahmen

1. Die Hostingdiensteanbieter ergreifen gegebenenfalls 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 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.

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. 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 Werkzeuge.

2. Die Hostingdiensteanbieter 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 des Hostingdiensteanbieters zur Verhinderung eines erneuten Hochladens von Inhalten, 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 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 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 [vier] Wochen ab dieser Entscheidung, keine Informationen weitergegeben dürfen. 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. Die Mitgliedstaaten und Hostingdiensteanbieter können sich für die Verwendung spezieller Werkzeuge entscheiden, gegebenenfalls auch der von den zuständigen Einrichtungen der Union wie Europol eingeführten Werkzeuge, 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 betreffenden Mitgliedstaat zuständigen Behörden oder die Kontaktstelle nach Artikel 14 Absatz 2 in dem Mitgliedstaat, in dem sie ihre Hauptniederlassung haben oder über einen gesetzlichen Vertreter verfügen. Im Zweifelsfall können die Hostingdiensteanbieter diese Informationen an Europol zur weiteren Bearbeitung übermitteln.

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.

2. Hat ein Hostingdiensteanbieter keinen gesetzlichen Vertreter benannt, so liegt die Gerichtsbarkeit bei allen Mitgliedstaaten.

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.

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 genannten zuständigen Behörden bis zum [*sechs 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 [*sechs 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 Person;

   (d) die Finanzkraft der haftbaren juristischen 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 ausgestellten 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 [sechs 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*