Amtsblatt der Europäischen Union

C 135

Ausgabe in deutscher Sprache

Mitteilungen und Bekanntmachungen

64. Jahrgang

16. April 2021

Inhalt

DE

([1]) Text von Bedeutung für den EWR.

III

(Vorbereitende Rechtsakte)

RAT

STANDPUNKT (EU) Nr. 6/2021 DES RATES IN ERSTER LESUNG

im Hinblick auf den Erlass einer Verordnung des Europäischen Parlaments und des Rates zur Bekämpfung der Verbreitung terroristischer Online-Inhalte

Vom Rat am 16. März 2021 angenommen

(Text von Bedeutung für den EWR)

(2021/C 135/01)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

gemäß dem ordentlichen Gesetzgebungsverfahren [2],

in Erwägung nachstehender Gründe:

(1) Durch diese Verordnung soll das reibungslose Funktionieren des digitalen Binnenmarkts in einer offenen und demokratischen Gesellschaft gewährleistet werden, indem der Missbrauch von Hostingdiensten für terroristische Zwecke bekämpft und ein Beitrag zur öffentlichen Sicherheit in der gesamten Union geleistet wird. Das Funktionieren des digitalen Binnenmarkts sollte verbessert werden, indem die Rechtssicherheit für die Hostingdiensteanbieter erhöht, das Vertrauen der Nutzer in das Online-Umfeld gestärkt und die Schutzvorkehrungen für die Freiheit der Meinungsäußerung, einschließlich der Freiheit, Informationen und Ideen in einer offenen und demokratischen Gesellschaft zu erhalten und weiterzugeben, sowie für die Medienfreiheit und den Medienpluralismus erhöht werden.

(2) Regulatorische Maßnahmen zur Bekämpfung der Verbreitung terroristischer Online-Inhalte sollten durch die Strategien der Mitgliedstaaten zur Bekämpfung des Terrorismus flankiert werden, die unter anderem die Verbesserung der Medienkompetenz und die Stärkung des kritischen Denkens, die Entwicklung von alternativen Narrativen und Gegennarrativen und weitere Initiativen, die darauf abzielen, die Wirkung terroristischer Online-Inhalte sowie die Anfälligkeit für solche Inhalte zu verringern, sowie Investitionen in Sozialarbeit, Deradikalisierungsinitiativen und die Zusammenarbeit mit betroffenen Gemeinschaften einschließen sollten, um eine Radikalisierung in der Gesellschaft auf Dauer zu verhindern.

(3) Die Bekämpfung terroristischer Online-Inhalte, die Teil des umfassenderen Problems illegaler Online-Inhalte sind, erfordert eine Kombination aus legislativen, nichtlegislativen und freiwilligen Maßnahmen, basierend auf der Zusammenarbeit zwischen Behörden und Hostingdiensteanbietern und unter uneingeschränkter Achtung der Grundrechte.

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

[2] Standpunkt des Europäischen Parlaments vom 17. April 2019 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates in erster Lesung vom 16. März 2021. Standpunkt des Europäischen Parlaments vom ... (noch nicht im Amtsblatt veröffentlicht).

(4) Hostingdiensteanbieter, die im Internet aktiv sind, spielen in der digitalen Wirtschaft eine zentrale Rolle, indem sie Unternehmen sowie Bürgerinnen 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 die Dienste von Hostingdiensteanbietern allerdings von Dritten für illegale Aktivitäten im Internet ausgenutzt. Besonders besorgniserregend ist der Missbrauch dieser Dienste durch terroristische Vereinigungen und ihre Unterstützer mit dem Ziel, terroristische Online-Inhalte zu verbreiten und so ihre Botschaften weiterzutragen, Menschen zu radikalisieren und Anhänger anzuwerben sowie terroristische Aktivitäten zu ermöglichen und zu lenken.

(5) Terroristische Online-Inhalte haben sich — wenn auch nicht als einziger Faktor — als Katalysator für die Radikalisierung von Einzelpersonen erwiesen, die zu terroristischen Handlungen führen kann; daher haben diese Inhalte schwerwiegende negative Folgen für Nutzer, Bürgerinnen und Bürger und die Gesellschaft insgesamt, aber auch für die Anbieter von Online-Diensten, die solche Inhalte zur Verfügung stellen, da dies das Vertrauen ihrer Nutzer untergräbt und ihre Geschäftsmodelle schädigt. Die Hostingdiensteanbieter 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 dabei zu helfen, gegen terroristische Inhalte, die durch die Nutzung ihrer Dienste online verbreitet werden, vorzugehen und dabei die grundlegende Bedeutung des Rechts auf freie Meinungsäußerung, einschließlich der Freiheit, Informationen und Ideen in einer offenen und demokratischen Gesellschaft zu erhalten und weiterzugeben, zu berücksichtigen.

(6) Die Bemühungen der Union zur Bekämpfung terroristischer Online-Inhalte durch einen Rahmen für die freiwillige Zusammenarbeit zwischen den Mitgliedstaaten und den Hostingdiensteanbietern begannen 2015. Diese Bemühungen 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. Der Rechtsrahmen soll auf den freiwilligen Bemühungen aufbauen, die durch die Empfehlung (EU) 2018/334 der Kommission ([3]) verstärkt wurden, und entspricht der Forderung des Europäischen Parlaments, die Maßnahmen zur Bekämpfung illegaler und schädlicher Online-Inhalte im Einklang mit dem in der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates ([4]) festgelegten horizontalen Rahmen zu intensivieren, sowie der Forderung des Europäischen Rates, die Erkennung und Entfernung von zu terroristischen Handlungen anstiftenden Online-Inhalten zu verbessern.

(7) Diese Verordnung sollte die Anwendung der Richtlinie 2000/31/EG unberührt lassen. Insbesondere sollten etwaige Maßnahmen, die der Hostingdiensteanbieter im Einklang mit der vorliegenden Verordnung ergriffen hat, darunter auch spezifische Maßnahmen, nicht automatisch dazu führen, dass der Hostingdiensteanbieter den in der Richtlinie vorgesehenen Haftungsausschluss nicht in Anspruch nehmen kann. Darüber hinaus berührt diese Verordnung nicht die Befugnisse der nationalen Behörden und Gerichte, die Haftung von Hostingdiensteanbietern festzustellen, wenn die Voraussetzungen gemäß dieser Richtlinie für den Haftungsausschluss nicht erfüllt sind.

(8) Im Falle eines Widerspruchs zwischen dieser Verordnung und der Richtlinie 2010/13/EU ([5]) in Bezug auf Bestimmungen über audiovisuelle Mediendienste im Sinne von Artikel 1 Absatz 1 Buchstabe a der genannten Richtlinie sollte die Richtlinie 2010/13/EU Vorrang haben. Dies sollte die Verpflichtungen im Rahmen dieser Verordnung, insbesondere bezüglich der Verpflichtungen für Video-Sharing-Plattform-Anbieter, nicht berühren.

(9) In der vorliegenden Verordnung sollten Vorschriften festgelegt werden, mit denen der Missbrauch von Hostingdiensten für die Verbreitung terroristischer Online-Inhalte bekämpft werden soll, um das reibungslose Funktionieren des Binnenmarktes zu gewährleisten. Diese Vorschriften sollten die in der Union geschützten und insbesondere die in der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) garantierten Grundrechte uneingeschränkt achten.

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

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

([5]) Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) (ABl. L 95 vom 15.4.2010, S. 1)

(10) Mit dieser Verordnung soll zum Schutz der öffentlichen Sicherheit beigetragen werden; gleichzeitig enthält sie angemessene und solide Vorkehrungen zum Schutz der Grundrechte, einschließlich des Rechts auf Achtung des Privatlebens, auf den Schutz personenbezogener Daten, auf freie Meinungsäußerung — einschließlich der Freiheit, Informationen zu erhalten und weiterzugeben —, auf unternehmerische Freiheit und auf wirksamen Rechtsbehelf. Zudem ist jegliche Diskriminierung untersagt. Die zuständigen Behörden und Hostingdiensteanbieter sollten nur Maßnahmen ergreifen, die in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sind, wobei der besonderen Bedeutung der Meinungs- und Informationsfreiheit und der Medienfreiheit und des Medienpluralismus, die die wesentlichen Grundlagen einer pluralistischen und demokratischen Gesellschaft und einen der grundlegenden Werte der Union darstellen, Rechnung zu tragen ist. Maßnahmen, die sich auf die Meinungs- und Informationsfreiheit auswirken, sollten streng darauf ausgerichtet sein, die Verbreitung terroristischer Online-Inhalte unter Achtung des Rechts auf den rechtmäßigen Erhalt und die rechtmäßige Weitergabe von Informationen zu bekämpfen, wobei die zentrale Rolle der Hostingdiensteanbieter, öffentliche Debatten sowie die Verbreitung und den Erhalt von Informationen, Meinungen und Ideen nach geltendem Recht zu ermöglichen, zu berücksichtigen ist. Wirksame Maßnahmen zur Bekämpfung terroristischer Online-Inhalte und der Schutz der Meinungs- und Informationsfreiheit sind keine widersprüchlichen, sondern vielmehr einander ergänzende und sich gegenseitig verstärkende Ziele.

(11) 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 bekämpfen, sollte in dieser Verordnung im Einklang mit den Definitionen relevanter Straftatbestände in der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates ([6]) der Begriff „terroristische Inhalte“ präventiv definiert werden. In Anbetracht der Notwendigkeit, besonders schädliche terroristische Online-Propaganda zu bekämpfen, sollten in dieser Definition Materialien erfasst werden, die jemanden zur Begehung terroristischer Straftaten oder zu einem Beitrag zur Begehung dieser Straftaten anstiften oder dazu bestimmten, jemanden zur Beteiligung an Handlungen einer terroristischen Vereinigung zu bestimmen, terroristische Aktivitäten verherrlichen, unter anderem auch durch die Verbreitung von Materialien, die Bilder von terroristischen Anschlägen zeigen. Unter die Definition sollten auch Materialien fallen, die zum Zweck der Begehung oder des Beitrags zur Begehung terroristischer Straftaten Anleitungen zur Herstellung oder Verwendung von Sprengstoffen, Schusswaffen oder anderen Waffen oder schädlichen oder gefährlichen Stoffen sowie chemischen, biologischen, radiologischen und nuklearen Stoffen (CBRN-Stoffen) oder zu anderen spezifischen Methoden oder Verfahren, einschließlich der Auswahl von Anschlagszielen, enthalten. Bei solchen Materialien kann es sich um Texte, Bilder, Tonaufzeichnungen und Videos sowie um Live-Übertragungen terroristischer Straftaten handeln, mit denen die Gefahr einhergeht, dass weitere solcher Taten begangen werden. Bei der Beurteilung, ob es sich bei Materialien 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 Person, Vereinigung oder Organisation, die in der Liste der Union der an terroristischen Handlungen beteiligten Personen, Vereinigungen oder Organisationen aufgenommen wurde und restriktiven Maßnahmen unterliegt, hergestellt wurde, ihr zuzuschreiben ist oder in ihrem Namen verbreitet wird, sollte ein wichtiges Kriterium bei der Beurteilung darstellen.

(12) Materialien, die für Bildungs-, Presse- oder Forschungszwecke oder für künstlerische Zwecke oder zum Zweck der Sensibilisierung gegenüber terroristischen Aktivitäten verbreitet werden, sollten nicht als terroristische Inhalte gelten. Bei der Feststellung, ob es sich bei den von einem Inhalteanbieter bereitgestellten Materialien um „terroristische Inhalte“ im Sinne dieser Verordnung handelt, sollte insbesondere dem Recht auf Meinungs- und Informationsfreiheit, einschließlich der Medienfreiheit und des Medienpluralismus, und der Freiheit von Kunst und Wissenschaft Rechnung getragen werden. Insbesondere in Fällen, in denen der Inhalteanbieter eine redaktionelle Verantwortung trägt, sind Entscheidungen über die Entfernung verbreiteter Materialien unter Berücksichtigung der in einschlägigen Presse- und Medienvorschriften festgelegten journalistischen Standards, die im Einklang mit dem Unionsrecht einschließlich der Charta stehen, zu treffen. Ferner sollte die Formulierung radikaler, polemischer oder kontroverser Ansichten zu sensiblen politischen Fragen in der öffentlichen Debatte nicht als terroristischer Inhalt betrachtet werden.

(13) Zur wirksamen Bekämpfung der Verbreitung terroristischer Online-Inhalte unter Gewährleistung der Achtung des Privatlebens von Einzelpersonen sollte diese Verordnung für Anbieter von Diensten der Informationsgesellschaft gelten, die die durch einen Nutzer des Dienstes bereitgestellten Informationen und Materialien in seinem Auftrag speichern und öffentlich verbreiten, unabhängig davon, ob die Speicherung und öffentliche Verbreitung solcher Informationen und Materialien rein technischer, automatischer und passiver Art ist. Unter dem Begriff „speichern“ ist die Aufbewahrung von Daten im Speicher eines physischen oder virtuellen Servers zu verstehen. Anbieter von „reinen

([6]) 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).

Durchleitungsdiensten“, von „Cachingdiensten“ oder von anderen Diensten, die auf anderen Ebenen der Internet-Infrastruktur geleistet werden, die keine Speicherung beinhalten, wie Register und Registrierungsstellen, sowie Anbieter von Domain-Namen-Systemen (DNS) oder von Zahlungsdiensten oder Anbieter von Schutzdiensten gegen DDoS (Distributed Denial of Service/verteilter Dienstverweigerungsangriff) sollten daher nicht in den Anwendungsbereich dieser Verordnung fallen.

(14) Der Begriff „öffentliche Verbreitung“ sollte die Bereitstellung von Informationen für einen potenziell unbegrenzten Personenkreis umfassen, d. h. die Informationen sollten den Nutzern im Allgemeinen leicht zugänglich gemacht werden, ohne dass weitere Maßnahmen des Inhalteanbieters erforderlich wären, unabhängig davon, ob die Personen tatsächlich auf die betreffenden Informationen zugreifen. Dementsprechend sollte in Fällen, in denen eine Registrierung oder die Aufnahme in eine Nutzergruppe erforderlich ist, um Zugang zu Informationen zu erlangen, nur dann von einer öffentlichen Verbreitung der Informationen ausgegangen werden, wenn die Nutzer, die auf die Informationen zugreifen möchten, automatisch registriert oder aufgenommen werden, ohne eine menschliche Entscheidung oder Auswahl, wem Zugang gewährt wird. Interpersonelle Kommunikationsdienste im Sinne des Artikels 2 Nummer 5 der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates ([7]), wie beispielsweise E-Mail-Dienste oder Privatnachrichten-übermittlungsdienste, sollten nicht in den Anwendungsbereich der vorliegenden Verordnung fallen. Informationen sollten nur dann als im Sinne dieser Verordnung gespeichert und öffentlich verbreitet gelten, wenn dies auf direktes Verlangen des Inhalteanbieters hin geschieht. Folglich sollten Anbieter von Diensten wie Cloud-Infrastrukturen, die auf Verlangen von anderer Seite als von Seiten des Inhalteanbieters erbracht werden und Letzterem nur mittelbar zugutekommen, nicht unter die vorliegende Verordnung fallen. In den Anwendungsbereich der vorliegenden Verordnung sollten beispielsweise Anbieter von Dienstleistungen in sozialen Medien, von Video-, Bild- und Audio-Sharing-Diensten sowie von File-Sharing-Diensten und anderen Cloud-Diensten fallen, sofern diese Dienste dafür genutzt werden, um gespeicherte Informationen auf direktes Verlangen des Inhalteanbieters hin öffentlich zugänglich zu machen. Bietet ein Hostingdiensteanbieter mehrere Dienste an, so sollte diese Verordnung nur auf die in ihren Anwendungsbereich fallenden Dienste angewendet werden.

(15) Terroristische Inhalte werden häufig über Dienste öffentlich verbreitet, die von in Drittländern niedergelassenen Hostingdiensteanbietern bereitgestellt werden. Um die Nutzer in der Union zu schützen und um zu gewährleisten, dass alle im digitalen Binnenmarkt tätigen Hostingdiensteanbieter denselben Anforderungen unterliegen, sollte diese Verordnung für alle Anbieter von relevanten Diensten gelten, die in der Union bereitgestellt werden, unabhängig vom Land der Hauptniederlassung des Diensteanbieters. Ein Hostingdiensteanbieter sollte als Anbieter von Diensten in der Union gelten, wenn er natürliche oder juristische Personen in einem oder mehreren Mitgliedstaaten in die Lage versetzt, seine Dienste in Anspruch zu nehmen, und der Diensteanbieter eine wesentliche Verbindung zu diesem Mitgliedstaat oder diesen Mitgliedstaaten hat.

(16) Eine wesentliche Verbindung zur Union sollte dann als gegeben gelten, wenn der Hostingdiensteanbieter eine Niederlassung in der Union hat, seine Dienste von einer erheblichen Zahl von Nutzern in einem oder mehreren Mitgliedstaaten genutzt werden oder seine Tätigkeiten auf einen oder mehrere Mitgliedstaaten ausgerichtet sind. Die Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten sollte anhand aller relevanten Umstände, einschließlich Faktoren wie der Verwendung einer in dem betreffenden Mitgliedstaat gebräuchlichen Sprache oder Währung oder der Möglichkeit, Waren oder Dienstleistungen aus diesem Mitgliedstaat zu bestellen, bestimmt werden. Ferner ließe sich eine solche Ausrichtung auch von der Verfügbarkeit einer Anwendung im jeweiligen nationalen App-Store, von der Schaltung lokaler Werbung oder Werbung in einer im betreffenden Mitgliedstaat allgemein gebräuchlichen Sprache oder vom Management der Kundenbeziehungen, zum Beispiel durch die Bereitstellung eines Kundendienstes in einer im betreffenden Mitgliedstaat allgemein gebräuchlichen Sprache, ableiten. Das Vorhandensein einer wesentlichen Verbindung sollte auch dann angenommen werden, wenn ein Hostingdiensteanbieter seine Tätigkeit nach Artikel 17 Absatz 1 Buchstabe c der Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates ([8]) auf einen oder mehrere Mitgliedstaaten ausrichtet. Die bloße Zugänglichkeit der Internetseite eines Hostingdiensteanbieters, einer E-Mail-Adresse oder anderer Kontaktdaten in einem oder mehreren Mitgliedstaaten für sich genommen sollte nicht ausreichen, um eine wesentliche Verbindung zu begründen. Zudem sollte die Erbringung einer Dienstleistung zum Zwecke der bloßen Einhaltung des in der Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates ([9]) festgelegten Verbots der Diskriminierung nicht für sich genommen als Begründung einer wesentlichen Verbindung zur Union gelten.

([7]) Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (ABl. L 321 vom 17.12.2018, S. 36).

([8]) 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).

([9]) 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 60I vom 2.3.2018, S. 1).

(17) Das Verfahren und die Verpflichtungen, die sich nach einer Beurteilung durch die zuständigen Behörden aus den Entfernungsanordnungen, mit denen Hostingdiensteanbieter aufgefordert werden, terroristische Inhalte zu entfernen oder den Zugang zu ihnen zu sperren, ergeben, sollten harmonisiert werden. Angesichts der Geschwindigkeit, mit der terroristische Inhalte über Online-Dienste hinweg verbreitet werden, sollte den Hostingdiensteanbietern die Verpflichtung auferlegt werden, dafür zu sorgen, dass die in der Entfernungsanordnung genannten terroristischen Inhalte in allen Mitgliedstaaten innerhalb einer Stunde nach Erhalt der Entfernungsanordnung entfernt werden oder der Zugang dazu gesperrt wird. Von hinreichend begründeten Dringlichkeitsfällen abgesehen sollte die zuständige Behörde dem Hostingdiensteanbieter mindestens 12 Stunden, bevor sie erstmals eine Entfernungsanordnung gegenüber diesem Hostingdiensteanbieter erlässt, Informationen über Verfahren und geltende Fristen bereitstellen. Hinreichend begründete Dringlichkeitsfälle liegen dann vor, wenn der Umstand, dass die Entfernung von Inhalten oder die Sperrung des Zugangs zu den terroristischen Inhalten später als eine Stunde nach Erhalt der Entfernungsanordnung erfolgt, zu einem ernsthaften Schaden führen würde, beispielsweise in Situationen, in denen das Leben oder die körperliche Unversehrtheit einer Person unmittelbar bedroht sind, oder wenn solche Inhalte laufende Ereignisse zeigen, bei denen dem Leben oder der körperlicher Unversehrtheit einer Person Schaden zugefügt wird. Die zuständigen Behörden sollten feststellen, ob Fälle einen solchen Dringlichkeitsfall darstellen und ihre Entscheidung in der Entfernungsanordnung hinreichend begründen. Kann der Hostingdiensteanbieter der Entfernungsanordnung aufgrund des Vorliegens höherer Gewalt oder einer faktischen Unmöglichkeit, einschließlich aus sachlich vertretbaren technischen oder operativen Gründen, nicht innerhalb einer Stunde nach Erhalt Folge leisten, so sollte er die erlassende zuständige Behörde so schnell wie möglich davon in Kenntnis setzen und der Entfernungsanordnung nachkommen, sobald der Sachverhalt behoben ist.

(18) Die Entfernungsanordnung sollte eine Begründung enthalten, in der die Materialien, die entfernt oder gesperrt werden sollen, als terroristischer Inhalt eingestuft werden, sowie ausreichende Informationen zum Identifizieren des Inhalts enthalten — es sollten die exakte URL-Adresse sowie erforderlichenfalls weitere Angaben zur Verfügung gestellt werden, zum Beispiel ein Screenshot des betreffenden Inhalts. Diese Begründung sollte es den Hostingdiensteanbietern und letztendlich auch den Inhalteanbietern ermöglichen, ihr Recht auf wirksamen Rechtsbehelf effektiv wahrzunehmen. Die vorgetragene Begründung sollte nicht die Offenlegung sensibler Informationen nach sich ziehen, wenn dies die laufenden Ermittlungen gefährden könnte.

(19) Die zuständige Behörde sollte die Entfernungsanordnung — durch elektronische Mittel, die einen schriftlichen Nachweis unter Bedingungen ermöglichen, die dem Hostingdiensteanbieter die Feststellung der Authentizität der Anordnung ermöglichen, einschließlich der Richtigkeit des Datums und des Zeitpunkts der Absendung und des Eingangs der Anordnung, gestatten (z. B. über ein gesichertes E-Mail-System oder Plattformen oder sonstige gesicherte Kanäle, einschließlich der vom Hostingdiensteanbieter zur Verfügung gestellten), im Einklang mit dem Unionsrecht zum Schutz personenbezogener Daten — direkt an die vom Hostingdiensteanbieter für die Zwecke dieser Verordnung benannte oder eingerichtete Kontaktstelle übermitteln. Es sollte möglich sein, diese Anforderung unter anderem durch die Verwendung von qualifizierten Diensten für die Zustellung elektronischer Einschreiben gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([10]) zu erfüllen. Befindet sich die Hauptniederlassung des Hostingdiensteanbieters oder ist sein gesetzlicher Vertreter in einem anderen Mitgliedstaat als dem der erlassenden zuständigen Behörde ansässig oder niedergelassen, so ist der zuständigen Behörde dieses Mitgliedstaats gleichzeitig eine Kopie der Entfernungsanordnung zu übermitteln.

(20) Die zuständige Behörde des Mitgliedstaats, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder in dem sein gesetzlicher Vertreter ansässig oder niedergelassen ist, sollte die Möglichkeit haben, die von den zuständigen Behörden eines anderen Mitgliedstaats erlassene Entfernungsanordnung zu überprüfen, um festzustellen, ob sie einen schwerwiegenden oder offenkundigen Verstoß gegen diese Verordnung oder die in der Charta verankerten Grundrechte enthält oder ob dies nicht der Fall ist. Sowohl der Inhalteanbieter als auch der Hostingdiensteanbieter sollten das Recht haben, eine Prüfung durch die zuständige Behörde in dem Mitgliedstaat, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder wo sein gesetzlicher Vertreter ansässig oder niedergelassen ist, zu verlangen. Wird dies verlangt, so sollte die zuständige Behörde verpflichtet, darüber zu befinden, ob die Entfernungsanordnung einen solchen Verstoß enthält oder nicht. Wird in diesem Beschluss ein solcher Verstoß festgestellt, so sollte die Entfernungsanordnung ihre Rechtswirkung verlieren. Die Prüfung sollte schnell durchgeführt werden, um sicherzustellen, dass irrtümlich entfernte oder gesperrte Inhalte so schnell wie möglich wiederhergestellt werden.

([10]) 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).

(21) Hostingdiensteanbieter, die terroristischen Inhalten ausgesetzt sind, sollten — falls sie über Nutzungsbedingungen verfügen — Bestimmungen darin aufnehmen, mit denen sie dagegen vorgehen können, dass ihre Dienste für die öffentliche Verbreitung terroristischer Online-Inhalte missbraucht werden. Sie sollten diese Bestimmungen mit der gebotenen Sorgfalt und auf transparente, verhältnismäßige und diskriminierungsfreie Weise anwenden.

(22) Angesichts des Umfangs des Problems und der Schnelligkeit, die für eine wirksame Ermittlung und Entfernung terroristischer Inhalte erforderlich ist, sind wirksame und verhältnismäßige spezifische Maßnahmen ein wesentliches Element bei der Bekämpfung terroristischer Online-Inhalte. Im Hinblick auf die Verringerung der Zugänglichkeit terroristischer Inhalte in ihren Diensten sollten Hostingdiensteanbieter, die terroristischen Inhalten ausgesetzt sind, 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 spezifische Maßnahmen ergreifen. Hostingdiensteanbieter sollten festlegen, welche geeigneten, wirksamen und verhältnismäßigen spezifischen Maßnahmen ergriffen werden sollten, um terroristische Inhalte ermitteln und gegebenenfalls entfernen zu können. Spezifische Maßnahmen könnten geeignete technische oder operative Maßnahmen oder Kapazitäten wie Ausstattung mit Personal oder technischen Mitteln umfassen, um terroristische Inhalte zu ermitteln und unverzüglich zu entfernen oder zu sperren, sowie Mechanismen für Nutzer zur Meldung oder Kennzeichnung mutmaßlicher terroristischer Inhalte oder andere Maßnahmen, die der Hostingdiensteanbieter für geeignet und wirksam hält, um gegen die Verfügbarkeit terroristischer Inhalte über seine Dienste vorzugehen.

(23) Bei der Durchführung spezifischer Maßnahmen sollten die Hostingdiensteanbieter dafür sorgen, dass das Recht der Nutzer auf Meinungs- und Informationsfreiheit sowie die Medienfreiheit und der Medienpluralismus, die durch die Charta geschützt werden, gewahrt bleiben. Zusätzlich zu den gesetzlich festgelegten Anforderungen, einschließlich der Rechtsvorschriften über den Schutz personenbezogener Daten, sollten die Hostingdiensteanbieter mit der gebotenen Sorgfalt handeln und gegebenenfalls Schutzvorkehrungen treffen, einschließlich durch menschliche Aufsicht und Überprüfung, um unbeabsichtigte oder irrtümliche Entscheidungen zu vermeiden, die dazu führen, dass nicht terroristische Inhalte entfernt oder gesperrt werden.

(24) Der Hostingdiensteanbieter sollte der zuständigen Behörde über die ergriffenen spezifischen Maßnahmen Bericht erstatten, damit diese feststellen 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 gegenüber dem Hostingdiensteanbieter erlassenen Entfernungsanordnungen, der Größe und wirtschaftlichen Leistungsfähigkeit des Hostingdiensteanbieters und der Wirkung seiner Dienste bei der Verbreitung terroristischer Inhalte, z. B. unter Berücksichtigung der Zahl der Nutzer in der Union, sowie der Vorkehrungen, die getroffen wurden, um den Missbrauch seiner Dienste für die Verbreitung terroristischer Online-Inhalte zu bekämpfen.

(25) Ist die zuständige Behörde der Auffassung, dass die getroffenen spezifischen Maßnahmen die Risiken nicht hinreichend bekämpfen, sollte sie zusätzliche geeignete, wirksame und verhältnismäßige spezifische Maßnahmen fordern können. Eine Anordnung, solche zusätzlichen spezifischen Maßnahmen durchzuführen, sollte weder zur Auferlegung einer allgemeinen Pflicht zur Überwachung oder zum aktiven Forschen nach Hinweisen im Sinne des Artikels 15 Absatz 1 der Richtlinie 2000/31/EG, noch zu einer Verpflichtung zur Anwendung automatisierter Werkzeuge (Tools) führen. Hostingdiensteanbieter sollten jedoch die Möglichkeit haben, automatisierte Werkzeuge (Tools) anzuwenden, wenn sie dies für geeignet und erforderlich halten, um den Missbrauch ihrer Dienste für die Verbreitung terroristischer Online-Inhalte wirksam zu bekämpfen.

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

(27) Die Verpflichtung zur Speicherung der Inhalte für Verfahren der behördlichen oder gerichtlichen Überprüfung ist notwendig und gerechtfertigt, da gewährleistet werden muss, dass wirksame Rechtsbehelfe auch für Inhalteanbieter, deren Inhalte entfernt oder gesperrt wurden, zur Verfügung stehen und dass dieser Inhalt je nach dem Ergebnis dieser Verfahren wiederhergestellt wird. Die Verpflichtung zur Speicherung der Materialien für Ermittlungs- oder Strafverfolgungszwecke ist notwendig und gerechtfertigt, da das Material zur Störung oder Verhinderung terroristischer Aktivitäten wertvoll sein könnte. Daher sollte das Speichern entfernter terroristischer Inhalte zu Zwecken der Verhinderung, Erkennung, Ermittlung und Verfolgung terroristischer Straftaten ebenfalls als gerechtfertigt gelten. Terroristische Inhalte und die damit verbundenen Daten sollten nur für den Zeitraum gespeichert werden, der notwendig ist, um es den Strafverfolgungsbehörden zu ermöglichen, diese terroristischen

Inhalte zu überprüfen und zu entscheiden, ob sie für diese Zwecke benötigt werden. Für die Zwecke der Verhinderung, Erkennung, Ermittlung und Verfolgung terroristischer Straftaten sollte sich die Verpflichtung zur Datenspeicherung auf Daten beschränken, die wahrscheinlich eine Verbindung mit terroristischen Straftaten aufweisen und die daher zur Verfolgung terroristischer Straftaten oder zur Verhütung ernsthafter Bedrohungen der öffentlichen Sicherheit beitragen könnten. Wenn Hostingdiensteanbieter insbesondere durch ihre eigenen spezifischen Maßnahmen Materialien entfernen oder den Zugang dazu sperren, sollten sie die zuständigen Behörden unverzüglich über Inhalte in Kenntnis setzen, die Informationen enthalten, die im Zusammenhang mit einer unmittelbaren Bedrohung von Leben oder einer vermuteten terroristischen Straftat stehen.

(28) Um die Verhältnismäßigkeit zu gewährleisten, sollte der Speicherzeitraum auf sechs Monate begrenzt werden, damit Inhalteanbieter ausreichend Zeit haben, behördliche oder gerichtliche Überprüfungsverfahren einzuleiten, und damit die Strafverfolgungsbehörden auf die für die Ermittlung und Verfolgung terroristischer Straftaten relevanten Daten zugreifen können. Dieser Zeitraum sollte jedoch auf Verlangen der zuständigen Behörde oder des zuständigen Gerichts um den erforderlichen Zeitraum verlängert werden können, falls das genannte Verfahren innerhalb des genannten sechsmonatigen Zeitraums zwar eingeleitet, aber nicht abgeschlossen wurde. Die Dauer des Speicherzeitraums sollte außerdem so bemessen sein, dass die Strafverfolgungsbehörden das für die Ermittlungen und die Strafverfolgung erforderliche Material unter Wahrung des Gleichgewichts mit den Grundrechten speichern können.

(29) Diese Verordnung sollte die Verfahrensgarantien oder 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 Unions- oder nationalen Rechtsvorschriften gespeichert werden, nicht berühren.

(30) 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 Bürgerinnen und Bürger in den digitalen Binnenmarkt stärken. Hostingdiensteanbieter, die in einem bestimmten Kalenderjahr aufgrund der vorliegenden Verordnung Maßnahmen ergriffen haben oder solche Maßnahmen ergreifen mussten, sollten jährliche Transparenzberichte mit Informationen über ihre Maßnahmen im Zusammenhang mit der Ermittlung und Entfernung terroristischer Inhalte öffentlich zugänglich machen.

(31) Die zuständigen Behörden sollten jährliche Transparenzberichte veröffentlichen, die Angaben zur Anzahl der Entfernungsanordnungen, zur Anzahl der Fälle, in denen eine Anordnung nicht vollzogen wurde, zur Anzahl der Entscheidungen zu spezifischen Maßnahmen, zur Anzahl der Fälle, die behördlichen oder gerichtlichen Überprüfungsverfahren unterliegen, sowie zur Anzahl der Entscheidungen, durch die Sanktionen verhängt wurden, enthalten.

(32) Das Recht auf einen wirksamen Rechtsbehelf ist in Artikel 19 des Vertrags über die Europäische Union (EUV) und in Artikel 47 der Charta verankert. Jede natürliche oder juristische Person hat das Recht, gegen etwaige aufgrund der vorliegenden Verordnung getroffene Maßnahmen, die sich nachteilig auf ihre Rechte auswirken können, vor dem zuständigen nationalen Gericht einen wirksamen Rechtsbehelf einzulegen. Dieses Recht sollte insbesondere die Möglichkeit für die Hostingdienste- und Inhalteanbieter umfassen, Entfernungsanordnungen oder andere Entscheidungen aufgrund der Prüfung einer Entfernungsanordnung im Rahmen dieser Verordnung vor einem Gericht des Mitgliedstaats, dessen zuständige Behörde die Entfernungsanordnung erlassen oder die Entscheidung getroffen hat, wirksam anzufechten, sowie die Möglichkeit für die Hostingdiensteanbieter, Entscheidungen in Bezug auf spezifische Maßnahmen oder Sanktionen vor einem Gericht des Mitgliedstaats, dessen zuständige Behörden diese Entscheidung getroffen haben, wirksam anzufechten.

(33) Beschwerdeverfahren stellen eine notwendige Schutzvorkehrung gegen die irrtümliche Entfernung oder Sperrung von Online-Inhalten dar, wenn der Inhalt im Rahmen der Meinungs- und Informationsfreiheit geschützt ist. 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 oder gesperrte Inhalte wiederherstellen müssen, sollte die Möglichkeit unberührt lassen, dass die Hostingdiensteanbieter ihre Nutzungsbedingungen durchsetzen können.

(34) Wirksame Rechtsbehelfe gemäß Artikel 19 EUV und Artikel 47 der Charta setzen voraus, dass die Inhalteanbieter in Erfahrung bringen können, warum die von ihnen bereitgestellten Inhalte entfernt oder der Zugang zu ihnen gesperrt wurden. Zu diesem Zweck sollte der Hostingdiensteanbieter dem Inhalteanbieter Informationen zur Anfechtung der Entfernung oder Sperrung zur Verfügung stellen. Je nach den Umständen könnten Hostingdiensteanbieter Inhalte, die entfernt oder gesperrt wurden, durch einen Hinweis ersetzen, dass die Inhalte im Einklang mit der vorliegenden Verordnung entfernt oder gesperrt wurden. Auf Anfrage des Inhalteanbieters sollten weitere Informationen über die Gründe für die Entfernung oder Sperrung und die Rechtsbehelfe gegen die Entfernung oder Sperrung bereitgestellt werden. Sind die zuständigen Behörden der Auffassung, dass es aus Gründen der öffentlichen Sicherheit, auch im Rahmen einer Ermittlung, unangemessen oder kontraproduktiv ist, den Inhalteanbieter unmittelbar von der Entfernung oder Sperrung in Kenntnis zu setzen, so sollten sie den Hostingdiensteanbieter hierüber informieren.

(35) Für die Zwecke dieser Verordnung sollten die Mitgliedstaaten zuständige Behörden benennen. Dies sollte nicht die Einrichtung einer neuen Behörde erfordern und es sollte möglich sein, eine bereits bestehende Stelle mit den in dieser Verordnung festgelegten Aufgaben zu betrauen. Gemäß dieser Verordnung sollte es vorgeschrieben sein, dass die Behörden zu benennen sind, die für den Erlass von Entfernungsanordnungen, die Überprüfung von Entfernungsanordnungen, die Aufsicht über spezifische Maßnahmen und die Verhängung von Sanktionen zuständig sind, während es für jeden Mitgliedstaat gestattet sein sollte, zu entscheiden, wie viele zuständige Behörden er damit betraut und ob diese der Verwaltung, Strafverfolgung oder Justiz zugehörig sein sollen. Die Mitgliedstaaten sollten sicherstellen, dass die zuständigen Behörden ihre Aufgaben auf objektive und nicht diskriminierende Weise erfüllen und bei der Wahrnehmung der Aufgaben gemäß dieser Verordnung keine Weisungen von anderen Stellen einholen oder entgegennehmen. Dies sollte einer Aufsicht im Einklang mit dem nationalen Verfassungsrecht nicht entgegen stehen. Die Mitgliedstaaten sollten der Kommission die nach dieser Verordnung als zuständig bestimmten Behörden mitteilen, und die Kommission sollte im Internet ein Online-Register der jeweils zuständigen Behörden veröffentlichen. Dieses Online-Register sollte leicht zugänglich sein, damit die Hostingdiensteanbieter die Echtheit von Entfernungsanordnungen schnell prüfen können.

(36) Um Doppelarbeit und eine gegenseitige Behinderung bei Ermittlungen zu vermeiden und den Aufwand für die betroffenen Hostingdiensteanbieter so gering wie möglich zu halten, sollten die zuständigen Behörden Informationen austauschen und sich untereinander sowie gegebenenfalls mit Europol abstimmen und zusammenarbeiten, bevor sie Entfernungsanordnungen erlassen. Wenn sie über den Erlass einer Entfernungsanordnung entscheidet, sollte die zuständige Behörde Benachrichtigungen zu konfligierenden Ermittlungsinteressen gebührend berücksichtigen (Konfliktvermeidung). Wenn eine zuständige Behörde von der zuständigen Behörde eines anderen Mitgliedstaats über eine bereits bestehende Entfernungsanordnung informiert wird, sollte sie keine Entfernungsanordnung zum gleichen Sachverhalt erlassen. Bei der Umsetzung der Bestimmungen dieser Verordnung könnte Europol im Einklang mit seinem derzeitigen Mandat und bestehenden Rechtsrahmen Unterstützung leisten.

(37) Um die wirksame und ausreichend kohärente Durchführung spezifischer Maßnahmen seitens der Hostingdiensteanbieter zu gewährleisten, sollten sich die zuständigen Behörden in Bezug auf den Austausch mit Hostingdiensteanbietern hinsichtlich Entfernungsanordnungen und der Ermittlung, Umsetzung und Bewertung spezifischer Maßnahmen untereinander abstimmen und zusammenarbeiten. Eine solche Abstimmung und Zusammenarbeit ist auch bezüglich anderer Maßnahmen zur Durchführung dieser Verordnung, auch hinsichtlich der Annahme von Vorschriften über Sanktionen und der Verhängung von Sanktionen, erforderlich. Die Kommission sollte diese Abstimmung und Zusammenarbeit erleichtern.

(38) Es ist von wesentlicher Bedeutung, dass die zuständige Behörde des für die Verhängung der Sanktionen zuständigen Mitgliedstaats umfassend über den Erlass von Entfernungsanordnungen sowie den anschließenden Austausch zwischen dem Hostingdiensteanbieter und den zuständigen Behörden in anderen Mitgliedstaaten unterrichtet ist. Zu diesem Zweck sollten die Mitgliedstaaten geeignete und sichere Kommunikationskanäle oder -mechanismen vorsehen, die die fristgerechte Übermittlung der relevanten Informationen ermöglichen.

(39) Um den schnellen Austausch der zuständigen Behörden untereinander und mit den Hostingdiensteanbietern zu erleichtern und Doppelarbeit zu vermeiden, sollten die Mitgliedstaaten aufgefordert werden, die speziell dafür von Europol entwickelten Werkzeuge wie die aktuelle Verwaltungsanwendung für die Meldung von Internetinhalten (Internet Referral Management application) oder deren Nachfolger zu nutzen.

(40) Meldungen seitens der Mitgliedstaaten und seitens Europol haben sich als eine wirksame und schnelle Möglichkeit erwiesen, um Hostingdiensteanbieter auf spezifische Inhalte aufmerksam zu machen, die über ihre Dienste verfügbar sind, und sie so in die Lage zu versetzen, schnell zu reagieren. Neben den Entfernungsanordnungen sollten solche Meldungen als Mechanismus, mit dem Hostingdiensteanbieter auf Informationen aufmerksam gemacht werden, die als terroristische Inhalte gelten könnten, damit sie die Vereinbarkeit dieser Inhalte mit ihren Nutzungsbedingungen freiwillig prüfen können, weiterhin verfügbar sein. Die endgültige Entscheidung darüber, ob Inhalte aufgrund der Nichtvereinbarkeit mit ihren Nutzungsbedingungen entfernt werden oder nicht, liegt beim Hostingdiensteanbieter. Das in der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates ([11]) festgelegte Mandat von Europol sollte von der vorliegenden Verordnung unberührt bleiben. Daher sollten die Bestimmungen dieser Verordnung keinesfalls dahin gehend ausgelegt werden, dass sie die Mitgliedstaaten und Europol daran hindern würden, Meldungen als Instrument zur Bekämpfung terroristischer Online-Inhalte zu nutzen.

(41) Angesichts der besonders schwerwiegenden Folgen bestimmter terroristischer Online-Inhalte sollten die Hostingdiensteanbieter unverzüglich die einschlägigen Behörden des betreffenden Mitgliedstaats oder die zuständigen Behörden des Mitgliedstaats, in dem sie niedergelassen sind oder über einen gesetzlichen Vertreter verfügen, über terroristische Inhalte unterrichten, die im Zusammenhang mit einer unmittelbaren Bedrohung von Leben oder einer vermuteten terroristischen Straftat stehen. Um die Verhältnismäßigkeit zu gewährleisten, sollte diese Verpflichtung auf terroristische Straftaten im Sinne von Artikel 3 Absatz 1 der Richtlinie (EU) 2017/541 beschränkt werden. Diese Informationspflicht sollte nicht bedeuten, dass sich die Hostingdiensteanbieter aktiv um Nachweise einer solchen unmittelbaren Bedrohung von Leben oder einer vermuteten terroristischen Straftat bemühen müssen. Als betreffender Mitgliedstaat sollte der Mitgliedstaat gelten, der für die Ermittlung und strafrechtliche Verfolgung der genannten terroristischen Straftaten zuständig ist, und zwar auf der Grundlage der Staatsangehörigkeit des Täters bzw. des potenziellen Opfers der Straftat oder des Erfolgsorts der terroristischen Handlung. Im Zweifelsfall sollten Hostingdiensteanbieter die Informationen an Europol übermitteln, das entsprechend seinem Mandat die entsprechenden Folgemaßnahmen ergreift, auch durch die Weiterleitung dieser Informationen an die zuständigen nationalen Behörden. Die zuständigen Behörden der Mitgliedstaaten sollten die Möglichkeit haben, solche Informationen zu nutzen, um Ermittlungsmaßnahmen zu ergreifen, die nach den Unions- oder nationalen Rechtsvorschriften zur Verfügung stehen.

(42) Die Hostingdiensteanbieter sollten Kontaktstellen benennen oder einrichten, um die unverzügliche Bearbeitung von Entfernungsanordnungen zu erleichtern. Die Kontaktstelle sollte nur operativen Zwecken dienen. Die Kontaktstelle sollte in einer speziellen — internen oder ausgelagerten — Einrichtung bestehen, die die elektronische Übermittlung von Entfernungsanordnungen ermöglicht, sowie technisch oder personell so ausgestattet ist, dass eine unverzügliche Bearbeitung solcher Anordnungen möglich ist. Die Kontaktstelle muss sich nicht in der Union befinden. Es steht dem Hostingdiensteanbieter frei, eine bestehende Kontaktstelle zum Zwecke dieser Verordnung zu benennen, sofern die 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, sollte die Kontaktstelle eines Hostingdiensteanbieters, der terroristischen Inhalten ausgesetzt ist, ständig rund um die Uhr erreichbar sein. In den Informationen über die Kontaktstelle sollte die Sprache angegeben werden, in der die Kontaktstelle erreicht 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 Unionsorgane, in der ihre Nutzungsbedingungen verfügbar sind, zu ermöglichen.

(43) Da für Hostingdiensteanbieter 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 er seinen Hauptsitz hat oder sein gesetzlicher Vertreter ansässig oder niedergelassen ist. Dies sollte unbeschadet der Zuständigkeitsvorschriften gelten, die für die Zwecke von Entfernungsanordnungen und Entscheidungen aufgrund der Prüfung von Entfernungsanordnungen gemäß dieser Verordnung festgelegt wurden. In Bezug auf einen Hostingdiensteanbieter, der nicht in der Union niedergelassen ist und keinen gesetzlichen Vertreter benennt, sollte jeder Mitgliedstaat dennoch zuständig und in der Lage sein, Sanktionen zu verhängen, sofern der Grundsatz „ne bis in idem“ eingehalten wird.

([11]) 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).

(44) 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. Es sollte für die Hostingdiensteanbieter zum Zwecke dieser Verordnung möglich sein, einen bereits für andere Aufgaben benannten gesetzlichen Vertreter zu benennen, wenn dieser in der Lage ist, die Aufgaben wie in dieser Verordnung dargelegt auszuführen. Der gesetzliche Vertreter sollte befugt sein, im Namen des Hostingdiensteanbieters zu handeln.

(45) Sanktionen sind erforderlich, damit die wirksame Umsetzung dieser Verordnung durch die Hostingdiensteanbieter sichergestellt ist. Die Mitgliedstaaten sollten für Sanktionen, bei denen es sich um verwaltungs- oder strafrechtliche Sanktionen handeln kann, Regeln sowie gegebenenfalls auch Leitlinien für die Verhängung von Geldbußen, erlassen. Verstöße könnten in Einzelfällen mit Sanktionen belegt werden, während gleichzeitig der Grundsatz „ne bis in idem" sowie die Verhältnismäßigkeit gewahrt bleiben und sichergestellt wird, dass solche Sanktionen systematischen Verstößen Rechnung tragen. Sanktionen können unterschiedliche Formen annehmen, darunter die förmliche Verwarnung bei geringfügigen Verstößen oder finanzielle Sanktionen bei schwerwiegenderen oder systematischen Verstößen. Besonders schwere Sanktionen sollten für den Fall verhängt werden, dass der Hostingdiensteanbieter terroristische Inhalte systematisch oder fortwährend nicht innerhalb einer Stunde nach Eingang einer Entfernungsanordnung entfernt oder sperrt. Um Rechtssicherheit zu gewährleisten, sollte in dieser Verordnung festgelegt werden, welche Verstöße mit Sanktionen belegt werden können und welche Umstände bei der Bewertung der Art und Höhe der Sanktionen relevant sind. Bei der Entscheidung, ob finanzielle Sanktionen verhängt werden sollen, sollten die finanziellen Mittel des Hostingdiensteanbieter gebührend berücksichtigt werden. Darüber hinaus sollte die zuständige Behörde berücksichtigen, ob es sich bei dem Hostingdiensteanbieter um ein Start-up-Unternehmen, Kleinstunternehmen oder ein kleines oder mittleres Unternehmen im Sinne der Definition in der Empfehlung 2003/361/EG der Kommission ([12]) handelt. Weitere Umstände wie die Frage, ob das Verhalten des Hostingdiensteanbieters objektiv unvorsichtig oder verwerflich war, oder ob der Verstoß fahrlässig oder vorsätzlich begangen wurde, sollten ebenfalls berücksichtigt werden. Die Mitgliedstaaten sollten sicherstellen, dass Sanktionen bei Verstößen gegen diese Verordnung nicht dazu führen, dass nicht terroristische Materialien entfernt werden.

(46) Die Verwendung standardisierter Formulare erleichtert die Zusammenarbeit und den Informationsaustausch zwischen den zuständigen Behörden und den Hostingdiensteanbietern, sodass sie schneller und wirksamer kommunizieren können. Besonders wichtig ist es, nach Eingang einer Entfernungsanordnung unverzügliches Handeln zu gewährleisten. Solche Formulare senken die Übersetzungskosten und tragen zu einem höheren Standard des Verfahrens bei. Rückmeldungsformulare ermöglichen einen standardisierten Informationsaustausch, was besonders wichtig ist, wenn die Hostingdiensteanbieter der Entfernungsanordnung nicht nachkommen können. Mithilfe authentifizierter Übertragungskanäle kann die Echtheit der Entfernungsanordnung, einschließlich der Richtigkeit des Datums und des Zeitpunkts der Absendung und des Eingangs der Anordnung, gewährleistet werden.

(47) Um erforderlichenfalls eine schnelle 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 der vorliegenden 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 ([13]) niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, 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 Vorbereitung der delegierten Rechtsakte befasst sind.

(48) Die Mitgliedstaaten sollten Informationen über die Umsetzung der Verordnung sammeln. Die Mitgliedstaaten sollten die Transparenzberichte der Hostingdiensteanbieter nutzen können und diese, wo notwendig, durch ausführlichere Informationen, wie beispielsweise ihre eigenen Transparenzberichte gemäß dieser Verordnung, ergänzen. Es sollte ein detailliertes Programm zur Überwachung der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung aufgestellt werden, um die Bewertung der Durchführung dieser Verordnung zu erleichtern.

([12]) Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

([13]) ABl. L 123 vom 12.5.2016, S. 1.

(49) Anhand der Ergebnisse und Schlussfolgerungen des Umsetzungsberichts und der Ergebnisse der Überwachung sollte die Kommission innerhalb von drei Jahren nach dem Tag ihres Inkrafttretens eine Bewertung dieser Verordnung vornehmen. Die Bewertung sollte sich auf die Kriterien Effizienz, Erforderlichkeit, Wirksamkeit, Verhältnismäßigkeit, Relevanz, Kohärenz und Unionsmehrwert stützen. Bewertet werden sollte die Funktionsweise der verschiedenen in der Verordnung festgelegten operativen und technischen Maßnahmen, einschließlich der Wirksamkeit von Maßnahmen zur Verbesserung der Erkennung, Ermittlung und Entfernung terroristischer Online-Inhalte, der Wirksamkeit der Schutzvorkehrungen sowie der Auswirkungen auf potenziell beeinträchtigte Grundrechte, darunter die Meinungs- und Informationsfreiheit, die Medienfreiheit und der Medienpluralismus, die unternehmerische Freiheit, das Recht auf Privatsphäre und den Schutz personenbezogener Daten. Außerdem sollte die Kommission die Auswirkungen auf potenziell beeinträchtigte Interessen Dritter bewerten.

(50) Da das Ziel dieser Verordnung, nämlich die Gewährleistung eines reibungslosen Funktionierens des digitalen Binnenmarkts durch die Bekämpfung der Verbreitung terroristischer Online-Inhalte, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann und daher vielmehr wegen des Umfangs und der Wirkungen auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 EUV 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 Bekämpfung des Missbrauchs von Hostingdiensten zur öffentlichen Verbreitung terroristischer Online-Inhalte festgelegt, insbesondere:

a) angemessene und verhältnismäßige Sorgfaltspflichten, die von den Hostingdiensteanbietern anzuwenden sind, um die öffentliche Verbreitung terroristischer Inhalte durch ihre Dienste zu bekämpfen und erforderlichenfalls die unverzügliche Entfernung solcher Inhalte zu gewährleisten oder den Zugang zu ihnen zu verhindern;

b) Maßnahmen, die von den Mitgliedstaaten im Einklang mit dem Unionsrecht und vorbehaltlich angemessener Garantien zum Schutz der Grundrechte, insbesondere der Meinungs- und Informationsfreiheit in einer offenen und demokratischen Gesellschaft, umzusetzen sind, um

   i) terroristische Inhalte zu ermitteln und deren unverzügliche Entfernung durch die Hostingdiensteanbieter sicherzustellen und

   ii) die Zusammenarbeit unter den zuständigen Behörden der Mitgliedstaaten, den Hostingdiensteanbietern und gegebenenfalls Europol zu erleichtern.

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

(3) Materialien, die für Bildungs-, Presse-, Forschungszwecke oder künstlerische Zwecke oder für die Zwecke der Verhütung oder Bekämpfung des Terrorismus öffentlich verbreitet werden, einschließlich der Materialien, die eine Formulierung polemischer oder kontroverser Ansichten in der öffentlichen Debatte darstellen, gelten nicht als terroristische Inhalte. Im Rahmen einer Bewertung wird der wahre Zweck dieser Verbreitung ermittelt und geprüft, ob Materialien für die genannten Zwecke öffentlich verbreitet werden.

(4) Diese Verordnung berührt nicht die Pflicht, die in Artikel 6 EUV verankerten Rechte, Freiheiten und Grundsätze zu achten, und gilt unbeschadet der Grundprinzipien der Meinungs- und Informationsfreiheit einschließlich der Medienfreiheit und des Medienpluralismus.

(5) Die Richtlinien 2000/31/EG und 2010/13/EU bleiben von dieser Verordnung unberührt. Für audiovisuelle Mediendienste im Sinne des Artikels 1 Absatz 1 Buchstabe a der Richtlinie 2010/13/EU hat die Richtlinie 2010/13/EU Vorrang.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Hostingdiensteanbieter“ einen Anbieter von Diensten gemäß Artikel 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ([14]), die darin bestehen, die durch einen Inhalteanbieter bereitgestellten Informationen im Auftrag eines Inhalteanbieters zu speichern;

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

3. „öffentliche Verbreitung “ die Bereitstellung von Informationen im Auftrag eines Inhalteanbieters für einen potenziell unbegrenzten Personenkreis;

4. „in der Union Dienstleistungen anbieten“ die Befähigung von natürlichen oder juristischen Personen in einem oder mehreren Mitgliedstaaten zur Nutzung der Dienste eines Hostingdiensteanbieters, der eine wesentliche Verbindung zu diesem Mitgliedstaat oder diesen Mitgliedstaaten hat.

5. „wesentliche Verbindung“ eine Verbindung eines Hostingdiensteanbieters mit einem oder mehreren Mitgliedstaaten entweder aufgrund seiner Niederlassung in der Union oder anhand spezifischer faktengestützter Kriterien, wie

   a) eine erhebliche Zahl von Nutzern seiner Dienstleistungen in einem oder mehreren Mitgliedstaaten oder

   b) die Ausrichtung seiner Tätigkeiten auf einen oder mehrere Mitgliedstaaten.

6. „terroristische Straftaten“ Straftaten im Sinne des Artikels 3 der Richtlinie (EU) 2017/541;

7. „terroristische Inhalte“ eines oder mehrere der folgenden Materialien, die Folgendes beinhalten oder bewirken:

   a) die Anstiftung zur Begehung einer der in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten Straftaten, wenn durch solches Material direkt oder indirekt, z. B. durch die Verherrlichung terroristischer Handlungen, die Begehung terroristischer Straftaten befürwortet wird, mit der damit einhergehenden Gefahr, dass eine oder mehrere solche Taten begangen werden könnten;

   b) die Bestimmung eine Person oder einer Gruppe von Personen zur Begehung einer der in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten Straftaten oder zum Beitragen an der Begehung;

   c) die Bestimmung eine Person oder eine Gruppe von Personen zur Beteiligung an Handlungen einer terroristischen Vereinigung im Sinne des Artikels 4 Buchstabe b der Richtlinie (EU) 2017/541;

   d) die Unterweisung in der Herstellung oder im Gebrauch von Sprengstoffen, Schuss oder sonstigen Waffen oder schädlichen oder gefährlichen Stoffen beziehungsweise Unterweisung in anderen spezifischen Methoden oder Verfahren mit dem Ziel, eine der in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten terroristischen Straftaten zu begehen oder zu deren Begehung beizutragen;

   e) eine Drohung, eine der in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten Straftaten zu begehen;

([14]) Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

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

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

Abschnitt II

Maßnahmen zur Bekämpfung der Verbreitung terroristischer Online-Inhalte

Artikel 3

Entfernungsanordnungen

(1) Die zuständige Behörde jedes Mitgliedstaats ist befugt, eine Entfernungsanordnung zu erlassen, mit der die Hostingdiensteanbieter verpflichtet werden, in allen Mitgliedstaaten terroristische Inhalte zu entfernen oder den Zugang zu terroristischen Inhalten zu sperren.

(2) Wenn eine zuständige Behörde zuvor noch keine Entfernungsanordnung an einen Hostingdiensteanbieter erlassen hat, unterrichtet die Behörde diesen Hostingdiensteanbieter mindestens 12 Stunden vor Erlass der Entfernungsanordnung über die geltenden Verfahrensweisen und die Fristen.

Unterabsatz 1 gilt nicht in hinreichend begründeten Dringlichkeitsfällen.

(3) Die Hostingdiensteanbieter entfernen die terroristischen Inhalte oder sperren den Zugang zu terroristischen Inhalten in allen Mitgliedstaaten schnellstmöglich, in jedem Fall aber innerhalb einer Stunde nach Erhalt der Entfernungsanordnung.

(4) Die zuständigen Behörden erlassen Entfernungsanordnungen unter Verwendung des Formulars in Anhang I. Entfernungsanordnungen müssen folgende Angaben enthalten:

a) Angaben zur Identifizierung der zuständigen Behörde, die die Entfernungsanordnung erlassen hat, und die Authentifizierung der Entfernungsanordnung durch diese zuständige Behörde;

b) eine hinreichend detaillierte Darlegung der Gründe, aus denen der Inhalt als terroristischer Inhalt erachtet wird, und eine Bezugnahme auf die in Artikel 2 Absatz 7 aufgeführten einschlägigen Arten von Materialien;

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

d) eine Bezugnahme auf die vorliegende Verordnung als Rechtsgrundlage der Entfernungsanordnung;

e) Datum, Uhrzeit und elektronische Signatur der die Entfernungsanordnung erlassenden Behörde;

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

g) sofern notwendig und verhältnismäßig, die Entscheidung nach Artikel 11 Absatz 3, dass keine Informationen über die Entfernung oder die Sperrung terroristischer Inhalte weitergegeben werden dürfen.

(5) Die zuständige Behörde richtet die Entfernungsanordnung an die Hauptniederlassung des Hostingdiensteanbieters oder an den seinen nach Artikel 17 benannten gesetzlichen Vertreter.

Die zuständige Behörde übermittelt der Kontaktstelle gemäß Artikel 15 Absatz 1 die Entfernungsanordnung durch elektronische Mittel, 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) Der Hostingdiensteanbieter unterrichtet die zuständige Behörde unverzüglich über die Entfernung der terroristischen Inhalte oder die Sperrung der terroristischen Inhalte in allen Mitgliedstaaten unter Verwendung des Formulars in Anhang II und gibt dabei insbesondere den Zeitpunkt der Entfernung oder der Sperrung an.

(7) Kann der Hostingdiensteanbieter der Entfernungsanordnung aufgrund höherer Gewalt oder einer faktischen Unmöglichkeit, die dem Hostingdiensteanbieter nicht angelastet werden kann — einschließlich sachlich begründeter technischer oder betrieblicher Gründe —, nicht nachkommen, so teilt er dies der zuständigen Behörde, die die Entfernungsanordnung erlassen hat, unverzüglich mit und legt unter Verwendung des Formulars in Anhang III die Gründe hierfür dar.

Die in Absatz 3 genannte Frist beginnt, sobald die in Unterabsatz 1 des vorliegenden Absatzes angeführten Gründe nicht mehr vorliegen.

(8) Kann der Hostingdiensteanbieter der Entfernungsanordnung nicht nachkommen, weil diese offensichtliche Fehler oder unzureichende Informationen enthält, um die Anordnung auszuführen, so teilt er dies der zuständigen Behörde, die die Entfernungsanordnung erlassen hat, unverzüglich mit und ersucht unter Verwendung des Formulars in Anhang III um die notwendige Klarstellung.

Die in Absatz 3 genannte Frist beginnt, sobald der Hostingdiensteanbieter die notwendige Klarstellung erhalten hat.

(9) Eine Entfernungsanordnung wird nach Ablauf der Rechtsbehelfsfrist rechtskräftig, wenn kein Rechtsbehelf nach nationalem Recht eingelegt wurde oder wenn die Entfernungsanordnung nach Einlegung eines Rechtsbehelfs bestätigt wurde.

Wenn die Entfernungsanordnung rechtskräftig wird, unterrichtet die zuständige Behörde, die die Entfernungsanordnung erlassen hat, die nach Artikel 12 Absatz 1 Buchstabe c zuständige Behörde des Mitgliedstaats, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder in dem der gesetzliche Vertreter ansässig oder niedergelassen ist, über diese Tatsache.

Artikel 4

Verfahren für grenzüberschreitende Entfernungsanordnungen

(1) Hat der Hostingdiensteanbieter, vorbehaltlich des Artikels 3, seine Hauptniederlassung nicht in dem Mitgliedstaat der zuständigen Behörde, die die Entfernungsanordnung erlassen hat, oder verfügt er in diesem Mitgliedstaat nicht über einen gesetzlichen Vertreter, so übermittelt diese Behörde gleichzeitig eine Kopie der Entfernungsanordnung an die zuständige Behörde des Mitgliedstaats, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder in dem der gesetzliche Vertreter ansässig oder niedergelassen ist.

(2) Erhält ein Hostingdiensteanbieter eine Entfernungsanordnung gemäß diesem Artikel, so ergreift er die gemäß Artikel 3 festgelegten Maßnahmen und die erforderlichen Maßnahmen, um die Inhalte gemäß Absatz 7 des vorliegenden Artikels wiederherzustellen oder zu entsperren.

(3) Die zuständige Behörde des Mitgliedstaats, in dem der Hostingdiensteanbieter seine Hauptniederlassung oder in dem der gesetzliche Vertreter ansässig oder niedergelassen ist, kann von sich aus die Entfernungsanordnung innerhalb von 72 Stunden nach Erhalt der Kopie der Entfernungsanordnung gemäß Absatz 1 überprüfen, um festzustellen, ob sie schwerwiegend oder offenkundig gegen diese Verordnung verstößt oder mit den in der Charta verankerten Grundrechte und -freiheiten verbunden ist.

Bei Feststellung eines solchen Verstoßes erlässt sie, innerhalb derselben Frist, eine begründete Entscheidung.

(4) Hostingdiensteanbieter und Inhalteanbieter sind berechtigt, innerhalb von 48 Stunden nach Erhalt einer Entfernungsanordnung oder der Informationen gemäß Artikel 11 Absatz 2 einen begründeten Antrag bei der zuständigen Behörde des Mitgliedstaats, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder in dem der gesetzliche Vertreter ansässig oder niedergelassen ist, zu stellen, um die Entfernungsanordnung gemäß Absatz 3 Unterabsatz 1 des vorliegenden Artikels überprüfen zu lassen.

Die zuständige Behörde erlässt nach ihrer Prüfung der Entfernungsanordnung innerhalb von 72 Stunden nach Eingang des Antrags eine begründete Entscheidung, in der sie ihre Erkenntnisse darlegt, ob ein Verstoß vorliegt.

(5) Die zuständige Behörde unterrichtet vor dem Erlass einer Entscheidung gemäß Absatz 3 Unterabsatz 2 oder einer Entscheidung, in der ein Verstoß festgestellt wurde, gemäß Absatz 4 Unterabsatz 2 die zuständige Behörde, die die Entfernungsanordnung erlassen hat, über ihre Absicht, eine Entscheidung zu erlassen, sowie über die Gründe hierfür.

(6) Erlässt die zuständige Behörde des Mitgliedstaats, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder in dem der gesetzliche Vertreter ansässig oder niedergelassen ist, eine begründete Entscheidung gemäß Absatz 3 oder 4 des vorliegenden Artikels, so teilt sie diese Entscheidung unverzüglich der Behörde, die die Entfernungsanordnung erlassen hat, dem Hostingdiensteanbieter, dem Inhalteanbieter, der die Prüfung gemäß Absatz 4 beantragt hat, und — im Einklang mit Artikel 14 — Europol mit. Wenn bei der Prüfung ein Verstoß nach Absatz 3 oder 4 des vorliegenden Artikels festgestellt wird, verliert die Entfernungsanordnung ihre Rechtswirkung.

(7) Nach Erhalte einer Entscheidung über einen gemäß Absatz 6 mitgeteilten Verstoß, stellt der betroffene Hostingdiensteanbieter unverzüglich den Inhalt wieder her oder entsperrt ihn unverzüglich, unbeschadet der Möglichkeit, seine Nutzungsbedingungen im Einklang mit dem Unionsrecht und dem nationalen Recht durchzusetzen.

Artikel 5

Spezifische Maßnahmen

(1) Ein Hostingdiensteanbieter, der terroristischen Inhalten gemäß Absatz 4 ausgesetzt ist, nimmt gegebenenfalls Bestimmungen in seine Nutzungsbedingungen auf, mit denen er dagegen vorgeht, dass seine Dienste für die öffentliche Verbreitung terroristischer Inhalte missbraucht werden, und wendet diese Bestimmungen an.

Er handelt dabei mit der gebotenen Sorgfalt, verhältnismäßig und ohne Diskriminierung; unter allen Umständen unter gebührender Berücksichtigung der Grundrechte der Nutzer und trägt insbesondere der grundlegenden Bedeutung der Meinungs- und Informationsfreiheit in einer offenen und demokratischen Gesellschaft Rechnung, um zu verhindern, dass Materialien entfernt werden, bei denen es sich nicht um terroristische Inhalte handelt.

(2) Ist ein Hostingdiensteanbieter terroristischen Inhalten gemäß Absatz 4 ausgesetzt, so ergreift er spezifische Maßnahmen, um zu verhindern, dass über seine Dienste terroristische Inhalte öffentlich verbreitet werden.

Der Hostingdiensteanbieter entscheidet selbst über die zu treffenden spezifischen Maßnahmen. Diese Maßnahmen können eines oder mehrere der folgenden Elemente umfassen:

a) geeignete technische und operative Maßnahmen oder Kapazitäten, beispielsweise eine angemessene Ausstattung mit Personal oder technischen Mitteln, um terroristische Inhalte zu ermitteln und unverzüglich zu entfernen oder den Zugang dazu zu sperren;

b) leicht zugängliche und benutzerfreundliche Mechanismen, durch die Nutzer dem Hostingdiensteanbieter mutmaßliche terroristische Inhalte melden oder diese Inhalte kennzeichnen können;

c) weitere Mechanismen zur stärkeren Sensibilisierung für terroristische Inhalte in seinen Diensten, wie beispielsweise Mechanismen für Nutzer-Moderation;

d) jedwede andere Maßnahme, die der Hostingdiensteanbieter für geeignet hält, um gegen die Verfügbarkeit terroristischer Inhalte in seinen Diensten vorzugehen.

(3) Die spezifischen Maßnahmen müssen folgende Anforderungen erfüllen:

a) Sie müssen das Ausmaß der Betroffenheit der Dienste des Hostingdiensteanbieters durch terroristische Inhalte wirksam eindämmen;

b) sie müssen zielgerichtet und verhältnismäßig sein und insbesondere dem Schweregrad der Betroffenheit der Dienste des Hostingdiensteanbieters durch terroristische Inhalte sowie den technischen und operativen Fähigkeiten, der Finanzkraft, der Zahl der Nutzer der Dienste des Hostingdiensteanbieters und des Umfangs der Inhalte, die diese Nutzer liefern, Rechnung tragen;

c) sie werden unter umfassender Berücksichtigung der Rechte und der berechtigten Interessen der Nutzer, insbesondere ihrer Grundrechte auf Meinungs-und Informationsfreiheit, auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, angewendet;

d) sie werden mit der gebotenen Sorgfalt und ohne Diskriminierung angewendet.

Soweit die spezifischen Maßnahmen den Einsatz technischer Maßnahmen vorsehen, ist für geeignete und wirksame Schutzvorkehrungen zu sorgen — insbesondere durch menschliche Beaufsichtigung und Überprüfung — um für Genauigkeit zu sorgen und zu verhindern, dass Materialien entfernt werden, bei denen es sich nicht um terroristische Inhalte handelt.

(4) Ein Hostingdiensteanbieter gilt als terroristischen Inhalten ausgesetzt, wenn die zuständige Behörde des Mitgliedstaats seiner Hauptniederlassung oder in dem der gesetzliche Vertreter ansässig oder niedergelassen ist,

a) eine auf objektive Faktoren gestützte Entscheidung — wie beispielsweise der Tatsache, dass dem Hostingdiensteanbieter in den letzten zwölf Monaten zwei oder mehr rechtskräftige Entfernungsanordnungen zugegangen sind —

b) den Hostingdiensteanbieter von der Entscheidung gemäß Buchstabe a in Kenntnis gesetzt hat.

(5) Nach Erhalt einer Entscheidung gemäß Absatz 4 oder gegebenenfalls gemäß Absatz 6 erstattet der Hostingdiensteanbieter der zuständigen Behörde Bericht über die spezifischen Maßnahmen, die er ergriffen hat und zu ergreifen beabsichtigt, um den Absätzen 2 und 3 zu entsprechen. Er erledigt dies innerhalb von drei Monaten nach Eingang der Entscheidung und danach jährlich. Diese Verpflichtung endet, sobald die zuständige Behörde entschieden hat, dass der Hostingdiensteanbieter nach einem Antrag gemäß Absatz 7 nicht länger terroristischen Inhalten ausgesetzt ist.

(6) Gelangt die zuständige Behörde auf der Grundlage der Berichte gemäß Absatz 5 und gegebenenfalls anderer objektiver Faktoren zu der Auffassung, dass die spezifischen Maßnahmen nicht den Absätzen 2 und 3 entsprechen, so richtet die zuständige Behörde eine Entscheidung an den Hostingdiensteanbieter, mit der dieser aufgefordert wird, die erforderlichen Maßnahmen zu ergreifen, um sicherzustellen, dass den Absätzen 2 und 3 entsprochen wird.

Der Hostingdiensteanbieter entscheidet selbst über die zu wählenden spezifischen Maßnahmen.

(7) Ein Hostingdiensteanbieter kann die zuständige Behörde jederzeit ersuchen, eine Entscheidung nach den Absätzen 4 oder 6 zu überprüfen und gegebenenfalls anzupassen oder zu widerrufen.

Die zuständige Behörde trifft innerhalb von drei Monaten nach Eingang des Ersuchens auf der Grundlage objektiver Faktoren eine begründete Entscheidung und unterrichtet den Hostingdiensteanbieter über diese Entscheidung.

(8) Jede Anordnung, spezifische Maßnahmen zu ergreifen, gilt unbeschadet von Artikel 15 Absatz 1 der Richtlinie 2000/31/EG und geht für Hostingdiensteanbieter weder mit einer generellen Verpflichtung einher, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen, noch mit einer generellen Verpflichtung, aktiv nach Fakten oder Umständen zu suchen, die auf illegale Aktivitäten hindeuten.

Die Anordnung, spezifische Maßnahmen zu ergreifen, geht nicht mit einer Verpflichtung des Hostingdiensteanbieters zur Nutzung automatisierter Verfahren einher.

Artikel 6

Speichern von Inhalten und zugehörigen Daten

(1) Die Hostingdiensteanbieter speichern terroristische Inhalte, die infolge einer Entfernungsanordnung oder infolge spezifischer Maßnahmen nach Artikel 3 oder 5 entfernt oder gesperrt wurden, sowie zugehörige Daten, die infolge der Entfernung der terroristischen Inhalte entfernt wurden, zu folgenden Zwecken auf:

a) behördliche oder gerichtliche Überprüfungsverfahren oder Beschwerdebearbeitung gemäß Artikel 10 in Bezug auf die Entscheidung, terroristische Inhalte und zugehörige Daten zu entfernen oder den Zugang dazu zu sperren; oder

b) Verhinderung, Erkennung, Ermittlung und Verfolgung von terroristischen Straftaten.

(2) Die terroristischen Inhalte und zugehörigen Daten nach Absatz 1 werden für einen Zeitraum von sechs Monaten nach ihrer Entfernung oder Sperrung gespeichert. Auf Anordnung der zuständigen Behörde oder des zuständigen Gerichts werden die terroristischen Inhalte nur dann für einen weiteren festgelegten Zeitraum gespeichert, wenn und solange dies für laufende behördliche oder gerichtliche Überprüfungsverfahren nach Absatz 1 Buchstabe a erforderlich ist.

(3) Die Hostingdiensteanbieter stellen sicher, dass die nach Absatz 1 gespeicherten terroristischen Inhalte und zugehörigen Daten angemessenen technischen und organisatorischen Schutzvorkehrungen unterliegen.

Durch diese technischen und organisatorischen Schutzvorkehrungen wird sichergestellt, dass die gespeicherten 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 soweit erforderlich.

Abschnitt III

Schutzvorkehrungen und Rechenschaftspflicht

Artikel 7

Transparenzanforderungen an Hostingdiensteanbieter

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

(2) Ein Hostingdiensteanbieter, der in einem bestimmten Kalenderjahr Maßnahmen gegen die Verbreitung terroristischer Inhalte ergriffen hat oder gemäß der vorliegenden Verordnung zur Ergreifung von Maßnahmen aufgefordert wird, macht einen Transparenzbericht über die in diesem Jahr ergriffenen Maßnahmen öffentlich zugänglich. Er veröffentlicht diesen Bericht vor dem 1. März des Folgejahres.

(3) Die Transparenzberichte enthalten mindestens folgende Angaben:

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

b) Informationen über die Maßnahmen, die der Hostingdiensteanbieter trifft, um gegen ein erneutes Erscheinen von Online-Materialien vorzugehen, die zuvor entfernt oder gesperrt wurden, weil sie als terroristische Inhalte erachtet wurden, insbesondere wenn automatisierte Verfahren verwendet wurden;

c) Anzahl der nach Entfernungsanordnungen oder spezifischen Maßnahmen entfernten oder gesperrten Elemente mit terroristischem Inhalt und Anzahl der Entfernungsanordnungen, nach deren Erhalt der Inhalt gemäß Artikel 3 Absatz 7 Unterabsatz 1 und Artikel 3 Absatz 8 Unterabsatz 1 nicht entfernt oder gesperrt wurde, einschließlich der Gründe dafür;

d) Anzahl und Ergebnis der vom Hostingdiensteanbieter bearbeiteten Beschwerden gemäß Artikel 10;

e) Anzahl und Ergebnis der vom Hostingdiensteanbieter eingeleiteten behördlichen oder gerichtlichen Überprüfungsverfahren;

f) Anzahl der Fälle, in denen der Hostingdiensteanbieter infolge eines behördlichen oder gerichtlichen Überprüfungsverfahrens Inhalte wiederherstellen oder entsperren musste

g) Anzahl der Fälle, in denen der Hostingdiensteanbieter die Inhalte nach Prüfung einer Beschwerde des Inhalteanbieters wiederhergestellt oder entsperrt hat.

Artikel 8

Transparenzberichte der zuständigen Behörden

(1) Die zuständigen Behörden veröffentlichen jährliche Transparenzberichte über ihre Tätigkeiten im Rahmen der vorliegenden Verordnung. Diese Berichte enthalten für ein bestimmtes Kalenderjahr mindestens folgende Angaben:

a) Zahl der nach Artikel 3 erlassenen Entfernungsanordnungen, nach welcher sich die Anzahl der Entfernungsanordnungen gemäß Artikel 4 Absatz 1 richtet, die Zahl der nach Artikel 4 überprüften Entfernungsanordnungen sowie Angaben dazu, wieweit die betroffenen Hostingdiensteanbieter diesen Anordnungen nachgekommen sind, einschließlich der Anzahl der Fälle, in denen terroristische Inhalte entfernt oder gesperrt wurden sowie der Anzahl der Fälle, in denen dies nicht der Fall war;

b) Zahl der Entscheidungen gemäß Artikel 5 Absatz 4, 6 oder 7 sowie Angaben dazu, wieweit die Hostingdiensteanbieter diesen Entscheidungen nachgekommen sind, einschließlich einer Beschreibung der spezifischen Maßnahmen;

c) Zahl der Fälle, in denen gegen Entfernungsanordnungen oder Entscheidungen gemäß Artikel 5 Absätze 4 und 6 behördliche oder gerichtliche Überprüfungsverfahren eingelegt wurden, sowie Angaben zu den Ergebnissen der jeweiligen Verfahren;

d) Zahl der Entscheidungen, mit denen Sanktionen gemäß Artikel 18 verfügt wurden, einschließlich einer Beschreibung der Art der verfügten Sanktionen.

(2) Die jährlichen Transparenzberichte gemäß Absatz 1 dürfen keine Angaben enthalten, die laufende Tätigkeiten zur Verhinderung, Erkennung, Ermittlung oder Verfolgung terroristischer Straftaten oder die nationalen Sicherheitsinteressen beeinträchtigen könnten.

Artikel 9

Rechtsbehelfe

(1) Hostingdiensteanbieter, die eine gemäß Artikel 3 Absatz 1 erlassene Entfernungsanordnung oder eine gemäß Artikel 4 Absatz 4 oder gemäß Artikel 5 Absatz 4, 6 oder 7 getroffene Entscheidung erhalten haben, haben ein Recht auf einen wirksamen Rechtsbehelf. Dies schließt das Recht ein, die Entfernungsanordnung vor den Gerichten des Mitgliedstaats der zuständigen Behörde anzufechten, die die Entfernungsanordnung erlassen hat, sowie das Recht, die Entscheidung gemäß Artikel 4 Absatz 4 oder Artikel 5 Absatz 4, 6 oder 7 vor den Gerichten des Mitgliedstaats der zuständigen Behörde anzufechten, die die Entscheidung getroffen hat.

(2) Inhalteanbieter, deren Inhalte infolge einer Entfernungsanordnung entfernt oder gesperrt wurden, haben ein Recht auf einen wirksamen Rechtsbehelf. Dies schließt das Recht ein, die gemäß Artikel 3 Absatz 1 erlassene Entfernungsanordnung vor den Gerichten des Mitgliedstaats der zuständigen Behörde anzufechten, der die Entfernungsanordnung erlassen hat sowie das Recht, die Entscheidung gemäß Artikel 4 Absatz 4 vor den Gerichten des Mitgliedstaats der zuständigen Behörde anzufechten, die die Entscheidung getroffen hat.

(3) Die Mitgliedstaaten schaffen wirksame Verfahren für die Ausübung der Rechte gemäß des vorliegenden Artikels.

Artikel 10

Beschwerdemechanismen

(1) Jeder Hostingdiensteanbieter richtet einen wirksamen und zugänglichen Mechanismus ein, der Inhalteanbietern, deren Inhalte aufgrund spezifischer Maßnahmen nach Artikel 5 entfernt oder gesperrt wurden, die Möglichkeit gibt, Beschwerde gegen die Entfernung oder Sperrung einzulegen und die Wiederherstellung oder Entsperrung des Inhalts zu verlangen.

(2) Jeder Hostingdiensteanbieter prüft unverzüglich jede erhaltene Beschwerde gemäß des in Absatz 1 genannten Mechanismus und stellt unverzüglich den Inhalt wieder her und entsperrt ihn, wenn dessen Entfernung oder Sperrung nicht gerechtfertigt war. Er setzt den Beschwerdeführer innerhalb von zwei Wochen nach Eingang der Beschwerde über das Ergebnis der Beschwerde in Kenntnis.

Wird eine Beschwerde abgelehnt, setzt der Hostingdiensteanbieter den Beschwerdeführer über die Gründe in Kenntnis.

Eine Wiederherstellung des Inhalts oder dessen Entsperrung steht weiteren behördlichen oder gerichtlichen Überprüfungsverfahren gegen die Entscheidung des Hostingdiensteanbieters oder der zuständigen Behörde nicht entgegen.

Artikel 11

Unterrichtung der Inhalteanbieter

(1) Entfernt oder sperrt ein Hostingdiensteanbieter terroristische Inhalte, so stellt er dem Inhalteanbieter Informationen über die Entfernung oder Sperrung 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 Entfernungsanordnung mit oder übermittelt dem Inhalteanbieter eine Kopie der Entfernungsanordnung.

(3) Die Verpflichtung nach den Absätzen 1 und 2 gilt nicht, wenn die zuständige Behörde, die die Entfernungsanordnung erlassen hat — unter Würdigung der Verhältnismäßigkeit und Notwendigkeit — entscheidet, dass aus Gründen der öffentlichen Sicherheit wie der Verhinderung, Ermittlung, Erkennung und Verfolgung terroristischer Straftaten so lange wie erforderlich, längstens jedoch sechs Wochen ab dieser Entscheidung, keine Informationen weitergegeben werden dürfen. In diesem Fall gibt der Hostingdiensteanbieter keine Informationen über die Entfernung oder Sperrung terroristischer Inhalte weiter.

Diese zuständige Behörde kann bei Fortbestehen gerechtfertigter Gründe diesen Zeitraum um weitere sechs Wochen verlängern, sofern eine solche Nichtweitergabe weiterhin gerechtfertigt ist.

Abschnitt IV

Zuständige Behörden und Zusammenarbeit

Artikel 12

Benennung der zuständigen Behörden

(1) Jeder Mitgliedstaat benennt die Behörde oder die Behörden, die dafür zuständig sind,

a) Entfernungsanordnungen nach Artikel 3 zu erlassen;

b) Entfernungsanordnungen nach Artikel 4 zu überprüfen;

c) die Durchführung spezifischer Maßnahmen nach Artikel 5 zu überwachen;

d) Sanktionen nach Artikel 18 zu verhängen.

(2) Jeder Mitgliedstaat stellt sicher, dass eine Kontaktstelle bei der zuständigen Behörde gemäß Absatz 1 Buchstabe a für die Bearbeitung von Ersuchen um Klarstellung und Rückmeldungen im Zusammenhang mit den von den zuständigen Behörden erlassenen Entfernungsanordnungen benannt oder eingerichtet ist.

Mitgliedstaaten stellen sicher, dass die Angaben zur Kontaktstelle öffentlich zugänglich gemacht werden.

(3) Bis zum … [*zwölf Monate nach Inkrafttreten dieser Verordnung*] teilen die Mitgliedstaaten der Kommission die in Absatz 1 genannte zuständige Behörde oder genannten zuständigen Behörden sowie jede Änderung hierzu mit. Die Kommission veröffentlicht die Mitteilung und eventuelle Änderungen derselben im *Amtsblatt der Europäischen Union*.

(4) Bis zum … [*zwölf Monate nach Inkrafttreten dieser Verordnung*] erstellt die Kommission ein Online-Verzeichnis, in dem alle zuständigen Behörden gemäß Absatz 1 und die für jede dieser zuständigen Behörde benannte oder eingerichtete Kontaktstelle gemäß Absatz 2 aufgeführt sind. Die Kommission veröffentlicht regelmäßig alle Änderungen.

Artikel 13

Zuständige Behörden

(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden über die nötigen Befugnisse und ausreichende Mittel verfügen, um die Ziele dieser Verordnung zu erreichen und ihren sich daraus ergebenden Verpflichtungen nachkommen zu können.

(2) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden ihre Aufgaben gemäß vorliegender Verordnung auf objektive und diskriminierungsfreie Weise und unter uneingeschränkter Achtung der Grundrechte wahrnehmen. Die zuständigen Behörden holen bei der Wahrnehmung ihrer Aufgaben gemäß Artikel 12 Absatz 1 weder Weisungen von anderen Stellen ein, noch nehmen sie solche Weisungen entgegen.

Unterabsatz 1 dieses Absatzes steht einer Aufsicht im Einklang mit dem nationalen Verfassungsrecht nicht entgegen.

Artikel 14

Zusammenarbeit zwischen Hostingdiensteanbietern, zuständigen Behörden und Europol

(1) In Bezug auf Entfernungsanordnungen unterrichten die zuständigen Behörden einander, stimmen sich ab und arbeiten zusammen und unterrichten, gegebenenfalls Europol bzw. stimmen sich mit Europol ab, und arbeiten mit Europol zusammen, um Doppelarbeit zu vermeiden, die Koordinierung zu verstärken und Störung von Ermittlungen in verschiedenen Mitgliedstaaten zu vermeiden.

(2) In Bezug auf spezifische Maßnahmen nach Artikel 5 und Sanktionen nach Artikel 18 unterrichten die zuständigen Behörden der Mitgliedstaaten die zuständigen Behörden nach Artikel 12 Absatz 1 Buchstaben c und d, stimmen sich mit ihnen ab und arbeiten mit ihnen zusammen. Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden nach Artikel 12 Absatz 1 Buchstaben c und d im Besitz aller relevanten Informationen sind.

(3) Zum Zwecke von Absatz 1 sehen die Mitgliedstaaten geeignete und sichere Kommunikationskanäle oder Mechanismen vor, um sicherzustellen, dass die relevanten Informationen rechtzeitig ausgetauscht werden.

(4) Für die wirksame Umsetzung dieser Verordnung sowie um Doppelarbeit zu vermeiden, können sich die Mitgliedstaaten und Hostingdiensteanbieter für die Verwendung spezieller Verfahren entscheiden, auch der von Europol eingeführten Verfahren, um insbesondere Folgendes zu erleichtern:

a) die Bearbeitung von Entfernungsanordnungen nach Artikel 3 und diesbezügliche Rückmeldungen; und

b) die Zusammenarbeit zur Ermittlung und Durchführung spezifischer Maßnahmen nach Artikel 5.

(5) Verfügen Hostingdiensteanbieter über Kenntnisse über terroristische Inhalte, die zu einer unmittelbaren Bedrohung von Leben führen, so unterrichten sie unverzüglich die für die Ermittlung und Verfolgung von Straftaten in den betreffenden Mitgliedstaaten zuständigen Behörden. Ist es nicht möglich, die betreffenden Mitgliedstaaten festzustellen, so benachrichtigen die Hostingdiensteanbieter die Kontaktstelle nach Artikel 12 Absatz 2 in dem Mitgliedstaat, in dem sie ihre Hauptniederlassung haben oder in dem der gesetzliche Vertreter ansässig oder niedergelassen ist und übermitteln Informationen über diese terroristischen Inhalte zur weiteren Bearbeitung an Europol.

(6) Die zuständigen Behörden werden ermutigt, Europol Kopien ihrer Entfernungsanordnungen zu übersenden, damit Europol einen Jahresbericht vorlegen kann, der unter anderem eine Auswertung der Arten von terroristischen Inhalten enthält, die Gegenstand von Entfernungsanordnungen gemäß der vorliegenden Verordnung sind.

Artikel 15

Kontaktstellen der Hostingdiensteanbieter

(1) Jeder Hostingdiensteanbieter benennt oder errichtet eine Kontaktstelle ein, die den Erhalt von Entfernungsanordnungen auf elektronischem Weg ermöglicht und deren unverzügliche Bearbeitung nach den Artikeln 3 und 4 sicherstellt. Der Hostingdiensteanbieter sorgt dafür, dass die Informationen über die Kontaktstelle öffentlich zugänglich gemacht werden.

(2) In den Informationen nach Absatz 1 des vorliegenden Artikels sind die Amtssprachen der Unionsorgane gemäß der Verordnung Nr. 1/58 ([15]) anzugeben, in denen eine Kontaktaufnahme mit der Kontaktstelle möglich ist und in denen der weitere Austausch im Zusammenhang mit Entfernungsanordnungen nach Artikel 3 stattfindet. Zu diesen Sprachen gehört mindestens eine der Amtssprachen des Mitgliedstaats, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder sein gesetzlicher Vertreter ansässig oder niedergelassen ist.

([15]) Verordnung Nr. 1 zur Regelung der Sprachenfrage für die Europäische Atomgemeinschaft (ABl. 17 vom 6.10.1958, S. 385).

Abschnitt V

Anwendung und Durchsetzung

Artikel 16

Gerichtsbarkeit

(1) Die Gerichtsbarkeit für die Zwecke der Artikel 5, 18 und 21 liegt bei dem Mitgliedstaat, in dem sich die Hauptniederlassung des Hostingdiensteanbieters befindet. Hostingdiensteanbieter, deren Hauptniederlassung sich nicht in der Union befindet, gelten als der Gerichtsbarkeit des Mitgliedstaats unterworfen, in dem sein gesetzlicher Vertreter ansässig oder niedergelassen ist.

(2) Hat ein Hostingdiensteanbieter, dessen Hauptniederlassung sich nicht in der Union befindet, keinen gesetzlichen Vertreter benannt, so liegt die Gerichtsbarkeit bei allen Mitgliedstaaten.

(3) Entscheidet die zuständige Behörde eines Mitgliedstaats, die Gerichtsbarkeit gemäß Unterabsatz 2 auszuüben, unterrichtet sie alle zuständigen Behörden der anderen Mitgliedstaaten hiervon.

Artikel 17

Gesetzlicher Vertreter

(1) Ein Hostingdiensteanbieter, der keine Hauptniederlassung in der Union hat, benennt schriftlich eine natürliche oder juristische Person zu seinem gesetzlichen Vertreter in der Union für die Entgegennahme, Einhaltung und Durchsetzung von Entfernungsanordnungen und Entscheidungen, die von den zuständigen Behörden erlassen werden.

(2) Der Hostingdiensteanbieter stattet seinen gesetzlichen Vertreter mit den notwendigen Befugnissen und Ressourcen aus, damit dieser den betreffenden Entscheidungen und Entfernungsanordnungen nachkommen und mit den zuständigen Behörden zusammenarbeiten kann.

Der gesetzliche Vertreter ist in einem der Mitgliedstaaten, in dem der Hostingdiensteanbieter seine Dienste anbietet, ansässig oder niedergelassen.

(3) Der gesetzliche Vertreter kann für Verstöße aus dieser Verordnung haftbar gemacht werden; jegliche Haftung und rechtlichen Schritte gegen den Hostingdiensteanbieter bleiben hiervon unberührt.

(4) Der Hostingdiensteanbieter setzt die zuständige Behörde nach Artikel 12 Absatz 1 Buchstabe d in dem Mitgliedstaat, in dem der gesetzliche Vertreter ansässig oder niedergelassen ist, über die Benennung in Kenntnis.

Der Hostingdiensteanbieter macht Informationen über den gesetzlichen Vertreter öffentlich zugänglich.

Abschnitt VI

Schlussbestimmungen

Artikel 18

Sanktionen

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen der Hostingdiensteanbieter gegen diese Verordnung zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Diese Sanktionen beschränken sich auf Verstöße gegen: Artikel 3 Absätze 3 und 6, Artikel 4 Absätze 2 und 7, Artikel 5 Absätze 1, 2, 3, 5 und 6, Artikel 6, 7, 10 und 11, Artikel 14 Absatz 5, Artikel 15 Absatz 1 und Artikel 17.

Die Sanktionen gemäß Unterabsatz 1 müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis … [*von zwölf Monaten nach Inkrafttreten dieser Verordnung*] mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Entscheidung darüber, ob sie Sanktionen verhängen, und 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 des Hostingdiensteanbieters;

d) die Finanzkraft des Hostingdiensteanbieters;

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

f) die Art und Größe des Hostingdiensteanbieters, insbesondere ob es sich um ein Kleinst-, Klein- und mittlere Unternehmen handelt;

g) das Maß des Verschuldens des Hostingdiensteanbieters unter Berücksichtigung der technischen und organisatorischen Maßnahmen, die vom Hostingdiensteanbieter ergriffen wurden, um dieser Verordnung nachzukommen.

(3) Die Mitgliedstaaten stellen sicher, dass bei einem systematischen oder ständigen Verstoß gegen die Verpflichtungen aus Artikel 3 Absatz 3 finanzielle Sanktionen in Höhe von bis zu 4 % des vom Hostingdiensteanbieter im vorangegangenen Geschäftsjahr erwirtschafteten weltweiten Jahresumsatzes verhängt werden.

Artikel 19

Technische Anforderungen und Änderungen der Anhänge

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

(2) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 20 zur Änderung der Anhänge zu erlassen, um einem etwaigen Verbesserungsbedarf hinsichtlich des Inhalts der Entfernungsanordnungsformulare wirksam zu entsprechen und Informationen über die Unmöglichkeit der Ausführung der Entfernungsanordnung zur Verfügung zu stellen.

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 … [*Ein Jahr nach Inkrafttreten 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 vom 13. April 2016 über bessere Rechtsetzung 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 im vorangegangenen Kalenderjahr ergriffen wurden, und übermitteln sie der Kommission spätestens bis zum 31. März jeden Jahres. Diese Informationen umfassen Folgendes:

a) die Anzahl der erlassenen Entfernungsanordnungen und die Anzahl der entfernten oder gesperrten Elemente mit terroristischem Inhalt sowie wie schnell die Entfernung oder Sperrung stattfand;

b) spezifische Maßnahmen nach Artikel 5, einschließlich der Anzahl der entfernten oder gesperrten Elemente mit terroristischem Inhalt und wie schnell die Entfernung oder Sperrung erfolgt ist;

c) Anzahl der von den zuständigen Behörden angeforderten Zugriffe auf von Hostingdiensteanbietern nach Artikel 6 gespeicherte Inhalte;

d) Anzahl der eingeleiteten Beschwerdeverfahren und der von Hostingdiensteanbietern unternommenen Maßnahmen nach Artikel 10;

e) Anzahl der eingeleiteten behördlichen oder gerichtlichen Überprüfungsverfahren und der von der zuständigen Behörde nach nationalem Recht erlassenen Entscheidungen.

(2) Die Kommission stellt bis zum … [*zwei Jahre nach Inkrafttreten dieser Verordnung*] ein ausführliches Programm für das Monitoring der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung auf. 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

[Drei Jahre nach Inkrafttreten dieser Verordnung] führt die Kommission eine Evaluierung dieser Verordnung durch und legt dem Europäischen Parlament und dem Rat einen Bericht über deren Anwendung vor einschließlich:

a) des Funktionierens und der Wirksamkeit der Schutzvorkehrungen, insbesondere der in Artikel 4 Absatz 4, Artikel 6 Absatz 3 und Artikeln 7 bis 11 festgelegten;

b) der Auswirkungen der Anwendung der Verordnung auf die Grundrechte, insbesondere die Meinungs- und Informationsfreiheit, das Recht auf Achtung der Privatsphäre und das Recht auf den Schutz personenbezogener Daten, sowie

c) des Beitrags der Verordnung zum Schutz der öffentlichen Sicherheit.

Gegebenenfalls wird der Bericht um Legislativvorschläge ergänzt.

Die Mitgliedstaaten übermitteln der Kommission die für die Ausarbeitung des Berichts erforderlichen Informationen.

Die Kommission bewertet zudem die Notwendigkeit und die Durchführbarkeit der Schaffung einer europäischen Plattform in Bezug auf terroristische Online-Inhalte, um Kommunikation und Zusammenarbeit im Rahmen dieser Verordnung zu fördern.

Artikel 24

Inkrafttreten und Anwendung

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

Sie gilt ab dem … [*12 Monate nach Inkrafttreten dieser Verordnung*].

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

Geschehen zu …

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

ANHANG I

ENTFERNUNGSANORDNUNG

(Artikel 3 der Verordnung (EU) 2021/… des Europäischen Parlaments und des Rates ([1]) ([*]))

Nach Artikel 3 der Verordnung (EU) 2021/… ([*]) (im Folgenden „Verordnung“) muss der Empfänger dieser Entfernungsanordnung terroristische Inhalte in allen Mitgliedstaaten so schnell wie möglich, in jedem Fall aber innerhalb einer Stunde nach Erhalt dieser Anordnung entfernen oder den Zugang zu terroristischen Inhalten sperren.

Nach Artikel 6 der Verordnung speichern die Empfänger die entfernten oder gesperrten Inhalte und zugehörigen Daten für einen Zeitraum von sechs Monaten oder auf Anordnung der zuständigen Behörden oder Gerichte für einen längeren Zeitraum.

Nach Artikel 15 Absatz 2 der Verordnung wird diese Entfernungsanordnung in einer der vom Empfänger gemäß Artikel 14 Absatz 2 angegebenen Sprachen übermittelt.

ABSCHNITT A:

Mitgliedstaat der erlassenden zuständigen Behörde:

……

Hinweis: Angaben zur erlassenden zuständigen Behörde sind in den Abschnitten E und F zu machen.

Empfänger und ggf. gesetzlicher Vertreter:

……

Kontaktstelle:

……

Mitgliedstaat, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder in dem der gesetzliche Vertreter ansässig oder niedergelassen ist:

……

Uhrzeit und Datum des Erlasses der Entfernungsanordnung:

……

Referenznummer der Entfernungsanordnung:

……

([1]) Verordnung (EU) 2021/…([*]) des Europäischen Parlaments und des Rates zur Bekämpfung der Verbreitung terroristischer Online-Inhalte (ABl. L …).

([*]) Nummer der Verordnung aus Dokument ST 14308/20 (2018/0331 (COD)).

ABSCHNITT B: In allen Mitgliedstaaten so schnell wie möglich, in jedem Fall aber innerhalb einer Stunde nach Erhalt der Entfernungsanordnung zu entfernender oder zu sperrender terroristischer Inhalt:

Eine URL-Adresse und alle weiteren Informationen, die die Identifizierung und die genaue Lokalisierung des gemeldeten terroristischen Inhalts ermöglichen:

……

Gründe, das Material gemäß Artikel 2 Nummer 7 der Verordnung als terroristischen Inhalt anzusehen:

Das Material (Zutreffendes bitte ankreuzen):

☐ stiftet andere zur Begehung terroristischer Straftaten an, unter anderem durch Verherrlichung terroristischer Handlungen, durch Befürwortung der Begehung solcher Straftaten (Artikel 2 Absatz 7 Buchstabe a der Verordnung)

☐ bestimmt andere zur Begehung von oder zu einem Beitrag zur Begehung von terroristischen Straftaten (Artikel 2 Absatz 7 Buchstabe b der Verordnung)

☐ bestimmt andere zur Beteiligung an Handlungen einer terroristischen Vereinigung (Artikel 2 Absatz 7 Buchstabe c der Verordnung)

☐ enthält Anleitungen zur Herstellung oder den Gebrauch von Sprengstoffen, Schuss- oder sonstigen Waffen oder schädlichen oder gefährlichen Stoffen beziehungsweise Unterweisung in anderen spezifischen Methoden oder Verfahren mit dem Ziel, eine terroristischen Straftat zu begehen oder zu deren Begehung beizutragen (Artikel 2 Absatz 7 Buchstabe d der Verordnung)

☐ stellt eine Gefahr dar, dass eine der terroristischen Straftaten begangen wird (Artikel 2 Absatz 7 Buchstabe e der Verordnung).

Zusätzliche Informationen, nach denen das Material als terroristischer Inhalt angesehen wird:

……

……

……

ABSCHNITT C: Unterrichtung des Inhalteanbieters

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

☐ der Empfänger aus Gründen der öffentlichen Sicherheit **den Inhalteanbieter nicht** über die Entfernung oder Sperrung des terroristischen Inhalts **unterrichten darf**.

Wenn Vorstehendes nicht zutrifft, siehe Abschnitt G für Einzelheiten zu den Möglichkeiten, die Entfernungsanordnung im Mitgliedstaat der erlassenden zuständigen Behörde nach nationalem Recht anzufechten (eine Kopie Entfernungsanordnung muss dem Inhalteanbieter auf Anfrage übermittelt werden).

ABSCHNITT D: Unterrichtung der zuständigen Behörde in dem Mitgliedstaat, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder sein gesetzlicher Vertreter ansässig oder niedergelassen ist

Zutreffendes bitte ankreuzen:

☐ der Mitgliedstaat, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder sein gesetzlicher Vertreter ansässig oder niedergelassen ist, ist nicht der Mitgliedstaat der erlassenden zuständigen Behörde

☐ eine Kopie der Entfernungsanordnung wird der zuständigen Behörde des Mitgliedstaates, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder sein gesetzlicher Vertreter ansässig oder niedergelassen ist, übermittelt

ABSCHNITT E: Angaben zur erlassenden zuständigen Behörde

Art (Zutreffendes bitte ankreuzen):

☐ Richter, Gericht oder Ermittlungsrichter

☐ Strafverfolgungsbehörde

☐ andere zuständige Behörde → bitte auch Abschnitt F ausfüllen

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

Name der erlassenden zuständigen Behörde:

……

Name ihres Vertreters und Funktion (Titel/Amtsbezeichnung):

Aktenzeichen: ……

Anschrift: ……

Telefon: Telefonnummer (Ländervorwahl) (Gebiets-/Ortsvorwahl): ……

……

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

E-Mail-Adresse: ……

Datum: ……

Dienststempel (falls vorhanden) und Unterschrift ([2]): ……

([2]) Eine Unterschrift ist nicht erforderlich, wenn die Übermittlung der Entfernungsanordnung über authentifizierte Übertragungskanäle erfolgt, mit der die Echtheit der Entfernungsanordnung gewährleistet werden kann.

ABSCHNITT F: Kontaktangaben für Folgemaßnahmen

Kontaktangaben der erlassenden zuständigen Behörde zwecks einer Rückmeldung über den Zeitpunkt der Entfernung oder Sperrung oder zur Klärung weiterer Fragen:

.....

Kontaktangaben der zuständigen Behörde des Mitgliedstaates, in dem der Hostingdiensteanbieter seine Hauptniederlassung hat oder in dem sein gesetzlicher Vertreter ansässig oder niedergelassen ist:

.....

ABSCHNITT G: Informationen über verfügbare Rechtsbehelfe

Informationen über zuständige Stellen oder Gerichte, Fristen und Verfahren für die Anfechtung der Entfernungsanordnung:

Zuständige Stelle oder Gericht, vor der oder dem die Entfernungsanordnung angefochten werden kann:

.....

Frist für die Anfechtung der Entfernungsanordnung:

[Tage/Monate ab dem]

.....

Link zu den Bestimmungen der nationalen Rechtsvorschriften:

.....

ANHANG II

FORMULAR FÜR RÜCKMELDUNGEN NACH DER ENTFERNUNG ODER SPERRUNG TERRORISTISCHER INHALTE

(Artikel 3 Absatz 6 der Verordnung (EU) 2021/ … des Europäischen Parlaments und des Rates ([1]) ([*]))

ABSCHNITT A:

Empfänger der Entfernungsanordnung:

……

zuständige Behörde, die die Entfernungsanordnung erlassen hat:

……

Aktenzeichen der zuständigen Behörde, die die Entfernungsanordnung erlassen hat:

……

Aktenzeichen des Empfängers:

……

Uhrzeit und Datum des Erhalts der Entfernungsanordnung:

……

ABSCHNITT B: Gemäß der Entfernungsanordnung eingeleitete Maßnahmen

(Zutreffendes bitte ankreuzen):

☐ der terroristische Inhalt wurde entfernt

☐ Zugang zum terroristischen Inhalt wurde gesperrt

Uhrzeit und Datum der eingeleiteten Maßnahme:

……

([1]) Verordnung (EU) 2021/ … ([*]) des Europäischen Parlaments und des Rates zur Bekämpfung der Verbreitung terroristischer Online-Inhalte (ABl. L …).

([*]) Nummer der Verordnung aus Dokument ST 14308/20 (2018/0331 (COD)).

ABSCHNITT C: Angaben zum Empfänger

Name des Hostingdiensteanbieters

……

ODER

Name des gesetzlichen Vertreters des Hostingdiensteanbieters:

……

Mitgliedstaat der Hauptniederlassung des Hostingdiensteanbieters:

……

ODER

Mitgliedstaat der Niederlassung des gesetzlichen Vertreters des Hostingdiensteanbieters:

……

Name der bevollmächtigten Person:

……

E-Mail-Adresse der Kontaktstelle:

……

Termin:

……

ANHANG III

UNTERRICHTUNG ÜBER DIE UNMÖGLICHKEIT DER AUSFÜHRUNG DER ENTFERNUNGSANORDNUNG

(Artikel 3 Absätze 7 und 8 der Verordnung (EU) 2021/ … des Europäischen Parlaments und des Rates ([1]) ([*]))

ABSCHNITT A:

Empfänger der Entfernungsanordnung:

……

Zuständige Behörde, die die Entfernungsanordnung erlassen hat:

……

Aktenzeichen der zuständigen Behörde, die die Entfernungsanordnung erlassen hat:

……

Aktenzeichen des Empfängers:

……

Uhrzeit und Datum des Erhalts der Entfernungsanordnung:

……

ABSCHNITT B: Unmöglichkeit der Ausführung

1. Der Entfernungsanordnung kann aus folgenden Gründen nicht innerhalb der Frist nachgekommen werden (Zutreffendes bitte ankreuzen):

   ☐ höhere Gewalt oder eine faktische Unmöglichkeit, die dem Hostingdiensteanbieter nicht angelastet werden kann, einschließlich objektiv begründeter technischer oder operativer Gründe

   ☐ die Entfernungsanordnung enthält offensichtliche Fehler

   ☐ die Entfernungsanordnung enthält unzureichende Informationen

2. Bitte machen Sie nähere Angaben zu den Gründen für die Unmöglichkeit der Ausführung:

   ……

3. Falls die Entfernungsanordnung offensichtliche Fehler und/oder unzureichende Informationen enthält, geben Sie bitte die Fehler und weiteren Informationen an:

   ……

([1]) Verordnung (EU) 2021/ … ([*]) des Europäischen Parlaments und des Rates zur Bekämpfung der Verbreitung terroristischer Online-Inhalte (ABl. L …).

([*]) Nummer der Verordnung aus Dokument ST 14308/20 (2018/0331 (COD)).

ABSCHNITT C: Angaben zum Hostingdiensteanbieter oder zu seinem gesetzlichen Vertreter:

Name des Hostingdiensteanbieters :

……

ODER

Name des gesetzlichen Vertreters des Hostingdiensteanbieters:

……

Name der bevollmächtigten Person:

……

Kontaktangaben (E-Mail-Adresse):

……

Unterschrift:

……

Uhrzeit und Datum:

……

Begründung des Rates: Standpunkt (EU) Nr. 6/2021 des Rates in erster Lesung im Hinblick auf den Erlass einer Verordnung des Europäischen Parlaments und des Rates zur Bekämpfung der Verbreitung terroristischer Online-Inhalte

(2021/C 135/02)

I. EINLEITUNG

1. Am 12. September 2018 hat die Kommission dem Rat und dem Europäischen Parlament den oben genannten Vorschlag für eine Verordnung zur Verhinderung der Verbreitung terroristischer Online-Inhalte ([1]) unterbreitet. Die Rechtsgrundlage ist Artikel 114 [Angleichung der Rechtsvorschriften] des Vertrags über die Arbeitsweise der Europäischen Union, und der Vorschlag unterliegt dem ordentlichen Gesetzgebungsverfahren.

2. Der Europäische Wirtschafts- und Sozialausschuss (EWSA) wurde vom Rat mit Schreiben vom 24. Oktober 2018 konsultiert und hat seine Stellungnahme zu dem Vorschlag ([2]) am 12. Dezember 2018 auf seiner Plenartagung abgeben.

3. Am 6. Dezember 2018 hat sich der Rat auf eine allgemeine Ausrichtung ([3]) zu terroristischen Online-Inhalten geeinigt, die das Mandat für Verhandlungen mit dem Europäischen Parlament im Rahmen des ordentlichen Gesetzgebungsverfahrens darstellte.

4. Am 12. Februar 2019 hat der Europäische Datenschutzbeauftragte „formelle Bemerkungen" zum Verordnungsentwurf ([4]) an das Europäische Parlament, die Kommission und den Rat übermittelt. Am selben Tag hat die Agentur der Europäischen Union für Grundrechte auf Ersuchen des Europäischen Parlaments vom 6. Februar 2019 eine Stellungnahme zu dem Vorschlag ([5]) abgegeben.

5. Am 17. April 2019 hat das Europäische Parlament seinen Standpunkt in erster Lesung ([6]) zu dem Vorschlag der Kommission mit 155 Änderungen angenommen; dabei gab es 308 Ja-Stimmen, 204 Gegenstimmen und 70 Enthaltungen.

6. Der Rat und das Europäische Parlament haben im Oktober 2019 Verhandlungen aufgenommen, um eine frühzeitige Einigung in zweiter Lesung zu erzielen. Die Verhandlungen wurden am 10. Dezember 2020 mit einer vorläufigen Einigung zwischen dem Europäischen Parlament und dem Rat über einen Kompromisstext erfolgreich abgeschlossen.

7. Am 16. Dezember 2020 hat der AStV (2. Teil) den endgültigen Kompromisstext im Hinblick auf die mit dem Europäischen Parlament erzielte Einigung eingehend geprüft und vorläufig bestätigt. ([7])

8. Am 11. Januar 2021 wurde der Kompromiss vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments gebilligt. Am 13. Januar 2021 hat der Vorsitzende des LIBE-Ausschusses dem Präsidenten des AStV (2. Teil) in einem Schreiben mitgeteilt, dass er, sollte der Rat seinen Standpunkt in der dem genannten Schreiben beigefügten Fassung dem Europäischen Parlament förmlich übermitteln, dem Plenum empfehlen werde, den Standpunkt des Rates – vorbehaltlich der Überarbeitung durch die Rechts- und Sprachsachverständigen – in zweiter Lesung des Europäischen Parlaments ohne Abänderungen zu billigen ([8]).

([1]) Dok. 12129/18 + ADD 1-3.
([2]) ABl. C 110 vom 22.3.2019, S. 67 (Dok. 15729/19).
([3]) Dok. 15336/18.
([4]) Ref. 2018-0822 D2545 (WK 9232/2019).
([5]) Stellungnahme der FRA – 2/2019 (WK 9235/2019).
([6]) Siehe Dokument 8663/19 (Informatorischer Vermerk der GIP 2 (Interinstitutionelle Beziehungen) an den AStV, in dem das Ergebnis der ersten Lesung des Europäischen Parlaments vorgestellt wird); das Mandat des Parlaments wurde am 10./11. Oktober 2019 vom Plenum bestätigt.
([7]) Dok. 12906/20.
([8]) Dok. 5634/21.

II. **ZIEL**

9. Durch die Verordnung wird ein klarer Rechtsrahmen geschaffen, mit dem die Zuständigkeiten der Mitgliedstaaten und der Hostingdiensteanbieter festgelegt werden, um den Missbrauch von Hostingdiensten für die Verbreitung terroristischer Online-Inhalte zu bekämpfen, das reibungslose Funktionieren des digitalen Binnenmarktes zu gewährleisten und das Vertrauen in das Online-Umfeld sowie seine Sicherheit zu wahren. Insbesondere soll mit ihr klargestellt werden, dass die Hostingdiensteanbieter dafür zuständig sind, die Sicherheit ihrer Dienste zu gewährleisten sowie rasch und wirksam gegen terroristische Online-Inhalte vorzugehen, sie zu ermitteln und zu entfernen oder den Zugang dazu zu sperren. Mit ihr wird ein neues und wirksames operatives Instrument für die Beseitigung terroristischer Inhalte geschaffen, indem die Erteilung von Entfernungsanordnungen mit grenzüberschreitender Wirkung ermöglicht wird. Darüber hinaus sollen Vorkehrungen aufrechterhalten werden, um den Schutz der Grundrechte, einschließlich der Meinungs- und Informationsfreiheit in einer offenen und demokratischen Gesellschaft und der unternehmerischen Freiheit, zu gewährleisten. Die Verordnung sieht vor, dass terroristische Inhalte innerhalb einer Stunde nach Erhalt der Entfernungsanordnung zu entfernen sind, und legt fest, dass Online-Plattformen dafür zuständig sind, die Entfernung dieser Inhalte sicherzustellen. Zusätzlich zur Möglichkeit von Rechtsbehelfen, die durch das Recht auf wirksamen Rechtsbehelf garantiert wird, werden in der Verordnung eine Reihe von Schutzvorkehrungen und Beschwerdemechanismen eingeführt.

10. Die zuständige Behörde bzw. die zuständigen Behörden jedes Mitgliedstaats kann bzw. können allen Hostingdiensteanbietern, die in der EU Dienste anbieten, eine Entfernungsanordnung erteilen. Die zuständige Behörde bzw. die zuständigen Behörden des Mitgliedstaats, in dem sich die Hauptniederlassung des Hostingdiensteanbieters befindet, hat bzw. haben das Recht – und auf begründeten Antrag der Hostingdiensteanbieter oder Inhalteanbieter die Pflicht – die Entfernungsanordnung zu überprüfen, wenn sie als schwerwiegender oder offenkundiger Verstoß gegen diese Verordnung oder die in der Charta der Grundrechte der Europäischen Union verankerten Grundrechte erachtet wird. Die Mitgliedstaaten sollten die Vorschriften zu Sanktionen für Verstöße gegen die Pflichten festlegen und dabei unter anderem die Art des Verstoßes und die Größe des betreffenden Unternehmens berücksichtigen.

III. **ANALYSE DES STANDPUNKTS DES RATES IN ERSTER LESUNG**

ALLGEMEINES

11. Das Europäische Parlament und der Rat haben Verhandlungen geführt, um in zweiter Lesung auf der Grundlage eines Standpunkts des Rates in erster Lesung, den das Parlament unverändert billigen könnte, eine Einigung zu erreichen. Der Text des Standpunkts des Rates in erster Lesung zur Verordnung zur Verhinderung der Verbreitung terroristischer Online-Inhalte spiegelt den zwischen den beiden Gesetzgebern mit Unterstützung der Kommission erzielten Kompromiss voll und ganz wider.

ZUSAMMENFASSUNG DER WICHTIGSTEN PUNKTE

12. Auf Ersuchen des Europäischen Parlaments wurde der Titel der Verordnung zu „Verordnung zur Bekämpfung [...] der Verbreitung terroristischer Online-Inhalte“ geändert.

13. Die Bestimmung des Begriffs „terroristische Inhalte“ steht im Einklang mit den Begriffsbestimmungen der entsprechenden Straftaten gemäß der Richtlinie zur Terrorismusbekämpfung ([9]). Was den Anwendungsbereich betrifft, so umfasst der Standpunkt des Rates in erster Lesung Materialien, die öffentlich – d. h. für einen potenziell unbegrenzten Personenkreis – verbreitet werden. Material, das für Bildungs-, Presse-, Forschungszwecke oder künstlerische Zwecke oder zum Zweck der Sensibilisierung zur Verhinderung oder Bekämpfung von Terrorismus verbreitet wird, sollte nicht als terroristische Inhalte gelten. Dies umfasst auch Inhalte, die eine Formulierung polemischer oder kontroverser Ansichten zu sensiblen politischen Fragen in der öffentlichen Debatte darstellen. Im Rahmen einer Bewertung wird der wahre Zweck dieser Verbreitung ermittelt. Ferner wurde festgelegt, dass diese Verordnung nicht die Pflicht berührt, die in Artikel 6 EUV verankerten Rechte, Freiheiten und Grundsätze zu achten, und unbeschadet der Grundprinzipien der Meinungs- und Informationsfreiheit, einschließlich der Medienfreiheit und des Medienpluralismus, gilt.

([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).

14. Die Hostingdiensteanbieter ergreifen angemessene, sinnvolle und verhältnismäßige Maßnahmen, um den Missbrauch ihrer Dienste für die Verbreitung terroristischer Online-Inhalte wirksam zu bekämpfen. Sind Hostingdiensteanbieter terroristischen Inhalten ausgesetzt, so müssen sie spezifische Maßnahmen ergreifen, um die Verbreitung über ihre Dienste zu verhindern. In dem vereinbarten Text werden drei Artikel – Artikel 3 (Sorgfaltspflichten), Artikel 6 (Proaktive Maßnahmen) und Artikel 9 (Schutzvorkehrungen in Bezug auf proaktive Maßnahmen) – zu einem Artikel über „spezifische Maßnahmen" zusammengeführt. Diese Maßnahmen können von den einzelnen Hostingdiensteanbietern ausgewählt werden. Im Standpunkt des Rates in erster Lesung wird klargestellt, dass der Hostingdiensteanbieter verschiedene Maßnahmen, einschließlich automatisierter Maßnahmen, zur Bekämpfung der Verbreitung terroristischer Inhalte einsetzen kann, wobei diese an die Fähigkeiten des Hostingdiensteanbieters und die Art seiner geleisteten Dienste angepasst werden können. Ist die zuständige Behörde der Auffassung, dass die getroffenen spezifischen Maßnahmen die Risiken nicht hinreichend bekämpfen, wird sie zusätzliche geeignete, wirksame und verhältnismäßige spezifische Maßnahmen fordern können. Eine Anordnung, solche zusätzlichen spezifischen Maßnahmen durchzuführen, sollte jedoch weder zur Auferlegung einer allgemeinen Pflicht zur Überwachung oder zum aktiven Forschen nach Hinweisen im Sinne des Artikels 15 Absatz 1 der Richtlinie 2000/31/EG ([10]) noch zu einer Verpflichtung zur Anwendung automatisierter Werkzeuge (Tools) führen. Zur Gewährleistung der Transparenz sind von den Hostingdiensteanbietern jährliche Transparenzberichte über die gegen die Verbreitung terroristischer Inhalte ergriffenen Maßnahmen zu veröffentlichen.

15. Die Rolle des Mitgliedstaats der Hauptniederlassung in Bezug auf Entfernungsanordnungen mit grenzüberschreitender Wirkung wurde gestärkt, indem ein Prüfungsverfahren eingeführt wurde: Die zuständige Behörde des Mitgliedstaats, in dem sich die Hauptniederlassung des Hostingdiensteanbieters oder der gesetzliche Vertreter befindet, kann von sich aus die von den zuständigen Behörden eines anderen Mitgliedstaats ausgestellte Entfernungsanordnung überprüfen, um festzustellen, ob sie schwerwiegend oder offenkundig gegen die Verordnung oder die in der Charta der Grundrechte der Europäischen Union verankerten Grundrechte verstößt. Auf begründeten Antrag eines Hostingdiensteanbieters oder eines Inhalteanbieters ist der Mitgliedstaat der Hauptniederlassung verpflichtet zu überprüfen, ob solch ein Verstoß vorliegt.

16. Von hinreichend begründeten Dringlichkeitsfällen abgesehen sollten diejenigen Hostingdiensteanbieter, für die zuvor noch keine Entfernungsanordnung von dieser Behörde erteilt wurde, zwölf Stunden vorher eine Benachrichtigung mit Informationen über Verfahren und geltende Fristen erhalten, insbesondere um die Belastung kleiner und mittlerer Unternehmen (KMU) zu verringern.

17. Der Artikel über „Meldungen" – ein Mechanismus, mit dem Hostingdiensteanbieter auf terroristische Inhalte aufmerksam gemacht werden, damit sie freiwillig die Vereinbarkeit mit ihren Nutzungsbedingungen prüfen können – wird gestrichen; in einem Erwägungsgrund wird jedoch klargestellt, dass die Mitgliedstaaten und Europol weiterhin über diesen Mechanismus verfügen.

18. Terroristische Inhalte, die infolge von Entfernungsanordnungen oder infolge spezifischer Maßnahmen entfernt oder gesperrt wurden, sind für einen Zeitraum von sechs Monaten nach ihrer Entfernung oder Sperrung zu speichern; dieser Zeitraum kann verlängert werden, wenn und so lange dies im Zusammenhang mit einer Überprüfung erforderlich ist.

19. Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen der Hostingdiensteanbieter gegen die Verordnung zu verhängen sind. Sanktionen können unterschiedliche Formen annehmen, darunter die förmliche Verwarnung bei geringfügigen Verstößen oder finanzielle Sanktionen bei schwerwiegenderen Verstößen. Im Standpunkt des Rates in erster Lesung ist festgelegt, welche Verstöße mit Sanktionen belegt werden können und welche Umstände bei der Bewertung der Art und Höhe der Sanktionen relevant sind. Den Hostingdiensteanbietern könnten Sanktionen in Höhe von bis zu 4 % ihres erwirtschafteten weltweiten Jahresumsatzes auferlegt werden, sollten sie systematisch oder ständig gegen die Vorschrift verstoßen, innerhalb einer Stunde terroristische Inhalte zu entfernen oder zu sperren.

IV. **FAZIT**

20. Der Standpunkt des Rates entspricht voll und ganz dem Kompromiss, der in den Verhandlungen zwischen dem Europäischen Parlament und dem Rat mithilfe der Kommission erzielt worden ist. Dieser Kompromiss wird mit dem Schreiben des Vorsitzenden des LIBE-Ausschusses des Europäischen Parlaments an den Präsidenten des AStV (2. Teil) vom 13. Januar 2021 bestätigt.

([10]) 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).

ISSN 1977-088X (elektronische Ausgabe)
ISSN 1725-2407 (Papierausgabe)

Amt für Veröffentlichungen
der Europäischen Union
L-2985 Luxemburg
LUXEMBURG

DE