|  |  |
| --- | --- |
| Europäisches Parlament2019-2024 | EP logo RGB_Mute |

Plenarsitzungsdokument

<NoDocSe>A9-0256/2020</NoDocSe>

<Date>{11/12/2020}11.12.2020</Date>

<RefProcLect>\*\*\*I</RefProcLect>

<TitreType>BERICHT</TitreType>

<Titre>über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen</Titre>

<DocRef>(COM(2018)0225 – C8-0155/2018 – 2018/0108(COD))</DocRef>

<Commission>{LIBE}Ausschuss für bürgerliche Freiheiten, Justiz und Inneres</Commission>

Berichterstatterin: <Depute>Birgit Sippel</Depute>

PR\_COD\_1amCom

|  |
| --- |
| Erklärung der benutzten Zeichen |
|  \* Anhörungsverfahren \*\*\* Zustimmungsverfahren \*\*\*I Ordentliches Gesetzgebungsverfahren (erste Lesung) \*\*\*II Ordentliches Gesetzgebungsverfahren (zweite Lesung) \*\*\*III Ordentliches Gesetzgebungsverfahren (dritte Lesung)(Die Angabe des Verfahrens beruht auf der im Entwurf eines Rechtsakts vorgeschlagenen Rechtsgrundlage.) |

|  |
| --- |
| Änderungsanträge zu einem Entwurf eines Rechtsakts |
| **Änderungsanträge des Parlaments in Spaltenform**Streichungen werden durch ***Fett- und Kursivdruck*** in der linken Spalte gekennzeichnet. Textänderungen werden durch ***Fett- und Kursivdruck*** in beiden Spalten gekennzeichnet. Neuer Text wird durch ***Fett- und Kursivdruck*** in der rechten Spalte gekennzeichnet.Aus der ersten und der zweiten Zeile des Kopftextes zu jedem der Änderungsanträge ist der betroffene Abschnitt des zu prüfenden Entwurfs eines Rechtsakts ersichtlich. Wenn sich ein Änderungsantrag auf einen bestehenden Rechtsakt bezieht, der durch den Entwurf eines Rechtsakts geändert werden soll, umfasst der Kopftext auch eine dritte und eine vierte Zeile, in der der bestehende Rechtsakt bzw. die von der Änderung betroffene Bestimmung des bestehenden Rechtsakts angegeben werden.**Änderungsanträge des Parlaments in Form eines konsolidierten Textes**Neue Textteile sind durch ***Fett- und Kursivdruck*** gekennzeichnet. Auf Textteile, die entfallen, wird mit dem Symbol ▌hingewiesen oder diese Textteile erscheinen durchgestrichen. Textänderungen werden gekennzeichnet, indem der neue Text in ***Fett- und Kursivdruck*** steht und der bisherige Text gelöscht oder durchgestrichen wird.Rein technische Änderungen, die von den Dienststellen im Hinblick auf die Erstellung des endgültigen Textes vorgenommen werden, werden allerdings nicht gekennzeichnet. |

INHALT

Seite

ENTWURF EINER LEGISLATIVEN ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS 5

VERFAHREN DES FEDERFÜHRENDEN AUSSCHUSSES 66

NAMENTLICHE SCHLUSSABSTIMMUNG IM FEDERFÜHRENDEN AUSSCHUSS 67

ENTWURF EINER LEGISLATIVEN ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS

zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen

(COM(2018)0225 – C8-0155/2018 – 2018/0108(COD))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

*Das Europäische Parlament*,

– unter Hinweis auf den Vorschlag der Kommission an das Europäische Parlament und den Rat (COM(2018)0225),

– gestützt auf Artikel 294 Absatz 2 und Artikel 82 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage ihm der Vorschlag der Kommission unterbreitet wurde (C8-0155/2018),

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

– gestützt auf Artikel 59 seiner Geschäftsordnung,

– unter Hinweis auf den Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (A9-0256/2020),

1. legt den folgenden Standpunkt in erster Lesung fest;

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

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

Änderungsantrag 1

ABÄNDERUNGEN DES EUROPÄISCHEN PARLAMENTS[[1]](#footnote-1)\*

am Vorschlag der Kommission

---------------------------------------------------------

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische *Informationen* in *Strafverfahren*

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 82 Absatz 1,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[[2]](#footnote-2),

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Die Union hat sich die Erhaltung und Weiterentwicklung eines Raums der Freiheit, der Sicherheit und des Rechts zum Ziel gesetzt. Zum schrittweisen Aufbau eines solchen Raums hat die Union gemäß dem Grundsatz der gegenseitigen Anerkennung gerichtlicher Urteile und Entscheidungen, der seit der Tagung des Europäischen Rates vom 15. und 16. Oktober 1999 in Tampere allgemein als Eckstein der justiziellen Zusammenarbeit in Strafsachen in der Union gilt, Maßnahmen im Bereich der justiziellen Zusammenarbeit in Strafsachen zu erlassen.

(2) Für strafrechtliche Ermittlungen und Strafverfolgungsmaßnahmen in der gesamten Union werden Maßnahmen zur Einholung und Sicherung elektronischer ***Informationen*** immer wichtiger. Wirksame Verfahren zur Einholung elektronischer ***Informationen*** sind für die Bekämpfung von Kriminalität unerlässlich, unterliegen jedoch bestimmten Bedingungen ***und Garantien***, welche die uneingeschränkte Einhaltung der in ***Artikel 6 des Vertrags über die Europäische Union (EUV) und*** der Charta der Grundrechte der Europäischen Union ***(die Charta)*** anerkannten ▌Grundrechte und Grundsätze sicherstellen, insbesondere der Grundsätze der Notwendigkeit und Verhältnismäßigkeit, des ordnungsgemäßen Verfahrens, des ▌Schutzes der Privatsphäre ***und der personenbezogenen Daten sowie der Vertraulichkeit der Kommunikation***.

(3) ▐

(4) ▐

(5) ▐

(6) ▐

(7) Netzbasierte Dienstleistungen können von einem beliebigen Ort aus erbracht werden und erfordern keine physische Infrastruktur, Räumlichkeiten oder Personal in dem ▌Land***, in dem der Dienst angeboten wird***. ***Daher*** werden relevante ***elektronische Informationen*** häufig außerhalb des ermittelnden Staates ▌gespeichert***, was Herausforderungen bezüglich der Einholung elektronischer Informationen in Strafverfahren mit sich bringt***.

(8) ***Daher*** werden Ersuchen um justizielle Zusammenarbeit häufig an Staaten gerichtet, in denen viele Diensteanbieter niedergelassen sind▌. Zudem hat sich die Zahl der Ersuchen ▌ vervielfacht. Dies hat dazu geführt, dass die Einholung elektronischer ***Informationen*** über Kanäle der justiziellen Zusammenarbeit häufig lange dauert***, was aufgrund der Tatsache, dass elektronische Informationen häufig volatil sind, zu Problemen führen kann***. Zudem gibt es keinen ***harmonisierten*** Rahmen für die Zusammenarbeit mit Diensteanbietern, während einige Anbieter aus Drittstaaten direkte Ersuchen um Nichtinhaltsdaten, die nach geltendem innerstaatlichem Recht zulässig sind, akzeptieren. Folglich stützen sich alle Mitgliedstaaten ***zunehmend*** auf ***Kanäle*** für die ***freiwillige direkte*** Zusammenarbeit mit Diensteanbietern, wobei sie unterschiedliche nationale Instrumente, Bedingungen und Verfahren zugrunde legen.

(9) Der fragmentierte Rechtsrahmen stellt ***Strafverfolgungsbehörden, Justizbehörden und*** Diensteanbieter, die ***rechtlichen*** Ersuchen ▌Folge leisten wollen, vor Probleme***, da sie sich mit Rechtsunsicherheit und möglichen Gesetzeskollisionen konfrontiert sehen***. Daher ***müssen spezifische Vorschriften für die grenzüberschreitende justizielle Zusammenarbeit zur Sicherung und Herausgabe elektronischer Informationen vorgeschlagen werden, um das geltende EU-Recht zu ergänzen und die Regeln für die Zusammenarbeit zwischen Strafverfolgungsbehörden, Justizbehörden und Diensteanbietern im Bereich der elektronischen Informationen zu präzisieren und gleichzeitig die uneingeschränkte Einhaltung der in Artikel 6 EUV und der Charta verankerten Grundrechte und Grundsätze sowie der Rechtsstaatlichkeit sicherzustellen***.

***(9a) Die Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates[[3]](#footnote-3) regelt den Erwerb, den Zugang zu und die Vorlage von Beweismitteln in einem Mitgliedstaat für strafrechtliche Ermittlungen und Verfahren in einem anderen Mitgliedstaat. Die in der EEA vorgesehenen Verfahren und Fristen sind für elektronische Informationen, die volatiler sind und leichter und schneller gelöscht werden könnten, möglicherweise nicht geeignet. Die vorliegende Verordnung sieht daher spezifische Verfahren vor, die den Besonderheiten elektronischer Informationen Rechnung tragen. Um jedoch langfristig eine Fragmentierung des Unionsrahmens für die justizielle Zusammenarbeit in Strafsachen zu vermeiden, sollte die Kommission mittelfristig das Funktionieren der Verordnung in Bezug auf die Richtlinie 2014/41/EU bewerten.***

(10) ▐

***(10a) Diese Verordnung wahrt die Grundrechte und die Grundsätze, die in Artikel 6 EUV und in der Charta, im Völkerrecht und durch internationale Übereinkünfte, bei denen die Union oder alle Mitgliedstaaten Vertragsparteien sind, darunter die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten, sowie in den Verfassungen der Mitgliedstaaten in ihren jeweiligen Anwendungsbereichen anerkannt sind. Zu diesen Rechten und Grundsätzen gehören insbesondere die Achtung des Privat- und Familienlebens, der Schutz personenbezogener Daten, das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren, die Unschuldsvermutung und das Recht auf Verteidigung, die Grundsätze der Gesetzmäßigkeit und der Verhältnismäßigkeit sowie das Recht, wegen derselben Straftat nicht zweimal strafrechtlich verfolgt oder bestraft zu werden.***

***(10b) Diese Verordnung darf nicht in dem Sinne ausgelegt werden, dass sie es verbietet, die Ausführung einer Europäischen Herausgabeanordnung zu versagen, wenn objektive Anhaltspunkte dafür vorliegen, dass die Europäischen Herausgabeanordnung zum Zwecke der Verfolgung oder Bestrafung einer Person wegen ihres Geschlechts, ihrer Rasse, ethnischen Herkunft, Religion, sexuellen Ausrichtung oder Geschlechtsidentität, Nationalität, Sprache oder ihrer politischen Überzeugungen erlassen wurde oder dass die Stellung dieser Person aus einem dieser Gründe beeinträchtigt werden kann.***

(11) ***Das Funktionieren des*** Mechanismus der Europäischen Herausgabeanordnung und der Europäischen Sicherungsanordnung für elektronische ***Informationen*** in ***Strafverfahren basiert auf der Voraussetzung des*** gegenseitigen Vertrauens zwischen den Mitgliedstaaten ***und der Vermutung der Einhaltung des Unionsrechts durch andere Mitgliedstaaten, insbesondere der Grundrechte, die*** wesentliche ***Elemente des Raums der Freiheit, der Sicherheit und des Rechts innerhalb der Union sind***. ***Hat die Vollstreckungsbehörde jedoch berechtigten Grund zu der Annahme, dass die Ausführung einer Europäischen Herausgabeanordnung nicht mit ihren in Artikel 6 EUV und der Charta anerkannten Verpflichtungen bezüglich des Schutzes der Grundrechte vereinbar wäre, sollte die Ausführung der Europäischen Herausgabeanordnung versagt werden. Bevor die Vollstreckungsbehörde entscheidet, einen der in dieser Verordnung vorgesehenen Gründe für die Versagung der Anerkennung oder der Ausführung geltend zu machen, sollte sie die Anordnungsbehörde konsultieren, um alle erforderlichen zusätzlichen Informationen einzuholen***. ***Informationen über einen begründeten Vorschlag der Kommission an den Rat auf der Grundlage von Artikel 7 Absatz 1 und Artikel 7 Absatz 2 EUV, der auf systemische oder generelle Mängel hindeutet, sollten für die Zwecke dieser Bewertung von besonderer Bedeutung sein.***

***(11a) Sollte der Europäische Rat gemäß Artikel 7 Absatz 2 EUV einen Beschluss erlassen, in dem festgestellt wird, dass im Anordnungsmitgliedstaat eine schwerwiegende und anhaltende Verletzung der Grundsätze nach Artikel 2 EUV, wie etwa derjenigen, die dem Rechtsstaatsprinzip innewohnen, vorliegt, kann die ausführende Justizbehörde automatisch beschließen, einen der in dieser Verordnung vorgesehenen Gründe für die Versagung der Anerkennung oder der Ausführung geltend zu machen, ohne dass eine spezifische Bewertung vorgenommen werden muss.***

***(11b) Die Achtung des Privat- und Familienlebens und der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sind Grundrechte. Gemäß Artikel 7 und Artikel 8 Absatz 1 der Charta und Artikel 16 Absatz 1 AEUV hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation sowie auf den Schutz der sie betreffenden personenbezogenen Daten. Bei der Durchführung dieser Verordnung sollten die Mitgliedstaaten sicherstellen, dass personenbezogene Daten nur im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[[4]](#footnote-4) und der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates[[5]](#footnote-5) sowie der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates geschützt und verarbeitet werden[[6]](#footnote-6).***

***(11c) Gemäß dieser Verordnung eingeholte personenbezogene Daten sollten nur dann und auf eine solche Weise verarbeitet werden, wie dies für Zwecke der Prävention, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen und der Ausübung des Rechts auf Verteidigung notwendig und verhältnismäßig ist. Insbesondere sollten die Mitgliedstaaten sicherstellen, dass für die Übermittlung personenbezogener Daten von den zuständigen Behörden an die Diensteanbieter für die Zwecke dieser Verordnung geeignete Datenschutzvorkehrungen und -maßnahmen gelten, unter anderem Maßnahmen zur Wahrung der Datensicherheit. Die Diensteanbieter sollten sicherstellen, dass für die Übermittlung personenbezogener Daten an die zuständigen Behörden dieselben Garantien gelten. Der Zugang zu Informationen mit personenbezogenen Daten sollte befugten Personen vorbehalten sein.***

(12) ▐

(13) ▐

***(13a)*** ***Nach der Rechtsprechung des Europäischen Gerichtshofs stellt eine allgemeine und unterschiedslose Vorratsdatenspeicherung durch die nationalen Sicherheitsbehörden der EU einen schwerwiegenden Verstoß gegen die insbesondere in der Charta der Grundrechte der Europäischen Union verankerten Datenschutzvorschriften dar. Daher sollte die Anwendung dieser Verordnung weder zu einer allgemeinen und unterschiedslosen Vorratsspeicherung von Daten führen, noch sollte sie Rechte oder Pflichten von Diensteanbietern in Bezug auf die Sicherheit von Daten, einschließlich des Rechts auf Verschlüsselung, berühren.***

(14) ***Die Verfahrensrechte in Strafverfahren, die*** in den Richtlinien 2010/64/EU[[7]](#footnote-7), 2012/13/EU[[8]](#footnote-8), 2013/48/EU[[9]](#footnote-9), 2016/343[[10]](#footnote-10), 2016/800[[11]](#footnote-11) und 2016/1919[[12]](#footnote-12) des Europäischen Parlaments und des Rates ***verankert sind, sollten innerhalb des Geltungsbereichs dieser Richtlinien bei den unter diese Verordnung fallenden Strafverfahren für die Mitgliedstaaten gelten, die an diese Richtlinien gebunden sind***. ***Die Verfahrensgarantien der Charta sollten für alle unter diese Verordnung fallenden Verfahren gelten.***

***(14a) Hat der Anordnungsmitgliedstaat Grund zu der Annahme, dass in einem anderen Mitgliedstaat möglicherweise ein paralleles Strafverfahren läuft, sollte er die Behörden dieses Mitgliedstaats gemäß dem Rahmenbeschluss 2009/948/JI des Rates[[13]](#footnote-13) konsultieren.***

(15) Mit diesem Instrument werden die Regeln festgelegt, nach denen eine zuständige Justizbehörde in der Europäischen Union mittels einer Europäischen Herausgabe- oder Sicherungsanordnung ***im Rahmen eines Strafverfahrens*** von einem Diensteanbieter, der in der Union Dienstleistungen anbietet, verlangen kann, elektronische ***Informationen, die als*** Beweismittel ***dienen können,*** herauszugeben oder zu sichern. Diese Verordnung gilt in allen ***grenzüberschreitenden*** Fällen, in denen der Diensteanbieter in einem anderen Mitgliedstaat niedergelassen oder***, falls er nicht in der Union niedergelassen ist, rechtlich*** vertreten ist. ***Die Behörden der Mitgliedstaaten sollten keine innerstaatlichen Anordnungen mit extraterritorialen Wirkungen zur Herausgabe oder Sicherung elektronischer Informationen, die auf der Grundlage dieser Verordnung angefordert werden könnten, erlassen.***

(16) Bei den Diensteanbietern, die für die ***Einholung elektronischer Informationen*** in Strafverfahren von besonderer Relevanz sind, handelt es sich um die Anbieter elektronischer Kommunikationsdienste und bestimmte Anbieter von Diensten der Informationsgesellschaft, die die Interaktion zwischen den Nutzern erleichtern. Daher sollten beide Gruppen unter diese Verordnung fallen. Elektronische Kommunikationsdienste sind ***in der*** Richtlinie ***(EU) 2018/1972 des Europäischen Parlaments und des Rates[[14]](#footnote-14)*** definiert. Zu diesen Diensten zählen die interpersonelle Kommunikation wie die Internet-Telefonie („Voice-over-IP“), die Übermittlung von Sofortnachrichten und E-Mail-Dienste. Die Kategorien der ***in dieser Verordnung*** aufgeführten Dienste der Informationsgesellschaft sind diejenigen, bei denen die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung ist; gemeint sind damit insbesondere soziale Netzwerke, soweit sie nicht als elektronische Kommunikationsdienste gelten‚ Online-Marktplätze, die Transaktionen zwischen ihren Nutzern (wie Verbrauchern oder Unternehmen) erleichtern, und andere Hosting-Dienste‚ einschließlich Cloud-Computing-Diensten.

(17) ▐

(18) Anbieter von Internetinfrastrukturdiensten im Zusammenhang mit der Zuweisung von Namen und Nummern wie Domänennamen-Registrierungsstellen und ‑Register sowie ▌Proxy-Diensteanbieter oder regionale Internetregister für IP-Adressen sind besonders wichtig, wenn es um die Ermittlung von Akteuren geht, die für bösartige oder kompromittierte Websites verantwortlich sind. Diese Anbieter besitzen Daten, die ***die*** Identifizierung einer Person oder Einrichtung hinter einer für kriminelle Aktivitäten verwendeten Website oder ▌des Opfers ***einer*** kriminellen Aktivität ermöglichen ***könnten***.

***(18a) Anordnungen nach dieser Verordnung sollten an die Hauptniederlassung des Diensteanbieters oder im Falle von Diensteanbietern, die nicht in einem durch diese Verordnung gebundenen Mitgliedstaat niedergelassen sind, an den vom Diensteanbieter zu diesem Zweck benannten Vertreter gerichtet werden. Im Falle eines Diensteanbieters mit Niederlassungen in mehr als einem Mitgliedstaat, sollte die Hauptniederlassung der Ort seiner Hauptverwaltung in der Union sein, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Datenverarbeitung werden in einer anderen Niederlassung des Diensteanbieters in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall sollte die Niederlassung, die derartige Entscheidungen getroffen hat, als Hauptniederlassung gelten.***

(19) Diese Verordnung regelt nur die Erhebung ***von*** Daten, ▌die ein Diensteanbieter zum Zeitpunkt des ***Erlasses einer Europäischen*** Herausgabe- oder Sicherungsanordnung ***gespeichert hat***. Sie enthält weder eine allgemeine Verpflichtung zur Datenspeicherung noch wird mit ihr das Abfangen von Daten oder die Einholung von Daten, die zu einem späteren Zeitpunkt nach ***Erlass einer Europäischen*** Herausgabe- oder Sicherungsanordnung gespeichert werden, genehmigt.

(20) Zu den Datenkategorien, die unter diese Verordnung fallen, gehören Teilnehmerdaten, ***Verkehrsdaten*** und Inhaltsdaten. ***Diese Kategorien stehen im Einklang mit den*** Rechtsvorschriften vieler Mitgliedstaaten***, dem Unionsrecht wie der Richtlinie 2002/58/EG und der Rechtsprechung des Gerichtshofs sowie dem Völkerrecht, insbesondere dem Übereinkommen des Europarats über Computerkriminalität (SEV-Nr. 185) („Budapester Übereinkommen“).***

(21) ***Teilnehmerdaten*** sollten in dieser Verordnung als gesonderte Datenkategorie betrachtet werden. Die Beschaffung von ***Teilnehmerdaten*** wird ▌zur Identifizierung des ***zugrundeliegenden*** Nutzers ***angestrebt***, und das Ausmaß des Eingriffs in die Grundrechte ist ***geringer als bei anderen, sensibleren Datenkategorien***.

(22) Die Einholung von ***Verkehrsdaten*** hingegen wird in der Regel angestrebt, um Informationen ▌zu erhalten***, die eher in die Persönlichkeitsrechte der Betroffenen eingreifen, wie z. B. über die Kontakte und den Aufenthaltsort des Nutzers***; diese Daten können zur Erstellung eines ***umfassenden*** Profils einer Person herangezogen werden. ***Daher sind Verkehrsdaten in Bezug auf ihre Sensibilität mit Inhaltsdaten vergleichbar***.

***(22a) IP-Adressen können einen entscheidenden Ausgangspunkt für strafrechtliche Ermittlungen darstellen, bei denen die Identität eines Verdächtigen nicht bekannt ist. Nach dem EU-Besitzstand nach der Auslegung durch den Europäischen Gerichtshof sind IP-Adressen als personenbezogene Daten zu betrachten und müssen in vollem Umfang durch den EU-Besitzstand im Bereich des Datenschutzes geschützt werden. Darüber hinaus können sie unter bestimmten Umständen als Verkehrsdaten gelten. Für den Zweck einer bestimmten strafrechtlichen Ermittlung könnten die Strafverfolgungsbehörden jedoch eine IP-Adresse anfordern, um den Nutzer zu identifizieren und in einem weiteren Schritt den Namen oder die Adresse des Teilnehmers oder des registrierten Nutzers zu erhalten. In solchen Fällen sollte die gleiche Regelung wie für Teilnehmerdaten im Sinne dieser Verordnung angewandt werden.***

***(22b) Metadaten können leichter verarbeitet und analysiert werden als Inhaltsdaten, da sie bereits in ein strukturiertes und standardisiertes Format gebracht wurden, jedoch können durch sie, sofern sie aus elektronischen Kommunikationsdiensten oder -protokollen stammen, auch sehr sensible und personenbezogene Daten offengelegt werden. Es ist daher unerlässlich, dass Metadaten*** ***anderer*** ***elektronischer Kommunikationsdienste oder -protokolle, die durch die Nutzung der betreffenden Dienste oder von den Diensteanbeitern gespeichert, übermittelt, verbreitet oder ausgetauscht werden, als Inhaltsdaten zu betrachten sind*.**

(23)Alle Datenkategorien enthalten personenbezogene Daten und fallen somit unter die Garantien im Rahmen der Datenschutzvorschriften der Union‚ doch variiert die Intensität der Auswirkungen auf die Grundrechte ***zwischen den Kategorien***, insbesondere zwischen den ***Teilnehmerdaten*** einerseits und den ***Verkehrs-*** und Inhaltsdaten andererseits. Während ***Teilnehmerdaten und IP-Adressen*** dazu dienen ***könnten***, bei einer Untersuchung erste Hinweise zur Identität eines Verdächtigen zu erhalten, sind ***Verkehrs-*** und Inhaltsdaten ***meistens relevanter*** als Beweismittel ***und könnten letztlich zur Verurteilung des Verdächtigen führen***.Daher ist es von wesentlicher Bedeutung, dass alle diese Datenkategorien unter das Instrument fallen. Wegen des unterschiedlichen Ausmaßes des Eingriffs in die Grundrechte werden unterschiedliche ***Garantien und*** Bedingungen für die Einholung ***solcher*** Daten festgelegt*.*

(24) Die Europäische Herausgabeanordnung und die Europäische Sicherungsanordnung sind Ermittlungsmaßnahmen, die nur im Rahmen eines bestimmten Strafverfahrens ***in Bezug auf eine konkrete***, bereits ***begangene*** Straftat und nach einer individuellen Bewertung der Verhältnismäßigkeit und der Notwendigkeit in jedem Einzelfall erlassen werden sollten***, wobei die Rechte der verdächtigen oder beschuldigten Person zu berücksichtigen sind***.

(25) ▐

(26) Diese Verordnung sollte für Diensteanbieter gelten, die in der Union Dienstleistungen anbieten, und die in dieser Verordnung vorgesehenen Anordnungen dürfen nur für Daten erlassen werden, die in der Union angebotene Dienstleistungen betreffen. Dienstleistungen, die ausschließlich außerhalb der Union angeboten werden, fallen nicht unter diese Verordnung▌.

(27)Damit festgestellt werden kann, ob ein Diensteanbieter Dienstleistungen in der Union anbietet, muss geprüft werden, ob der Diensteanbieter ***offensichtlich beabsichtigt, betroffenen*** Personen***, entweder juristischen oder natürlichen Personen,*** in einem oder mehreren Mitgliedstaaten ***Dienstleistungen in der Union anzubieten***. Allerdings sollte die bloße Zugänglichkeit einer Online-Schnittstelle, beispielsweise die Zugänglichkeit der Website***, einer E-Mail-Adresse oder anderer Kontaktdaten eines*** Diensteanbieters oder eines Vermittlers ***oder die Verwendung einer Sprache, die in dem Drittland, in dem der Diensteanbieter niedergelassen ist, allgemein verwendet wird, nicht als ausreichend angesehen werden, um eine solche Absicht festzustellen***.

(28) Eine wesentliche Verbindung zur Union sollte für die Bestimmung des Anwendungsbereichs dieser Verordnung ebenfalls relevant sein. Eine solche wesentliche Verbindung zur Union sollte dann als gegeben gelten, wenn der Diensteanbieter eine Niederlassung in der Union hat. In Ermangelung einer solchen Niederlassung sollte das Kriterium einer wesentlichen Verbindung anhand der Existenz einer erheblichen Zahl von Nutzern in einem oder mehreren Mitgliedstaaten oder der Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten beurteilt werden. Die Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten ***sollte auf der Grundlage aller relevanten Umstände bestimmt werden***, einschließlich Faktoren wie der Verwendung einer in dem betreffenden Mitgliedstaat gebräuchlichen Sprache oder Währung oder der Möglichkeit, Waren oder Dienstleistungen zu bestellen▌.

***(28a) Situationen, in denen eine unmittelbare Gefahr für das Leben oder die körperliche Unversehrtheit einer Person besteht, sollten als Notfälle behandelt werden und kürzere Fristen für den Diensteanbieter und die Vollstreckungsbehörde vorsehen. Wenn die Störung oder Zerstörung einer kritischen Infrastruktur eine unmittelbare Gefahr für das Leben oder die körperliche Unversehrtheit einer Person darstellen würde, sollte eine solche Situation auch als Notfall im Einklang mit dem EU-Recht behandelt werden.***

(29) Eine Europäische Herausgabeanordnung sollte nur erlassen werden, wenn dies notwendig und verhältnismäßig ist***, wobei die Rechte der verdächtigten oder beschuldigten Person und die Schwere der Straftat zu berücksichtigen sind***. Bei der Prüfung dieser Frage sollte berücksichtigt werden, ob ***sie unter denselben Bedingungen in einem vergleichbaren innerstaatlichen Fall hätte erlassen werden können, ob ausreichend Grund zu der Annahme besteht, dass eine Straftat begangen wurde, wenn sie schwerwiegend genug ist, um die grenzüberschreitende Herausgabe der Daten zu rechtfertigen, und wenn die angeforderten Informationen für diese Ermittlungen relevant sind Die*** Anordnung ***sollte*** auf das Maß beschränkt ***sein***, das ***unbedingt*** erforderlich ist, um das rechtmäßige Ziel der Einholung der relevanten und erforderlichen Daten, die nur in dem betreffenden Einzelfall als Beweismittel dienen können, zu erreichen***, und sie sollte auf Daten bestimmter Personen in direktem Zusammenhang mit dem konkreten Verfahren beschränkt sein***. ***Der direkte Zusammenhang zwischen der Person, deren Daten angefordert werden, und dem Zweck der konkreten Verarbeitung muss jederzeit nachweisbar sein.***

(30) Wenn eine Europäische Herausgabe- oder Sicherungsanordnung erlassen wird, sollte stets eine Justizbehörde entweder am Erlass oder an der Validierung der Anordnung beteiligt sein. Da ***Verkehrs-*** und Inhaltsdaten sensibler sind, muss der Erlass oder die Validierung von Europäischen Herausgabeanordnungen zur Herausgabe von Daten dieser beiden Kategorien von einem Richter überprüft werden. Da ***Teilnehmerdaten*** weniger sensibel sind, können Europäische Herausgabeanordnungen für deren Offenlegung auch von den zuständigen Staatsanwälten erlassen oder validiert werden***, wenn die betreffenden Staatsanwälte in der Lage sind, ihre Aufgaben objektiv wahrzunehmen. Wenn dies im nationalen Recht vorgesehen ist, erfordert die Ausführung der Anordnung möglicherweise die Einbeziehung eines Gerichts im Vollstreckungsstaat in das Verfahren***.

***(30a) Die zuständige Anordnungsbehörde sollte als unabhängig betrachtet werden, wenn sie nicht dem Risiko ausgesetzt ist, in einem konkreten Fall direkt oder indirekt externe Weisungen oder Anweisungen im Zusammenhang mit der Entscheidungsfindung insbesondere von der Exekutive, wie z. B. einem Justizminister, zu erhalten. Diese Unabhängigkeit sollte als gegeben gelten, wenn die zuständige Anordnungsbehörde auf der Grundlage der entsprechenden gesetzlichen Vorschriften und eines institutionellen Rahmens in der Lage ist, ihre Zuständigkeiten objektiv wahrzunehmen und bei der Wahrnehmung ihrer Aufgaben, die mit dem Erlass einer Europäischen Herausgabeanordnung oder Sicherungsanordnung verbunden sind, unabhängig handelt, wobei alle belastenden und entlastenden Beweismittel zu berücksichtigen sind und ohne der Gefahr ausgesetzt zu sein, dass ihre Entscheidungsbefugnis externen Weisungen oder Anweisungen unterliegt.***

(31) Aus dem gleichen Grund muss in Bezug auf den sachlichen Anwendungsbereich dieser Verordnung folgende Unterscheidung getroffen werden: Anordnungen zur Herausgabe von Teilnehmerdaten und ***IP-Adressen zu dem einzigen Zweck der Identifizierung der Person*** können wegen jeder Straftat erlassen werden, wohingegen für den Zugang zu ***Verkehrs-*** und Inhaltsdaten strengere Anforderungen gelten sollten, um dem sensibleren Charakter solcher Daten Rechnung zu tragen. Die Festlegung eines Mindeststrafmaßes ermöglicht ein verhältnismäßigeres Vorgehen; außerdem ist in dieser Verordnung eine Reihe weiterer Ex-ante- und Ex-post-Bedingungen und -Garantien vorgesehen, die für die Wahrung der Verhältnismäßigkeit und der Rechte der betroffenen Personen sorgen sollen. Gleichzeitig sollte ein Mindeststrafmaß die Wirksamkeit des Instruments und seine Anwendung durch die Praktiker nicht einschränken. Den Erlass von Anordnungen für Ermittlungen zuzulassen, bei denen es um Straftaten geht, die mit einer Höchststrafe von mindestens drei Jahren geahndet werden, begrenzt den Anwendungsbereich des Instruments auf schwerere Straftaten, ohne die Möglichkeiten seiner Anwendung durch die Praktiker übermäßig zu beeinträchtigen. Eine erhebliche Zahl von Straftaten, die von den Mitgliedstaaten als weniger schwerwiegend eingestuft werden, was sich in einem niedrigeren Höchststrafmaß niederschlägt, fällt somit nicht in den Anwendungsbereich des Instruments. Ferner ist es von Vorteil, dass das Instrument in der Praxis leicht anwendbar ist.

(32) Es gibt bestimmte Straftatbestände‚ bei denen die ***Informationen*** in der Regel ausschließlich in elektronischer und somit naturgemäß in nicht dauerhafter Form zur Verfügung stehen. Dies gilt für Cyberstraftaten, auch solche, die an sich möglicherweise nicht als schwerwiegend gelten, aber zu weitreichenden oder erheblichen Schäden führen können, insbesondere in Fällen mit geringen individuellen Auswirkungen, aber hohem Gesamtschaden. In den meisten Fällen, in denen die Straftat mithilfe eines Informationssystems begangen wurde, würde die Anwendung desselben Mindeststrafmaßes wie bei anderen Arten von Straftaten hauptsächlich dazu führen, dass Straftaten ungeahndet bleiben. Dies rechtfertigt die Anwendung der Verordnung auch bei den Straftaten, bei denen das Strafmaß weniger als drei Jahre Freiheitsentzug beträgt. Zudem ist bei Straftaten im Zusammenhang mit Terrorismus im Sinne der Richtlinie (EU) 2017/541 ***des Europäischen Parlaments und des Rates[[15]](#footnote-15) sowie bei Straftaten im Zusammenhang mit dem sexuellen Missbrauch und der sexuellen Ausbeutung von Kindern im Sinne der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates[[16]](#footnote-16)*** ein Höchststrafmaß von mindestens drei Jahren nicht erforderlich.

(33) ▐

(34) ▐

(35) Auf Immunitäten und Vorrechte für Personengruppen (wie Diplomaten) oder besonders geschützte Beziehungen (wie das Recht auf Vertraulichkeit der Kommunikation zwischen Anwalt und Mandant***, Quellengeheimnis***) ***oder Vorschriften in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien*** wird in anderen Instrumenten zur gegenseitigen Anerkennung wie der Europäischen Ermittlungsanordnung Bezug genommen. ***Es gibt keine einheitliche Definition dessen, was eine Immunität oder ein Vorrecht im Unionsrecht darstellt. Die genaue Definition dieser Begriffe wird daher dem nationalen Recht überlassen. Dazu können Schutzmaßnahmen gehören, die für medizinische (z. B. Ärzte) und juristische Berufe, Geistliche oder anderweitig geschützte Berater gelten, aber auch, obwohl sie nicht unbedingt als Formen des Vorrechts oder der Immunität angesehen werden, Vorschriften in Bezug auf die Pressefreiheit und die freie Meinungsäußerung in anderen Medien (z. B. für Journalisten). Daher sollte das geltende nationale*** Recht ***bereits*** bei Erlass der Anordnung ***berücksichtigt werden***, da die Anordnungsbehörde die Anordnung nur dann erlassen darf, wenn ***sie unter denselben Bedingungen in einem*** vergleichbaren innerstaatlichen ***Fall hätte*** erlassen werden ***können***. Zusätzlich zu diesem Grundprinzip sollten die Immunitäten und Vorrechte, die ***Daten*** im ***Vollstreckungsstaat*** schützen, im Anordnungsstaat nach Möglichkeit genauso berücksichtigt werden als wären sie im nationalen Recht des Anordnungsstaats vorgesehen. Dies gilt insbesondere, wenn das Recht des ***Vollstreckungsstaats*** einen höheren Schutz vorsieht als das Recht des Anordnungsstaats. Als zusätzliche Schutzmaßnahme sollten diese Aspekte nicht nur beim Erlass der Anordnung berücksichtigt werden, sondern auch zu einem späteren Zeitpunkt***, während des Notifizierungsverfahrens oder*** bei der Prüfung der Relevanz und Zulässigkeit der betreffenden Daten in der jeweiligen Phase des Strafverfahrens und im Falle eines Vollstreckungsverfahrens durch die ***Vollstreckungsbehörde***.

(36) Die Europäische Sicherungsanordnung kann wegen jeder Straftat erlassen werden***, wenn sie unter denselben Bedingungen in einem vergleichbaren innerstaatlichen Fall im Anordnungsstaat hätte erlassen werden können, wenn ausreichend Grund zu der Annahme besteht, dass eine Straftat begangen wurde, wenn sie schwerwiegend genug ist, um die grenzüberschreitende Sicherung der Daten zu rechtfertigen, und wenn die angeforderten Informationen für diese Ermittlungen relevant sind***. ***Sie ist auf Daten bestimmter Personen beschränkt, die in direktem Zusammenhang mit den in dieser Verordnung genannten konkreten Verfahren stehen, und der direkte Zusammenhang zwischen der Person, deren Daten angefordert werden, und dem Zweck der konkreten Verarbeitung muss jederzeit nachweisbar sein.*** Ziel ***der Europäischen Sicherungsanordnung ist es***, die Entfernung, Löschung oder Änderung relevanter Daten in Situationen zu verhindern, in denen mehr Zeit für die Erwirkung der Herausgabe dieser Daten benötigt wird ▐.

(37) Europäische Herausgabe- und Sicherungsanordnungen sollten an ***die Hauptniederlassung des Diensteanbieters, in der sich der für die Verarbeitung Verantwortliche befindet, oder, falls dieser nicht in der Union oder einem der durch diese Verordnung gebundenen Mitgliedstaaten niedergelassen ist, an seinen*** vom Diensteanbieter benannten Vertreter gerichtet werden. ***Gleichzeitig sollte sie direkt an die Vollstreckungsbehörde gerichtet werden.***

(38) Europäische Herausgabe- und Sicherungsanordnungen sollten ▐in Form eines Zertifikats über eine Europäische Herausgabeanordnung („European Production Order Certificate“, EPOC) beziehungsweise eines Zertifikats über eine Europäische Sicherungsanordnung („European Preservation Order Certificate“, EPOC-PR) übermittelt werden ▐. Die Zertifikate sollten dieselben obligatorischen Angaben enthalten wie die Anordnungen ▐. Erforderlichenfalls ***sollte*** ein Zertifikat in eine der Amtssprachen des ***Vollstreckungsstaats und des Diensteanbieters*** oder in eine andere Amtssprache, der ***der Mitgliedstaat oder*** der Diensteanbieter zugestimmt hat, übersetzt werden. ***In diesem Zusammenhang sollten die Mitgliedstaaten jederzeit das Recht haben, in einer der Kommission übermittelten Erklärung anzugeben, dass sie Übersetzungen von EPOC und EPOC-PR in einer oder mehreren Amtssprachen der Union, die nicht die Amtssprache oder Amtssprachen des jeweiligen Mitgliedstaats sind, akzeptieren. Die Kommission sollte die Erklärungen allen Mitgliedstaaten und dem Europäischen Justiziellen Netz für Strafsachen zur Verfügung stellen.***

(39) Die zuständige Anordnungsbehörde sollte das EPOC oder das EPOC-PR ***über ein gemeinsames europäisches digitales Austauschsystem, das von der Kommission bis zum [Datum der Anwendung dieser Verordnung] eingerichtet wird,*** direkt an ***die*** Adressaten übermitteln***. Dieses System sollte gesicherte Kanäle für die Abwicklung autorisierter grenzüberschreitender Kommunikation, die Authentifizierung und die Übermittlung der Anordnungen und der angeforderten Daten zwischen den zuständigen Behörden und den Diensteanbietern ermöglichen, indem es einen wirksamen, zuverlässigen und reibungslosen Austausch der relevanten Informationen und ein hohes Maß an Sicherheit, Vertraulichkeit und Integrität sowie den notwendigen Schutz der Privatsphäre und der personenbezogenen Daten im Einklang mit der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[[17]](#footnote-17), der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und der Richtlinie 2002/58/EG gewährleistet. Zu diesem Zweck sollten offene und gängige elektronische Signatur- und Verschlüsselungstechnologien eingesetzt werden, die dem neuesten Stand der Technik entsprechen. Das System sollte den Adressaten auch*** einen schriftlichen Nachweis unter Bedingungen ***ermöglichen***, die ***den*** ***Adressaten*** die Feststellung der Echtheit ***der Anordnung und der Anordnungsbehörde*** gestatten.

***(39a) Wenn Diensteanbieter oder Mitgliedstaaten bereits spezielle Systeme oder andere gesicherte Kanäle für die Bearbeitung von Datenersuchen für Strafverfolgungszwecke eingerichtet haben, sollte es möglich sein, diese Systeme oder Kanäle mit diesem gemeinsamen europäischen digitalen Austauschsystem zu verbinden.***

(40) ***Bei Erhalt eines EPOC für Teilnehmerdaten oder IP-Adressen zum alleinigen Zweck der Identifizierung einer Person sollte der Diensteanbieter sicherstellen, dass*** die angeforderten Daten ▐spätestens innerhalb von zehn Tagen nach Erhalt des EPOC ***und in dringenden Fällen innerhalb von 16 Stunden an die Anordnungsbehörde*** übermittelt werden. ***Entscheidet die Vollstreckungsbehörde, einen der in dieser Verordnung aufgeführten Gründe für die Versagung der Anerkennung oder der Ausführung innerhalb der Fristen geltend zu machen, sollte sie die Anordnungsbehörde und den Diensteanbieter unverzüglich von ihrer Entscheidung in Kenntnis setzen. Die Anordnungsbehörde sollte die Daten löschen. Wurden die angeforderten Daten noch nicht an die Anordnungsbehörde übermittelt, darf der Diensteanbieter, an den die Anordnung gerichtet ist, die Daten nicht übermitteln.***

***(40a) Nach Erhalt eines EPOC für Verkehrs- oder Inhaltsdaten sollte der Diensteanbieter zügig handeln, um die angeforderten Daten zu sichern. Hat die Vollstreckungsbehörde einen der in dieser Verordnung aufgeführten Gründe für die Versagung der Anerkennung oder der Ausführung innerhalb der Fristen geltend gemacht, sollte sie die Anordnungsbehörde und den Diensteanbieter unverzüglich von ihrer Entscheidung in Kenntnis setzen. Unterliegt der Anordnungsstaat einem Verfahren nach Artikel 7 Absatz 1 oder 2 EUV, sollte der Diensteanbieter die angeforderten Daten erst nach ausdrücklicher schriftlicher Genehmigung durch die Vollstreckungsbehörde übermitteln. Unbeschadet dieser besonderen Bestimmung sollte der Diensteanbieter in Fällen, in denen die Vollstreckungsbehörde keinen der in dieser Verordnung aufgeführten Gründe innerhalb der Fristen geltend gemacht hat, sicherstellen, dass die angeforderten Daten unverzüglich direkt an die Anordnungsbehörde oder die Strafverfolgungsbehörden, wie im EPOC angegeben, übermittelt werden.***

(41) ▐

(42) Nach Erhalt eines EPOC-PR sollte der Diensteanbieter sollte der Diensteanbieter ***zügig handeln, um*** die angeforderten Daten für höchstens 60 Tage ***zu*** sichern***. Die 60-Tage-Frist ist so berechnet, dass ein offizielles Ersuchen um Herausgabe gestellt werden kann. Sie kann nur dann um weitere 30 Tage verlängert werden, wenn dies erforderlich ist, um eine weitere Bewertung der Relevanz der Daten für die laufenden Ermittlungen zu ermöglichen, um zu verhindern, dass potenziell relevante Daten vor Ablauf der Europäischen Sicherungsanordnung verloren gehen. Übermittelt*** die Anordnungsbehörde ***den Adressaten die anschließende Europäische Herausgabeanordnung innerhalb dieser Fristen, sollte der Diensteanbieter die*** Daten ***so lange sichern, wie es für die Ausführung der Europäischen Herausgabeanordnung erforderlich ist***.

***(42a) Um dem Diensteanbieter die Möglichkeit zu geben, in Fällen, in denen das EPOC oder das EPOC-PR in Form oder Inhalt unvollständig sein, offensichtliche Fehler enthalten oder nicht genügend Informationen für die Ausführung der Anordnung enthalten könnte, Probleme zu beheben, muss ein Kommunikationsverfahren festgelegt werden, um die Anordnungsbehörde um Klärung oder erforderlichenfalls Berichtigung zu ersuchen. Darüber hinaus kann es Fälle geben, in denen der Diensteanbieter die Informationen im Falle höherer Gewalt oder einer faktischen Unmöglichkeit, die er nicht zu vertreten hat, aus anderen Gründen überhaupt nicht, nicht vollständig oder nicht fristgerecht bereitstellen kann. Solche Gründe können technischer oder betrieblicher Natur sein (z. B. betriebliche Zwänge bei kleinen und mittleren Unternehmen). In diesen Fällen sollte der Diensteanbieter sich an die Anordnungsbehörden wenden und seine Ansicht angemessen begründen, ebenso wie in Fällen, in denen er die Anordnung für offensichtlich missbräuchlich oder übertrieben hält. So stünde beispielsweise eine Anordnung, mit der die Herausgabe von Daten gefordert wird, die eine nicht definierte Personengruppe in einem geografischen Gebiet betreffen oder in keiner Verbindung zu einem konkreten Strafverfahren stehen, in offensichtlichem Widerspruch zu den Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung. Das Kommunikationsverfahren sollte allgemein die Berichtigung oder erneute Prüfung des EPOC durch die Anordnungsbehörde in einem frühen Stadium ermöglichen. Ist eine Klärung oder Berichtigung erforderlich, sollte die Anordnungsbehörde zügig und spätestens innerhalb von fünf Tagen reagieren. Reagiert die Anordnungsbehörde nicht, sollte die Anordnung als null und nichtig betrachtet werden. Sind die entsprechenden Bedingungen erfüllt, sollte die Anordnungsbehörde eine neue Frist setzen oder die Anordnung zurückziehen. Um die Verfügbarkeit der Daten zu gewährleisten, sollte der Diensteanbieter die angeforderten Daten während dieses Verfahrens sichern, soweit dies möglich ist.***

***(42b) Ungeachtet des Grundsatzes des gegenseitigen Vertrauens sollte die Vollstreckungsbehörde die Möglichkeit haben, die Anerkennung oder Ausführung einer Europäischen Herausgabeanordnung zu verweigern, wenn diese Verweigerung darauf beruht, dass die Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung gemäß dieser Verordnung nicht erfüllt sind, oder auf weiteren spezifischen Gründen, die in dieser Verordnung aufgeführt sind.***

***(42c) Der Grundsatz „ne bis in idem“ ist ein grundlegender Rechtsgrundsatz in der Union, der in der Charta anerkannt ist und in der Rechtsprechung des Gerichtshofs entwickelt wurde. Daher sollte die Vollstreckungsbehörde bei der Bewertung der Anordnung die Ausführung einer Europäischen Herausgabeanordnung ablehnen, wenn ihre Ausführung diesem Grundsatz zuwiderlaufen würde.***

***(42d) Außerdem sollte die Vollstreckungsbehörde die Ausführung einer Europäischen Herausgabeanordnung ablehnen, wenn sie die Anordnung bewertet und berechtigter Grund zu der Annahme besteht, dass die Ausführung der Europäischen Herausgabeanordnung mit den Verpflichtungen des Mitgliedstaats gemäß Artikel 6 EUV und der Charta unvereinbar wäre.***

***(42e) Wenn die Anerkennung oder Ausführung einer Europäischen Herausgabeanordnung die Verletzung einer Immunität oder eines Vorrechts im Vollstreckungsstaat nach sich ziehen würde, sollte die Vollstreckungsbehörde diese Anordnung außerdem in den Fällen ablehnen, in denen sie von der Vollstreckungsbehörde bewertet wird.***

***(42f) Aufgrund des stärker in die Privatsphäre eingreifenden Charakters Europäischer Herausgabeanordnungen für Verkehrs- und Inhaltsdaten sollten der Vollstreckungsbehörde für diese Datenkategorien zusätzliche fakultative Gründe für die Versagung der Anerkennung oder der Ausführung zur Verfügung stehen.***

(43) ***Da die Unterrichtung der Person, deren Daten angefordert werden, ein wesentliches Element im Hinblick auf die Datenschutzrechte und die Verteidigungsrechte ist, um eine wirksame Überprüfung und einen wirksamen Rechtsbehelf gemäß Artikel 6 EUV und der Charta zu ermöglichen, sollte der Diensteanbieter*** die Person, deren Daten angefordert werden, hierüber ***unverzüglich*** informieren. ***Bei der Unterrichtung der Person sollte der Diensteanbieter die erforderlichen betrieblichen und technischen Maßnahmen, die dem neuesten Stand der Technik entsprechen, ergreifen, um die Sicherheit, Vertraulichkeit und Integrität des EPOC oder des EPOC-PR und der herausgegebenen oder gesicherten Daten zu gewährleisten.***

***(43a) So lange wie dies notwendig und verhältnismäßig ist, um eine Behinderung des betreffenden Strafverfahrens zu vermeiden oder die Grundrechte einer anderen Person zu schützen, kann die Anordnungsbehörde unter gebührender Berücksichtigung der Auswirkungen der Maßnahme auf die Grundrechte der Person, deren Daten angefordert werden, den Diensteanbieter auf der Grundlage einer gerichtlichen Anordnung, die hinreichend begründet sein, die Dauer der Geheimhaltungspflicht angeben und einer regelmäßigen Überprüfung unterliegen sollte, auffordern, davon abzusehen, die Person, deren Daten angefordert werden, hiervon in Kenntnis zu setzen. Fordert die Anordnungsbehörde den Diensteanbieter auf, die Person nicht in Kenntnis zu setzen, sollte die Anordnungsbehörde die Person, deren Daten angefordert werden, unverzüglich von der Herausgabe oder Sicherung der Daten in Kenntnis setzen. Diese Unterrichtung könnte so lange verzögert werden, wie dies unter Berücksichtigung der Rechte der verdächtigten und beschuldigten Person und unbeschadet der Verteidigungsrechte und wirksamer Rechtsbehelfe erforderlich und verhältnismäßig ist. Nutzerinformationen sollten Informationen über alle verfügbaren Rechtsbehelfe, die in dieser Verordnung genannt sind, enthalten.***

***(43b) Elektronische Informationen, die auf der Grundlage dieser Verordnung erlangt wurden, sollten nicht für andere Verfahren als diejenigen verwendet werden, für die sie gemäß dieser Verordnung erlangt wurden, es sei denn, es besteht eine akute Gefahr für das Leben oder die körperliche Unversehrtheit einer Person. Wenn die Störung oder Zerstörung einer kritischen Infrastruktur unmittelbar eine akute Gefahr für das Leben oder die körperliche Unversehrtheit einer Person bedeuten würde, sollte eine solche Situation im Einklang mit dem EU-Recht ebenfalls als akute Gefahr für das Leben oder die körperliche Unversehrtheit einer Person angesehen werden.***

***(43c) Elektronische Informationen, die unter Verstoß gegen eine der in dieser Verordnung aufgeführten Bedingungen erhoben wurden, sollten unverzüglich gelöscht werden. Elektronische Informationen, die für die Ermittlungen oder die Strafverfolgung, für die sie herausgegeben oder gesichert wurden, nicht mehr erforderlich sind, einschließlich für etwaige Rechtsbehelfe, sollten ebenfalls unverzüglich gelöscht werden, es sei denn, dies würde die Verteidigungsrechte der verdächtigten oder beschuldigten Person beeinträchtigen. Zu diesem Zweck sollte festgelegt werden, dass regelmäßig überprüft wird, ob die elektronischen Informationen noch gespeichert werden müssen. Die Person, deren Daten angefordert werden, sollte über die Löschung in Kenntnis gesetzt werden.***

***(43d) Elektronische Informationen, die unter Verstoß gegen diese Verordnung gesammelt wurden, sollten vor Gericht nicht zugelassen sein. Dies sollte auch für alle Fälle gelten, in denen die in dieser Verordnung festgelegten Kriterien nicht erfüllt sind. Wurden elektronische Informationen erlangt, bevor ein in dieser Verordnung aufgeführter Grund für die Versagung der Anerkennung geltend gemacht wurde, sollten sie ebenfalls vor Gericht nicht zugelassen sein. Bei der Bewertung der Zulässigkeit elektronischer Informationen, die nach dieser Verordnung erlangt wurden, sollten die zuständigen Justizbehörden in jedem Stadium des Verfahrens sicherstellen, dass die Verteidigungsrechte und die Fairness des Verfahrens gewahrt bleiben. Bei einer solchen Bewertung sollten die zuständigen Justizbehörden auch gebührend berücksichtigen, ob die in dieser Verordnung festgelegten Kriterien erfüllt wurden, insbesondere wenn die angeforderten Daten durch Immunitäten oder Vorrechte geschützt sein könnten.***

***(43e) Auf Antrag des Diensteanbieters sollte der Anordnungsstaat die dem Diensteanbieter entstandenen gerechtfertigten Kosten im Zusammenhang mit der Ausführung der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung erstatten. Zu diesem Zweck sollten die Mitgliedstaaten die Kommission über die Vorschriften für die Erstattung informieren, die die Kommission veröffentlichen sollte. Ist der Diensteanbieter aus praktischen Gründen, wie der wirtschaftlichen Größe des Diensteanbieters, unterschiedlichen Sprachregelungen zwischen dem Anordnungsstaat und dem Vollstreckungsstaat oder unterschiedlichen nationalen Vorschriften für die Kostenerstattung zwischen diesen Staaten, erheblich daran gehindert, die Erstattung von Kosten im Zusammenhang mit der Ausführung einer Europäischen Herausgabeanordnung oder einer Europäischen Ermittlungsanordnung beim Anordnungsstaat geltend zu machen, sollte der Diensteanbieter berechtigt sein, die Erstattung der Kosten beim Vollstreckungsstaat zu beantragen. Wählt der Diensteanbieter den Vollstreckungsstaat, sollte der Anordnungsstaat dem Vollstreckungsstaat diese Kosten erstatten.***

***(43f) Die Mitgliedstaaten sollten die Vorschriften über Sanktionen festlegen, die bei Verstößen gegen die Verpflichtungen gemäß dieser Verordnung zu verhängen sind. Diese Sanktionen sollten wirksam, verhältnismäßig und abschreckend sein. Wenn die angemessene Sanktion für Verstöße von Diensteanbietern festgelegt wird, sollten die zuständigen Behörden alle einschlägigen Umstände berücksichtigen, beispielsweise Art, Schwere und Dauer des Verstoßes, ob der Verstoß absichtlich oder fahrlässig begangen wurde, und ob der Diensteanbieter bereits vergleichbare Verstöße zu verantworten hatte. Besonderes Augenmerk sollte in dieser Hinsicht auf Kleinstunternehmen gelegt werden.***

***(43g) Handelt ein Diensteanbieter mit der gebotenen Sorgfalt, insbesondere im Hinblick auf Datenschutzverpflichtungen, und hat er die Anordnungsbehörde gemäß dieser Verordnung um Klärung oder Rechtfertigung ersucht, sollte er nicht für die Folgen etwaiger Verzögerungen haftbar gemacht werden. Darüber hinaus sollten Sanktionen, die bei Verstößen gegen die Verpflichtungen des Diensteanbieters gemäß dieser Verordnung verhängt wurden, aufgehoben werden, wenn eine Anordnung gemäß dieser Verordnung erfolgreich angefochten wurde.***

(44) ***Kommt der Diensteanbieter einem EPOC innerhalb der Fristen oder einem EPOC-PR nicht nach, ohne ausreichende Gründe anzugeben, und hat die Vollstreckungsbehörde in Bezug auf das EPOC keinen der in dieser Verordnung vorgesehenen Gründe geltend gemacht,*** kann die Anordnungsbehörde ▐die zuständige Behörde des ***Vollstreckungsstaats ersuchen, die Anordnung auszuführen***. ***In einem solchen Fall sollte der Vollstreckungsstaat den Diensteanbieter förmlich auffordern, der Anordnung nachzukommen, und ihn über die Möglichkeit informieren, die Ausführung zu verweigern, indem er einen der Gründe geltend macht, die dem Diensteanbieter nach dieser Verordnung für eine Berichtigung oder erneute Prüfung der Anordnung zur Verfügung stehen.*** ***Kommt ein Diensteanbieter seinen Verpflichtungen immer noch nicht nach, sollten die Mitgliedstaaten eine Sanktion gemäß dieser Verordnung verhängen.***

(45) ▐

(46) ▐

(47) Neben den Personen, ***um*** deren Daten ***ersucht wird, kann*** auch ***das Recht eines Drittstaats*** von der Ermittlungsmaßnahme betroffen sein. ***In solchen Situationen wäre die justizielle Zusammenarbeit auf der Grundlage internationaler Übereinkünfte im Allgemeinen der geeignetste Weg, um elektronische Informationen anzufordern, wenn es zu Gesetzeskollisionen mit einem Drittstaat kommt. Unbeschadet solcher internationaler Übereinkünfte und*** um im Hinblick auf die souveränen Interessen von Drittstaaten ein entgegenkommendes Verhalten sicherzustellen, den Betroffenen zu schützen und einander widersprechenden Verpflichtungen für Diensteanbieter entgegenzuwirken, ist in dieser Verordnung ein spezielles Verfahren für die ▐ Überprüfung vorgesehen, wenn ***der Diensteanbieter oder die Vollstreckungsbehörde der Auffassung ist, dass*** die Befolgung einer Europäischen Herausgabeanordnung ***oder einer Europäischen Sicherungsanordnung mit den geltenden Rechtsvorschriften eines Drittstaats kollidieren*** würde, ***die eine Offenlegung der betreffenden Daten verbieten***.

(48) Zu diesem Zweck sollte der ***Diensteanbieter oder die Vollstreckungsbehörde***, wenn er***/sie*** der Auffassung ist, dass die Europäische Herausgabeanordnung ***oder die Europäische Sicherungsanordnung*** im konkreten Fall eine Verletzung einer aus dem Recht eines Drittstaats erwachsenden Verpflichtung zur Folge hätte, die Anordnungsbehörde ***und die betreffenden Adressaten unverzüglich, spätestens jedoch innerhalb von zehn Tagen nach Erhalt der Anordnung,*** hiervon in Kenntnis setzen ***und damit die Ausführung der Anordnung aussetzen***. ***Eine solche Mitteilung sollte alle relevanten Einzelheiten über das Recht des Drittstaats, seine Anwendbarkeit im vorliegenden Fall und die Art der kollidierenden Verpflichtung enthalten.*** Die Anordnungsbehörde sollte dann ***innerhalb von zehn Tagen nach Erhalt der Mitteilung*** die Europäische Herausgabeanordnung ***oder die Europäische Sicherungsanordnung*** überprüfen, ***wobei sie*** Kriterien ***wie die durch das einschlägige Recht geschützten Interessen, den Zusammenhang zwischen der Strafsache und dem Drittstaat, die Verbindung zwischen dem Diensteanbieter und dem Drittstaat, die Interessen des Anordnungsstaates an der Erlangung der elektronischen Informationen und die möglichen Konsequenzen der Befolgung der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung für die Adressaten berücksichtigt***. ***Während dieses Verfahrens sollten die angeforderten Daten nach Möglichkeit gesichert werden.***

***(48a) Die Anordnungsbehörde sollte die Anordnung bei Bedarf zurücknehmen, aufrechterhalten oder anpassen können, um die einschlägigen Kriterien umzusetzen. Im Fall einer Rücknahme sollte die Anordnungsbehörde die Adressaten unverzüglich davon in Kenntnis setzen. Entscheidet die Anordnungsbehörde, die Anordnung aufrechtzuerhalten, sollte sie die Adressaten von ihrer Entscheidung in Kenntnis setzen. Die Vollstreckungsbehörde sollte unter gebührender Berücksichtigung der Entscheidung der Anordnungsbehörde innerhalb von zehn Tagen nach Eingang der Entscheidung der Anordnungsbehörde eine endgültige Entscheidung auf der Grundlage der in dieser Verordnung aufgeführten Kriterien treffen und die Anordnungsbehörde und den Diensteanbieter von ihrer endgültigen Entscheidung in Kenntnis setzen.***

(49) Bei der Prüfung, ob in dem betreffenden Fall ein Widerspruch zwischen verschiedenen Verpflichtungen besteht, ***sollten die Anordnungsbehörde und die Vollstreckungsbehörde im Einklang mit der Richtlinie (EU) 2016/680 und soweit dies die in dieser Verordnung vorgesehenen Fristen nicht behindert, Informationen von der zuständigen Behörde des Drittstaats einholen***, beispielsweise wenn die Überprüfung Fragen zur Auslegung des Rechts des betreffenden Drittstaats aufwirft.

(50) Das Fachwissen über die Auslegung könnte gegebenenfalls auch durch Sachverständigengutachten eingeholt werden. Informationen und die Rechtsprechung zur Auslegung der Rechtsvorschriften ***eines Drittstaats*** und zu Verfahren in Bezug auf widersprüchliche Bestimmungen in den Mitgliedstaaten sollten auf einer zentralen Plattform wie dem Projekt SIRIUS und/oder dem Europäischen Justiziellen Netz zur Verfügung gestellt werden***, um*** von den Erfahrungen und dem Fachwissen ▐ zu denselben oder ähnlichen Fragen zu profitieren. Eine erneute Konsultation des Drittstaats sollte gegebenenfalls aber dennoch möglich sein.

(51) ▐

(52) ▐

(53) ▐

(54) ▐ Im Einklang mit Artikel 47 der Charta der Grundrechte der Europäischen Union ***ist es von wesentlicher Bedeutung, dass alle Personen, deren Daten im Wege einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung angefordert wurden, unbeschadet der nach der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 verfügbaren Rechtsbehelfe das Recht haben, in dem Anordnungsstaat und dem Vollstreckungsstaat gemäß nationalem Recht wirksame Rechtsbehelfe gegen diese Anordnungen einzulegen, einschließlich der*** Möglichkeit ▐, die Rechtmäßigkeit ***der Anordnung***, einschließlich ***ihrer*** Notwendigkeit und Verhältnismäßigkeit▐, anzufechten. ***Die sachlichen Gründe für den Erlass der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung sollten im Anordnungsstaat angefochten werden; dies lässt die Garantien der Grundrechte im Vollstreckungsstaat unberührt***. ***Die Anordnungsbehörde und die Vollstreckungsbehörde sollten geeignete Maßnahmen ergreifen, um sicherzustellen, dass Informationen über die Möglichkeiten, Rechtsbehelfe nach nationalem Recht einzulegen, rechtzeitig zur Verfügung gestellt werden, auch darüber, wann diese Rechtsbehelfe eingelegt werden können, und um sicherzustellen, dass sie wirksam ausgeübt werden können.***

(55) ▐

(56) ▐

(57) ▐

***(57a) Für das Monitoring der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung sollte die Kommission auf der Grundlage der von den Mitgliedstaaten eingegangenen Daten einen Jahresbericht über das vorangegangene Kalenderjahr veröffentlichen. Zu diesem Zweck sollten die Mitgliedstaaten eine ausführliche Statistik führen, die sie anhand der bei den zuständigen Behörden erhobenen Daten zu verschiedenen Aspekten dieser Verordnung erstellen, und zwar aufgeschlüsselt nach der Art der angeforderten Daten, den Adressaten (angesprochene Exekutivbehörde), der Art des angesprochenen Diensteanbieters [elektronische Kommunikationsdienste, Dienste der Informationsgesellschaft oder Internetdomänennamen- und IP-Adressendienste (wie IP-Adressenanbieter, Domänennamen-Register, Domänennamen-Registrierungsstellen und damit verbundene Proxy-Dienste)] und danach aufgeschlüsselt, ob es sich um einen Notfall handelte oder nicht. Gegebenenfalls sollten die erhobenen Daten auch die geltend gemachten Gründe für die Versagung der Anerkennung oder der Ausführung, die eingelegten Rechtsmittel, die verhängten Sanktionen, die vom Diensteanbieter geltend gemachten Kosten und das eingeleitete Vollstreckungsverfahren enthalten.***

(58) Die Kommission sollte eine Bewertung dieser Verordnung vornehmen, die sich auf die fünf Kriterien Effizienz, Wirksamkeit, Relevanz, Kohärenz und EU-Mehrwert stützen***,*** die Grundlage für Folgenabschätzungen▐bilden ***und eine Bewertung der Inanspruchnahme von Ausnahmeregelungen (Ausnahmeregelung für Notfälle, Ausnahmeregelung vom Grundsatz der Nutzerinformationen) sowie eine Bewertung des Funktionierens des gemeinsamen europäischen Austauschsystems und des Funktionierens dieser Verordnung in Bezug auf die Richtlinie 2014/41/EU umfassen*** sollte. Es sollten regelmäßig Informationen eingeholt werden, die in die Bewertung dieser Verordnung einfließen.

(59) Die Verwendung vorübersetzter und standardisierter Formulare erleichtert die Zusammenarbeit und den Informationsaustausch zwischen ***verschiedenen*** Justizbehörden s***owie mit*** Diensteanbietern ***und ermöglicht eine schnellere und wirksamere Übermittlung elektronischer Informationen*** in benutzerfreundlicher Weise ▐. Solche Formulare ***könnten auch*** die Übersetzungskosten ***senken und*** zu einem hohen Qualitätsstandard ***beitragen***. Antwortformulare sollten einen standardisierten Informationsaustausch ermöglichen▐. Zudem dürften die Formulare auch die Erhebung von Statistiken erleichtern.

(60) ▐

(61) Für die Einholung ***elektronischer Informationen*** sollten die auf dieser Verordnung basierenden Maßnahmen Europäische Ermittlungsanordnungen gemäß der Richtlinie 2014/41/EU ***oder Rechtshilfeverfahren*** nicht ersetzen. Die Behörden der Mitgliedstaaten sollten das für ihre jeweilige Situation am besten geeignete Instrument auswählen; unter Umständen ziehen sie die Europäische Ermittlungsanordnung vor, wenn sie um eine Reihe verschiedener Arten von Ermittlungsmaßnahmen ersuchen, die unter anderem die Herausgabe elektronischer ***Informationen*** aus einem anderen Mitgliedstaat umfassen.

(62) ▐

(63) Da das Ziel dieser Verordnung, nämlich die Verbesserung der grenzüberschreitenden Sicherstellung und Einholung elektronischer ***Informationen***, von den Mitgliedstaaten aufgrund seines grenzüberschreitenden Charakters nicht ausreichend verwirklicht werden kann, sondern auf Unionsebene besser zu verwirklichen ist, kann die Union gemäß dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Erreichung dieses Ziels erforderliche Maß hinaus.

(64) Gemäß Artikel 3 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts ***hat*** Irland schriftlich mitgeteilt, dass ***es*** sich an der Annahme und der Anwendung dieser Verordnung beteiligen ***möchte, und*** das Vereinigte Königreich ***beteiligt sich*** unbeschadet des Artikels 4 des Protokolls nicht an der Annahme dieser Verordnung, die daher für ***das Vereinigte Königreich*** weder bindend noch ***diesem Staat*** gegenüber anwendbar ist.

(65) Nach den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 22 über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Verordnung, die daher für Dänemark weder bindend noch diesem Staat gegenüber anwendbar ist.

(66) Der Europäische Datenschutzbeauftragte wurde gemäß ***Artikel 42*** Absatz 2 der Verordnung ***(EU) 2018/1725*** des Europäischen Parlaments und des Rates[[18]](#footnote-18) angehört und gab am ***6. November 2019*** eine Stellungnahme[[19]](#footnote-19) ab –

HABEN FOLGENDE VERORDNUNG ERLASSEN:

Kapitel 1: Gegenstand, Begriffsbestimmungen und Anwendungsbereich

Artikel 1

Gegenstand

(1) Mit dieser Verordnung werden die Regeln festgelegt, nach denen eine Behörde eines Mitgliedstaats ***im Rahmen eines Strafverfahrens*** von einem Diensteanbieter, der in der Union Dienstleistungen anbietet ***und der in einem anderen Mitgliedstaat niedergelassen ist oder – falls er dort nicht niedergelassen ist – rechtlich vertreten ist***, verlangen kann, elektronische ***Informationen, die als*** Beweismittel ***dienen können,*** herauszugeben oder zu sichern, unabhängig davon, wo sich die Daten befinden.

 ***Die Behörden der Mitgliedstaaten erlassen keine innerstaatlichen Anordnungen mit extraterritorialen Wirkungen zur Herausgabe oder Sicherung elektronischer Informationen, die auf der Grundlage dieser Verordnung angefordert werden könnten.***

***(1a) Der Erlass einer Europäischen Herausgabeanordnung oder Sicherungsanordnung kann auch im Namen einer verdächtigten oder beschuldigten Person im Rahmen der geltenden Verteidigungsrechte im Einklang mit den nationalen strafrechtlichen Verfahren beantragt werden.***

(2) Diese Verordnung berührt nicht die Verpflichtung zur Achtung der Grundrechte und der Rechtsgrundsätze, die ***in der Charta und*** in Artikel 6 EUV verankert sind, einschließlich der Verteidigungsrechte von Personen, gegen die ein Strafverfahren geführt wird; die Verpflichtungen der Strafverfolgungs- oder Justizbehörden ***oder der Diensteanbieter*** in dieser Hinsicht bleiben unberührt.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Europäische Herausgabeanordnung“ eine ▌Entscheidung***, die von*** einer ***Justizbehörde*** eines Mitgliedstaats ***(„Anordnungsstaat“) erlassen oder validiert wird und die an einen*** Diensteanbieter ***gerichtet ist***, der in der Union Dienstleistungen anbietet und in einem anderen Mitgliedstaat***, der an diese Verordnung gebunden ist („Vollstreckungsstaat“),*** niedergelassen oder ***rechtlich*** vertreten ist, ***zur*** Herausgabe ▌elektronischer ***Informationen***;

2. „Europäische Sicherungsanordnung“ eine ▌Entscheidung***, die von*** einer ***Justizbehörde*** eines Mitgliedstaats ***(„Anordnungsstaat“) erlassen oder validiert wird und die an einen*** Diensteanbieter ***gerichtet ist***, der in der Union Dienstleistungen anbietet und in einem anderen Mitgliedstaat***, der an diese Verordnung gebunden ist („Vollstreckungsstaat“),*** niedergelassen oder ***rechtlich*** vertreten ist, ***zur Sicherung elektronischer Informationen*** im Hinblick auf ein späteres Ersuchen um Herausgabe ▌;

3. „Diensteanbieter“ jede natürliche oder juristische Person, die eine oder mehrere der folgenden Kategorien von Dienstleistungen anbietet ***und, soweit personenbezogene Daten betroffen sind, als Verantwortlicher im Sinne der Verordnung (EU) 2016/679 fungiert***:

a) elektronische Kommunikationsdienste im Sinne des Artikels 2 Nummer 4 der [Richtlinie über den europäischen Kodex für die elektronische Kommunikation];

b) Dienste der Informationsgesellschaft im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates[[20]](#footnote-20), bei denen die Speicherung von Daten eine bestimmende Komponente der für den Nutzer erbrachten Dienstleistung ist ▌;

c) Internetdomänennamen- und IP-Adressendienste wie IP-Adressenanbieter, Domänennamen-Register, Domänennamen-Registrierungsstellen und damit verbundene ▐ Proxy-Dienste;

4. „der/die in der Union Dienstleistungen anbietet/anbieten“

a) der/die juristische oder natürliche Personen in einem oder mehreren Mitgliedstaaten in die Lage versetzt/versetzen, die unter Nummer 3 genannten Dienste in Anspruch zu nehmen, und

b) eine wesentliche Verbindung zu dem/den unter Buchstabe a genannten Mitgliedstaat(en) hat/haben; ***eine solche wesentliche Verbindung zur Union gilt dann als gegeben, wenn der Diensteanbieter eine Niederlassung in der Union hat, oder – in Ermangelung einer solchen – aufgrund der Existenz einer erheblichen Zahl von Nutzern in einem oder mehreren Mitgliedstaaten oder der Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten;***

5. ***„Hauptniederlassung“ im Falle eines Diensteanbieters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Datenverarbeitung werden in einer anderen Niederlassung des Diensteanbieters in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, in der derartige Entscheidungen getroffen werden, als Hauptniederlassung;***

6. „elektronische ***Informationen***“ ***Teilnehmerdaten, Verkehrsdaten oder Inhaltsdaten***‚ die zum Zeitpunkt ***des Erlasses*** einer ***Europäischen*** Herausgabe- oder Sicherungsanordnung ***rechtmäßig*** von einem Diensteanbieter ▌gespeichert werden ***und die angefordert werden, um während der Ermittlung, der Strafverfolgung und des Gerichtsverfahrens in Bezug auf eine Straftat in einem Mitgliedstaat im Einklang mit nationalem Recht als Beweismittel zu dienen***;

7. „Teilnehmerdaten“ alle Daten, die ***im normalen Geschäftsverlauf erhoben werden und den angegebenen Namen, Geburtsdatum, Postanschrift oder geografische Anschrift, Abrechnungs- und Zahlungsdaten, Telefonnummer oder E-Mail-Adresse zur Identifizierung des Teilnehmers oder Kunden sowie die Art der erbrachten Dienstleistung und die Dauer des Vertrags mit dem Diensteanbieter*** betreffen ***und die zu dem einzigen Zweck der Identifizierung des Nutzers des Dienstes unbedingt erforderlich sind***;

8. „***Verkehrsdaten***“ ▌Daten, ***die im normalen Geschäftsverkehr erhoben wurden,*** über***:***

***a) die Art der bereitgestellten Dienstleistung und ihre Dauer, sofern dies technische Daten betrifft sowie Daten, mit denen technische Maßnahmen oder Schnittstellen identifiziert werden, die von einem Teilnehmer oder Kunden verwendet oder dem Teilnehmer oder Kunden zur Verfügung gestellt werden, und Daten im Zusammenhang mit der Validierung der Nutzung des Dienstes – mit Ausnahme von Kennwörtern oder anderen Authentifizierungsmitteln, die anstelle eines Kennworts verwendet werden –, die von einem Nutzer bereitgestellt oder auf Anfrage eines Nutzers erstellt werden;***

***b) den Beginn und das Ende der Zugangssitzung eines Nutzers in Bezug auf einen Dienst, wie das Datum und die Uhrzeit der Nutzung oder der Anmeldung bei und Abmeldung von dem Dienst;***

***c) Metadaten der elektronischen Kommunikation, wie sie in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs von Inhalten elektronischer Kommunikation verarbeitet werden, darunter die zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts einer Kommunikation verwendeten Daten, die im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdienste verarbeiteten Daten über den Standort der Endeinrichtung sowie Datum, Uhrzeit, Dauer und Art der Kommunikation;***

9. ▐

10. „Inhaltsdaten“ ***die vom Diensteanbieter*** in einem digitalen Format gespeicherten Daten wie Text, Sprache, Videos, Bilder und Tonaufzeichnungen, mit Ausnahme von Teilnehmer- ▌oder ***Verkehrsdaten***;

11. „Informationssystem“ ein Informationssystem im Sinne des Artikels 2 Buchstabe a der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates[[21]](#footnote-21);

12. „Anordnungsstaat“ den Mitgliedstaat, in dem die Europäische Herausgabeanordnung oder die Europäische Sicherungsanordnung erlassen wird;

***12a. „Anordnungsbehörde“ die Behörde im Anordnungsstaat, die in dem betreffenden Fall für den Erlass der Europäischen Herausgabeanordnung oder Europäischen Sicherungsanordnung zuständig ist;***

13. „Vollstreckungsstaat“ den Mitgliedstaat, in dem der ***Diensteanbieter*** niedergelassen ***oder rechtlich vertreten*** ist und an den die Europäische Herausgabeanordnung und das Zertifikat über eine Europäische Herausgabeanordnung oder die Europäische Sicherungsanordnung und das Zertifikat über eine Europäische Sicherungsanordnung zur ***Mitteilung und*** Vollstreckung ***der Anordnung im Einklang mit dieser Verordnung*** übermittelt werden;

14. „Vollstreckungsbehörde“ die zuständige Behörde im Vollstreckungsstaat, an die die Anordnungsbehörde die Europäische Herausgabeanordnung und das Zertifikat über eine Europäische Herausgabeanordnung oder die Europäische Sicherungsanordnung und das Zertifikat über eine Europäische Sicherungsanordnung zur ***Mitteilung und*** Vollstreckung ***der Anordnung im Einklang mit dieser Verordnung*** übermittelt; ***sofern dies im nationalen Recht vorgesehen ist, kann die Vollstreckungsbehörde eine Gerichtsbehörde des Vollstreckungsstaats sein;***

15. „Notfälle“ Situationen, in denen eine unmittelbare Gefahr für das Leben oder die körperliche Unversehrtheit einer Person ▌besteht.

Artikel 3

Anwendungsbereich

(1) Diese Verordnung gilt ***für Mitgliedstaaten und*** für Diensteanbieter, die Dienstleistungen in ***einem oder mehreren durch diese Verordnung gebundenen Mitgliedstaaten*** anbieten ***und die in einem dieser Mitgliedstaaten niedergelassen oder rechtlich vertreten sind***.

***(1a) Diese Verordnung gilt nicht für Verfahren, die von der Anordnungsbehörde eingeleitet wurden, um einem anderen Mitgliedstaat oder einem Drittstaat Rechtshilfe zu leisten.***

(2) Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen dürfen nur ***im Rahmen und für die Zwecke von*** Strafverfahren während des Ermittlungs- und des Gerichtsverfahrens erlassen werden. Die Anordnungen können auch in Verfahren wegen einer Straftat erlassen werden, für die eine juristische Person im Anordnungsstaat zur Verantwortung gezogen oder bestraft werden kann.

(3) Die in dieser Verordnung vorgesehenen Anordnungen dürfen nur für Daten erlassen werden, die in der Union angebotene Dienstleistungen im Sinne des Artikels 2 Nummer 3 betreffen.

Kapitel 2: Europäische Herausgabeanordnung, Europäische Sicherungsanordnung und Zertifikate

Artikel 4

Anordnungsbehörde:

(1) Eine Europäische Herausgabeanordnung ***im Hinblick auf den Erhalt*** von Teilnehmerdaten ***und IP-Adressen zu dem einzigen Zweck der Bestimmung der Identität von Einzelpersonen mit direktem Bezug zu dem Verfahren nach Artikel 3 Absatz 2*** kann erlassen werden von

 a) einem Richter, einem Gericht, einem Ermittlungsrichter oder einem Staatsanwalt mit Zuständigkeit in dem betreffenden Fall oder

b) jeder anderen vom Anordnungsstaat bezeichneten zuständigen Behörde, die in dem betreffenden Fall in ihrer Eigenschaft als Ermittlungsbehörde in einem Strafverfahren nach nationalem Recht für die Anordnung der Erhebung von Beweismitteln zuständig ist. Eine solche Europäische Herausgabeanordnung wird von einem Richter, einem Gericht, einem Ermittlungsrichter oder einem Staatsanwalt im Anordnungsstaat validiert, nachdem dieser bzw. dieses überprüft hat, ob die Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung nach dieser Verordnung eingehalten sind.

(2) Eine Europäische Herausgabeanordnung zur Herausgabe von ***Verkehrsdaten*** und Inhaltsdaten kann erlassen werden von

 a) einem Richter, einem Gericht oder einem Ermittlungsrichter mit Zuständigkeit in dem betreffenden Fall oder

 b) jeder anderen vom Anordnungsstaat bezeichneten zuständigen Behörde, die in dem betreffenden Fall in ihrer Eigenschaft als Ermittlungsbehörde in einem Strafverfahren nach nationalem Recht für die Anordnung der Erhebung von Beweismitteln zuständig ist. Eine solche Europäische Herausgabeanordnung wird von einem Richter, einem Gericht oder einem Ermittlungsrichter im Anordnungsstaat validiert, nachdem dieser bzw. dieses überprüft hat, ob die Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung nach dieser Verordnung eingehalten sind.

(3) Eine Europäische Sicherungsanordnung ***für alle Datenkategorien*** kann erlassen werden von

a) einem Richter, einem Gericht, einem Ermittlungsrichter oder einem Staatsanwalt mit Zuständigkeit in dem betreffenden Fall oder

b) jeder anderen vom Anordnungsstaat bezeichneten zuständigen Behörde, die in dem betreffenden Fall in ihrer Eigenschaft als Ermittlungsbehörde in einem Strafverfahren nach nationalem Recht für die Anordnung der Erhebung von Beweismitteln zuständig ist. Eine solche Europäische Sicherungsanordnung wird von einem Richter, einem Gericht, einem Ermittlungsrichter oder einem Staatsanwalt im Anordnungsstaat validiert, nachdem dieser bzw. dieses überprüft hat, ob die Voraussetzungen für den Erlass einer Europäischen Sicherungsanordnung nach dieser Verordnung eingehalten sind.

(4) Wenn die Anordnung von einer Justizbehörde gemäß Absatz 1 Buchstabe b, Absatz 2 Buchstabe b und Absatz 3 Buchstabe b validiert wurde, kann diese Behörde auch als Anordnungsbehörde für die Zwecke der Übermittlung des Zertifikats über eine Europäische Herausgabeanordnung und des Zertifikats über eine Europäische Sicherungsanordnung angesehen werden.

Artikel 5

Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung

(1) Eine Anordnungsbehörde darf nur dann eine Europäische Herausgabeanordnung erlassen, wenn die in diesem Artikel genannten Voraussetzungen erfüllt sind.

(2) Die Europäische Herausgabeanordnung muss für die Zwecke eines Verfahrens nach Artikel 3 Absatz 2 notwendig und verhältnismäßig sein***, wobei die Rechte der betroffenen Person zu berücksichtigen sind.*** ***Sie*** darf nur erlassen werden, wenn ***sie unter denselben Bedingungen in einem*** vergleichbaren innerstaatlichen ***Fall hätte erlassen werden können, wenn ausreichend Grund zu der Annahme besteht, dass eine*** Straftat ***begangen wurde, wenn sie schwerwiegend genug ist, um die grenzüberschreitende Herausgabe der Daten zu rechtfertigen, und wenn die angeforderten Informationen für diese Ermittlungen relevant sind***. ***Sie ist auf die Daten bestimmter Personen mit direktem Bezug zu den in Artikel 3 Absatz 2 genannten spezifischen Verfahren beschränkt.***

(3) ***Eine*** Europäische ***Herausgabeanordnung im Hinblick auf den Erhalt von Teilnehmerdaten oder IP-Adressen zu dem einzigen Zweck der Bestimmung der Identität von Einzelpersonen mit direktem Bezug zu dem spezifischen Verfahren nach Artikel 3 Absatz 2 kann*** für alle Straftaten erlassen werden.

(4) ***Eine*** Europäische ***Herausgabeanordnung*** zur Herausgabe von ***Verkehrs-*** oder Inhaltsdaten ***kann*** nur ***bei Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden,*** erlassen werden.

***(4a)*** ***Europäische Herausgabeanordnungen zur Herausgabe von Verkehrs- oder Inhaltsdaten können außerdem für folgende Straftaten erlassen werden:***

***a) für die folgenden Straftaten, wenn diese ganz oder teilweise mittels eines Informationssystems begangen werden:***

***– Straftaten im Sinne der Artikel 3, 4 und 5 des Rahmenbeschlusses 2001/413/JI des Rates;***

***– Straftaten im Sinne der Artikel 3 bis 8 der Richtlinie 2013/40/EU;***

***b) für Straftaten im Sinne der Artikel 3 bis 12 und 14 der Richtlinie (EU) 2017/541;***

***ba) für Straftaten im Sinne der Artikel 3 bis 7 der Richtlinie 2011/93/EU.***

(5) Die Europäische Herausgabeanordnung enthält folgende Angaben:

a) die Anordnungsbehörde und gegebenenfalls die validierende Behörde; ***für Verkehrs- und Inhaltsdaten und wenn der Anordnungsstaat einem Verfahren nach Artikel 7 Absatz 1 oder 2 des Vertrags über die Europäische Union unterliegt, Informationen über das besondere Verfahren nach Artikel 9 Absatz 2a dieser Verordnung;***

b) ***die*** Adressaten der Europäischen Herausgabeanordnung gemäß Artikel 7;

c) ***die persönlich identifizierbaren Personen oder, wenn*** der einzige Zweck der Anordnung ▌darin ***besteht***, eine Person zu identifizieren, ***jede andere eindeutige Kennung wie Benutzername oder Login-ID***;

d) die Kategorie der angeforderten Daten (Teilnehmerdaten, ***Verkehrsdaten*** oder Inhaltsdaten);

e) ▌die Zeitspanne, für die die Herausgabe angefordert wird***, möglichst eng eingegrenzt***;

f) die anwendbaren Bestimmungen des Strafrechts des Anordnungsstaats;

g) in Notfällen die ***ordnungsgemäße Begründung*** hierfür;

h) ▐

i) die Gründe für die Notwendigkeit und Verhältnismäßigkeit der Maßnahme ***unter gebührender Berücksichtigung der Auswirkungen der Maßnahme auf die Grundrechte der spezifischen Personen, deren Daten angefordert werden, und der Schwere der Straftat.***

(6) ▐

(7) Wenn die Anordnungsbehörde Grund zu der Annahme hat, dass angeforderte ***Daten*** durch Immunitäten und Vorrechte geschützt sind, die nach dem Recht des Mitgliedstaats, in dem die Anordnung an den Diensteanbieter gerichtet wird, ***oder dem Recht des Mitgliedstaats, in dem die Person, deren Daten angefordert werden, ansässig ist oder durch das Berufsgeheimnis oder das Anwaltsgeheimnis gebunden ist,***  gewährt werden, oder dass die Offenlegung der betreffenden Daten sich auf die grundlegenden Interessen dieses Mitgliedstaats wie die nationale Sicherheit oder Verteidigung auswirken könnte, muss die Anordnungsbehörde vor Erlass der Europäischen Herausgabeanordnung den Sachverhalt klären, unter anderem indem sie die zuständigen Behörden des betreffenden Mitgliedstaats entweder direkt oder über Eurojust oder das Europäische Justizielle Netz ***für Strafsachen*** konsultiert. Stellt die Anordnungsbehörde fest, dass die angeforderten ***Daten*** durch solche Immunitäten und Vorrechte geschützt sind oder dass ihre Offenlegung Auswirkungen auf die grundlegenden Interessen des anderen Mitgliedstaats hätte, so erlässt sie die Europäische Herausgabeanordnung nicht.

Artikel 6

Voraussetzungen für den Erlass einer Europäischen Sicherungsanordnung

(1) Eine Anordnungsbehörde darf nur dann eine Europäische Sicherungsanordnung erlassen, wenn die in diesem Artikel genannten Voraussetzungen erfüllt sind.

(2) Eine Europäische Sicherungsanordnung kann erlassen werden, wenn dies notwendig und verhältnismäßig ist, um die Entfernung, Löschung oder Änderung von Daten im Hinblick auf ein späteres Ersuchen um Herausgabe dieser Daten im Wege der Rechtshilfe, einer Europäischen Ermittlungsanordnung oder einer Europäischen Herausgabeanordnung zu verhindern***, wobei die Rechte der betroffenen Person zu berücksichtigen sind***. Europäische Sicherungsanordnungen zur Sicherung von Daten können für alle Straftaten erlassen werden***, wenn sie unter denselben Bedingungen in einem vergleichbaren innerstaatlichen Fall im Anordnungsstaat hätten erlassen werden können, wenn ausreichend Grund zu der Annahme besteht, dass eine Straftat begangen wurde, wenn sie schwerwiegend genug ist, um die grenzüberschreitende Sicherung der Daten zu rechtfertigen, und wenn die angeforderten Informationen für diese Ermittlungen relevant sind***. ***Sie sind auf die Daten bestimmter Personen mit direktem Bezug zu den in Artikel 3 Absatz 2 genannten spezifischen Verfahren beschränkt.***

(3) Die Europäische Sicherungsanordnung enthält folgende Angaben:

a) die Anordnungsbehörde und gegebenenfalls die validierende Behörde;

b) ***die*** Adressaten der Europäischen Sicherungsanordnung gemäß Artikel 7;

c) die ***persönlich identifizierbaren*** Personen, deren Daten gesichert werden sollen, ***oder, wenn*** der einzige Zweck der Anordnung ▌darin ***besteht***, eine Person zu identifizieren***, jede andere eindeutige Kennung wie Benutzername oder Login-ID***;

d) die Kategorie der zu sichernden Daten (Teilnehmerdaten, ***Verkehrsdaten*** oder Inhaltsdaten);

e) ▌die Zeitspanne, für die die Sicherung angefordert wird***, möglichst eng eingegrenzt***;

f) die anwendbaren Bestimmungen des Strafrechts des Anordnungsstaats;

g) die Gründe für die Notwendigkeit und Verhältnismäßigkeit der Maßnahme ***unter gebührender Berücksichtigung der Auswirkungen der Maßnahme auf die Grundrechte der spezifischen Personen, deren Daten angefordert werden, und der Schwere der Straftat***.

***(3a) Wenn die Anordnungsbehörde Grund zu der Annahme hat, dass angeforderte Daten durch Immunitäten und Vorrechte geschützt sind, die nach dem Recht des Mitgliedstaats, in dem die Anordnung an den Diensteanbieter gerichtet wird, gewährt werden, oder dass die Sicherung der betreffenden Daten sich auf die grundlegenden Interessen dieses Mitgliedstaats wie die nationale Sicherheit oder Verteidigung auswirken könnte, muss die Anordnungsbehörde vor Erlass der Europäischen Sicherungsanordnung den Sachverhalt klären, unter anderem indem sie die zuständigen Behörden des betreffenden Mitgliedstaats entweder direkt oder über Eurojust oder das Europäische Justizielle Netz in Strafsachen konsultiert. Stellt die Anordnungsbehörde fest, dass die angeforderten Daten durch solche Immunitäten und Vorrechte geschützt sind oder dass ihre Sicherung Auswirkungen auf die grundlegenden Interessen des anderen Mitgliedstaats hätte, erlässt sie die Europäische Sicherungsanordnung nicht.***

***Artikel 6a***

***Gesetzlicher Vertreter***

***(1) Diensteanbieter, die in den durch diese Verordnung gebundenen Mitgliedstaaten Dienstleistungen anbieten, aber nicht in der Union niedergelassen sind, benennen einen gesetzlichen Vertreter für die Entgegennahme, Befolgung und Vollstreckung von Europäischen Herausgabeanordnungen und Europäischen Sicherungsanordnungen, die die zuständigen Behörden der Mitgliedstaaten zum Zwecke der Erhebung elektronischer Informationen in Strafverfahren erlassen. Der gesetzliche Vertreter muss in einem der (durch diese Verordnung gebundenen) Mitgliedstaaten, in denen der Diensteanbieter seine Dienstleistungen anbietet, niedergelassen sein.***

***(2) Diensteanbieter, die in den durch diese Verordnung gebundenen Mitgliedstaaten Dienstleistungen anbieten, aber in einem nicht durch diese Verordnung gebundenen Mitgliedstaat niedergelassen sind, benennen einen gesetzlichen Vertreter für die Entgegennahme, Befolgung und Vollstreckung von Europäischen Herausgabeanordnungen und Europäischen Sicherungsanordnungen, die die zuständigen Behörden der Mitgliedstaaten zum Zwecke der Erhebung elektronischer Informationen in Strafverfahren erlassen. Der gesetzliche Vertreter muss in einem der durch diese Verordnung gebundenen Mitgliedstaaten, in denen der Diensteanbieter seine Dienstleistungen anbietet, niedergelassen sein.***

***(3) Diensteanbieter, die einer Gruppe angehören, dürfen gemeinsam einen gesetzlichen Vertreter benennen.***

***(4) Der gesetzliche Vertreter wird mit der Entgegennahme, Befolgung und Vollstreckung dieser Beschlüsse und Anordnungen im Namen des betreffenden Diensteanbieters beauftragt.***

***(5) Nach der Benennung des gesetzlichen Vertreters teilen Diensteanbieter dies dem Mitgliedstaat, in dem ihr gesetzlicher Vertreter niedergelassen ist, schriftlich mit. Die Mitteilung umfasst die Benennung und die Kontaktangaben des gesetzlichen Vertreters sowie etwaige diesbezügliche Änderungen.***

***(6) In der Mitteilung ist anzugeben, welche Amtssprache(n) der Union im Sinne der Verordnung Nr. 1/58 im Verkehr mit dem gesetzlichen Vertreter verwendet werden kann/können. Anzugeben ist mindestens eine der Sprachen, die von dem Mitgliedstaat, in dem der gesetzliche Vertreter niedergelassen ist, akzeptiert werden.***

***(7) Die den Mitgliedstaaten gemäß diesem Artikel übermittelten Informationen werden auf einer eigens dafür eingerichteten Internetseite des Europäischen Justiziellen Netzes für Strafsachen zugänglich gemacht. Diese Informationen werden regelmäßig aktualisiert.***

***(8) Die Mitgliedstaaten stellen sicher, dass der benannte gesetzliche Vertreter, der die betreffenden Beschlüsse und Anordnungen entgegennimmt, haftbar gemacht werden kann, wenn er den Pflichten gemäß dieser Verordnung nicht nachkommt; die Haftung des Diensteanbieters und die rechtlichen Schritte, die gegen diesen eingeleitet werden können, bleiben hiervon unberührt.***

***(9) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diesen Artikel zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.***

Artikel 7

Adressaten einer Europäischen Herausgabeanordnung und einer Europäischen Sicherungsanordnung

(1) ***Zum Zweck der Erhebung elektronischer Informationen in Strafverfahren werden*** die Europäische Herausgabeanordnung und die Europäische Sicherungsanordnung ▌direkt ***und gleichzeitig*** gerichtet ***an***

***a) die Hauptniederlassung des Diensteanbieters oder gegebenenfalls den gesetzlichen Vertreter im Vollstreckungsstaat***, den der Diensteanbieter zum Zweck der Beweismittelerhebung in Strafverfahren benannt hat; ***und***

***b) die Vollstreckungsbehörde.***

***(1a) Die Mitgliedstaaten stellen sicher, dass ein in ihrem Hoheitsgebiet niedergelassener Diensteanbieter diesem Mitgliedstaat schriftlich mitteilt, wo sich seine Hauptniederlassung befindet. Die Mitteilung umfasst die Kontaktangaben sowie etwaige diesbezügliche Änderungen.***

***(1b) Die den Mitgliedstaaten gemäß Absatz 1a übermittelten Informationen werden auf einer eigens dafür eingerichteten Internetseite des Europäischen Justiziellen Netzes für Strafsachen zugänglich gemacht. Diese Informationen werden regelmäßig aktualisiert.***

(2) ▐

(3) ▐

(4) ▐

***Artikel 7a***

***Gemeinsames europäisches Austauschsystem***

***(1) Bis zum ... [Datum der Anwendung dieser Verordnung] richtet die Kommission ein gemeinsames europäisches Austauschsystem mit gesicherten Kanälen für die Abwicklung autorisierter grenzüberschreitender Kommunikation, die Authentifizierung und die Übermittlung der Anordnungen und der angeforderten Daten zwischen den zuständigen Behörden und Diensteanbietern ein. Die zuständigen Behörden und Diensteanbieter nutzen dieses System für die Zwecke dieser Verordnung.***

***(2) Die Kommission stellt sicher, dass das System einen wirksamen, zuverlässigen und reibungslosen Austausch der einschlägigen Informationen sowie ein hohes Maß an Sicherheit, Vertraulichkeit und Integrität sowie den notwendigen Schutz der Privatsphäre und der personenbezogenen Daten gemäß der Verordnung (EU) 2018/1725, der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und der Richtlinie 2002/58/EG gewährleistet. Zu diesem Zweck werden offene und gängige elektronische Signaturen und Verschlüsselungstechnologien angewandt, die dem neuesten Stand der Technik entsprechen.***

***(3) Wenn Diensteanbieter oder Mitgliedstaaten bereits spezielle Systeme oder andere sichere Kanäle für die Bearbeitung von Datenersuchen für Strafverfolgungszwecke eingerichtet haben, muss es möglich sein, diese Systeme oder Kanäle mit dem gemeinsamen europäischen Austauschsystem zu verbinden.***

*Artikel 8*

*Zertifikate über eine Europäische Herausgabe- oder Sicherungsanordnung*

(1) Eine Europäische Herausgabe- oder Sicherungsanordnung wird ***den*** Adressaten nach Artikel 7 ***über das in Artikel 7a genannte System*** in Form eines Zertifikats über eine Europäische Herausgabeanordnung (EPOC) beziehungsweise eines Zertifikats über eine Europäische Sicherungsanordnung (EPOC-PR) übermittelt.

Die Anordnungsbehörde oder die validierende Behörde füllt das EPOC gemäß Anhang I oder das EPOC-PR gemäß Anhang II aus, unterzeichnet es und bestätigt seine inhaltliche Richtigkeit.

(2) Die Übermittlung des EPOC oder des EPOC-PR erfolgt direkt ***über das in Artikel 7a genannte System, wobei die Adressaten*** einen schriftlichen Nachweis ***erbringen können, der den*** Adressaten die Feststellung ***der Anordnungsbehörde und*** der Echtheit ***der Anordnung gestattet***.

(3) Das EPOC enthält ***alle*** in Artikel 5 Absatz 5 Buchstaben a bis ***i*** aufgeführten Angaben, einschließlich ausreichender Informationen, um ***den*** Adressaten die Feststellung der Anordnungsbehörde und die Kontaktaufnahme mit dieser zu ermöglichen***, sowie Informationen über die Mittel und technischen Schnittstellen, die ihr zur Verfügung stehen, um die herausgegebenen Daten zu erhalten, oder Informationen darüber, wo diese Informationen zu finden sind***.

(4) Das EPOC-PR enthält ***alle*** in Artikel 6 Absatz 3 Buchstaben a bis ***g*** aufgeführten Angaben, einschließlich ausreichender Informationen, um ***den*** Adressaten die Feststellung der Anordnungsbehörde und die Kontaktaufnahme mit dieser zu ermöglichen. ▌

(5) Im Bedarfsfall sind das EPOC oder das EPOC-PR in eine ***der Amtssprachen des Vollstreckungsstaats oder in eine andere vom Vollstreckungsstaat gemäß Absatz 5a ausdrücklich*** akzeptierte ***Sprache*** zu übersetzen.

***Artikel 8a***

***Ausführung eines EPOC für Teilnehmerdaten und IP-Adressen***

***Zu dem einzigen Zweck der Identifizierung einer Person***

***(1) Ein EPOC für Teilnehmerdaten und IP-Adressen zu dem einzigen Zweck der Identifizierung einer Person ist direkt und gleichzeitig zu richten an:***

***a) die Hauptniederlassung des Diensteanbieters oder gegebenenfalls den Sitz des gesetzlichen Vertreters; und***

***b) die Vollstreckungsbehörde.***

***Die gleichzeitige Unterrichtung der Vollstreckungsbehörde hat keine aufschiebende Wirkung bezüglich der Pflichten des Diensteanbieters gemäß Absatz 1.***

***(2) Nach Erhalt des EPOC für Teilnehmerdaten und IP-Adressen zu dem einzigen Zweck der Identifizierung einer Person stellt der Diensteanbieter sicher, dass die angeforderten Daten so bald wie möglich, spätestens jedoch innerhalb von zehn Tagen nach Erhalt des EPOC, direkt an die Anordnungsbehörde oder die im EPOC angegebenen Strafverfolgungsbehörden übermittelt werden. Bei der Übermittlung der angeforderten Daten übermittelt der Diensteanbieter der Vollstreckungsbehörde gleichzeitig zur Information eine Kopie der übermittelten Daten.***

***(3) In Notfällen übermittelt der Diensteanbieter die angeforderten Daten unverzüglich, spätestens jedoch innerhalb von 16 Stunden nach Erhalt des EPOC. Bei der Übermittlung der angeforderten Daten stellt der Diensteanbieter die Daten gleichzeitig der Vollstreckungsbehörde zur Information zur Verfügung.***

***(4) Entscheidet die Vollstreckungsbehörde, einen der in Artikel 10a Absatz 1 aufgeführten Gründe geltend zu machen, handelt sie so bald wie möglich, spätestens jedoch innerhalb der in Absatz 1 oder 2 genannten Fristen, und setzt die Anordnungsbehörde und den Diensteanbieter unverzüglich von ihrer Entscheidung in Kenntnis. Die Anordnungsbehörde löscht die Daten. Wurden die angeforderten Daten der Anordnungsbehörde noch nicht übermittelt, übermittelt der Diensteanbieter, an den die Anordnung gerichtet ist, die Daten nicht.***

***(5) Wenn das EPOC unvollständig ist, offensichtliche formale oder inhaltliche Fehler enthält oder keine ausreichenden Informationen zur Ausführung des EPOC enthält, setzt der Diensteanbieters die im EPOC angegebene Anordnungsbehörde sowie Vollstreckungsbehörde unverzüglich hiervon in Kenntnis und ersucht unter Verwendung des Formulars in Anhang III um Klarstellung oder, sofern erforderlich, Berichtigung durch die Anordnungsbehörde. Die Anordnungsbehörde reagiert umgehend, spätestens jedoch innerhalb von fünf Tagen. Die in den Absätzen 1 und 2 genannten Fristen gelten erst, wenn die Klarstellung erfolgt ist. Reagiert die Anordnungsbehörde nicht, wird die Anordnung als null und nichtig betrachtet.***

***(6) Wenn der Diensteanbieter seinen Verpflichtungen aufgrund höherer Gewalt oder einer faktischen Unmöglichkeit infolge von Umständen, die nicht dem Diensteanbieter angelastet werden können, unter anderem weil die Person, deren Daten angefordert werden, kein Kunde des Diensteanbieters ist oder weil die Daten vor Erhalt des EPOC gelöscht wurden, nicht nachkommen kann, setzt der Diensteanbieter die im EPOC angegebene Anordnungsbehörde sowie Vollstreckungsbehörde unverzüglich hiervon in Kenntnis und legt unter Verwendung des Formulars in Anhang III die Gründe hierfür dar. Wenn die entsprechenden Voraussetzungen erfüllt sind, zieht die Anordnungsbehörde das EPOC zurück und setzt die Adressaten von ihrer Entscheidung in Kenntnis.***

***(7) In allen Fällen, in denen der Diensteanbieter die angeforderten Informationen aus anderen Gründen, auch aus technischen oder betrieblichen Gründen, überhaupt nicht, nicht vollständig oder nicht fristgerecht bereitstellt, informiert er die im EPOC angegebene Anordnungsbehörde sowie Vollstreckungsbehörde unverzüglich, spätestens jedoch innerhalb der in den Absätzen 1 und 2 genannten Fristen unter Verwendung des Formulars in Anhang III über die Gründe hierfür. Die Anordnungsbehörde überprüft die Anordnung im Lichte der vom Diensteanbieter übermittelten Informationen und legt gegebenenfalls eine neue Frist für die Adressaten fest. Ist der Diensteanbieter der Ansicht, dass das EPOC nicht ausgeführt werden kann, weil ausschließlich aus den in dem EPOC enthaltenen Informationen hervorgeht, dass es offensichtlich missbräuchlich ist oder über den Zweck der Anordnung hinausgeht, übermittelt er das Formular in Anhang III auch der im EPOC angegebenen Anordnungsbehörde und Vollstreckungsbehörde, wodurch eine aufschiebende Wirkung bezüglich der Übermittlung der angeforderten Daten eintritt. In diesen Fällen kann die Vollstreckungsbehörde die Anordnungsbehörde entweder direkt oder über Eurojust oder das Europäische Justizielle Netz für Strafsachen um Klarstellungen zu der Europäischen Herausgabeanordnung ersuchen. Die Anordnungsbehörde reagiert umgehend, spätestens jedoch innerhalb von fünf Tagen. Die in den Absätzen 1 und 2 genannten Fristen gelten erst, wenn die Klarstellung erfolgt ist. Reagiert die Anordnungsbehörde nicht, wird die Anordnung als null und nichtig betrachtet.***

***(8) Wenn der Diensteanbieter die angeforderten Daten nicht umgehend gemäß den Absätzen 3, 4 und 5 bereitstellt, muss er die angeforderten Daten, soweit möglich, sichern. Die Daten werden so lange gesichert, bis sie herausgegeben werden oder das EPOC zurückgezogen wird oder als null und nichtig zu betrachten ist.***

Artikel 9

Ausführung eines EPOC ***für Verkehrs- oder Inhaltsdaten***

***(-1a) Ein EPOC für Verkehrs- oder Inhaltsdaten wird direkt und gleichzeitig gerichtet an***

***a) die Hauptniederlassung des Diensteanbieters oder gegebenenfalls den Sitz des gesetzlichen Vertreters; und***

***b) die Vollstreckungsbehörde.***

(1) Nach Erhalt des EPOC ***für Verkehrs- oder Inhaltsdaten wird der Diensteanbieter umgehend tätig, um die Daten zu sichern.***

***(1a) Entscheidet die Vollstreckungsbehörde aus einem der in Artikel 10a genannten Gründe, die Ausführung des EPOC zu versagen, so handelt sie so bald wie möglich,*** spätestens ***jedoch*** innerhalb von zehn Tagen nach Erhalt des EPOC***, und unterrichtet die Anordnungsbehörde und den Diensteanbieter umgehend über diese Entscheidung.*** (2) ***Entscheidet die Vollstreckungsbehörde*** in Notfällen***, die Anerkennung oder Vollstreckung des EPOC aus einem der in Artikel 10a genannten Gründe zu versagen, handelt sie so bald wie möglich,*** spätestens jedoch innerhalb von ***16*** Stunden nach Erhalt des EPOC***, und setzt die Anordnungsbehörde und den Diensteanbieter umgehend von dieser Entscheidung in Kenntnis***.

***(2a) Unterliegt der Anordnungsstaat einem Verfahren nach Artikel 7 Absatz 1 oder Artikel 7 Absatz 2 des Vertrags über die Europäische Union, übermittelt der Diensteanbieter die angeforderten Daten erst nach ausdrücklicher schriftlicher Zustimmung der Vollstreckungsbehörde. Zu diesem Zweck bewertet die Vollstreckungsbehörde die Anordnung der Anordnungsbehörde mit der gebotenen Sorgfalt und prüft insbesondere die Gründe für die Versagung der Anerkennung oder der Ausführung gemäß Artikel 10a, bevor sie innerhalb der in den Absätzen 1a und 2 genannten Fristen ihre schriftliche Zustimmung erteilt.***

***(2b) Hat die Vollstreckungsbehörde innerhalb der Frist von zehn Tagen nicht einen der in Artikel 10a genannten Gründe geltend gemacht, sorgt der Diensteanbieter, an den die Anordnung gerichtet ist, unbeschadet von Absatz 2a innerhalb der in den Absätzen 1a und 2 genannten Fristen dafür, dass die angeforderten Daten umgehend direkt an die Anordnungsbehörde oder die Strafverfolgungsbehörden gemäß den Angaben im EPOC übermittelt werden.***

***(2c) Ist es der Vollstreckungsbehörde in einem bestimmten Fall nicht möglich, die Frist nach Absatz 1 oder 2 einzuhalten, unterrichtet sie die Anordnungsbehörde und den Diensteanbieter unverzüglich auf beliebige Weise und gibt dabei die Gründe für die Verzögerung und die voraussichtliche Zeit, die für die Entscheidung benötigt wird, an.***

(3) Wenn ▌das EPOC unvollständig ist, offensichtliche ***formale oder inhaltliche*** Fehler enthält oder keine ausreichenden Informationen zur Ausführung des EPOC enthält, setzt der ***Diensteanbieter*** die im EPOC angegebene Anordnungsbehörde ***und Vollstreckungsbehörde*** unverzüglich hiervon in Kenntnis und bittet unter Verwendung des Formulars in Anhang III um Klarstellung ***oder, sofern erforderlich, Berichtigung durch die Anordnungsbehörde***. Die Anordnungsbehörde reagiert umgehend, spätestens jedoch innerhalb von fünf Tagen. Die in den Absätzen ***1a*** und 2 genannten Fristen gelten erst, wenn die Klarstellung erfolgt ist. ***Reagiert die Anordnungsbehörde nicht, wird die Anordnung als null und nichtig betrachtet.***

(4) Wenn der ***Diensteanbieter seinen Verpflichtungen*** aufgrund höherer Gewalt oder einer faktischen Unmöglichkeit ***infolge von Umständen***, die nicht ▌dem Diensteanbieter angelastet werden ***können***, nicht nachkommen kann, unter anderem weil die Person, deren Daten angefordert werden, kein Kunde ▌des Diensteanbieters ist oder weil die Daten vor Erhalt des EPOC gelöscht wurden, setzt der ***Diensteanbieter*** die im EPOC angegebene Anordnungsbehörde ***und Vollstreckungsbehörde*** unverzüglich hiervon in Kenntnis und legt unter Verwendung des Formulars in Anhang III die Gründe hierfür dar. Wenn die entsprechenden Voraussetzungen erfüllt sind, zieht die Anordnungsbehörde das EPOC zurück ***und setzt die Adressaten von ihrer Entscheidung in Kenntnis***.

(5) In allen Fällen, in denen der ***Diensteanbieter*** die angeforderten Informationen aus anderen Gründen***, auch aus technischen oder betrieblichen Gründen,*** überhaupt nicht, nicht vollständig oder nicht fristgerecht bereitstellt, informiert er die ***im EPOC angegebene*** Anordnungsbehörde ***und Vollstreckungsbehörde*** unverzüglich, spätestens jedoch innerhalb der in den Absätzen ***1a*** und 2 genannten Fristen unter Verwendung des Formulars in Anhang III über die Gründe hierfür. Die Anordnungsbehörde überprüft die Anordnung im Lichte der vom Diensteanbieter übermittelten Informationen und setzt gegebenenfalls eine neue Frist für ***die Adressaten*** fest.

Ist der ***Diensteanbieter*** der Ansicht, dass das EPOC nicht ausgeführt werden kann, weil ausschließlich aus den in dem EPOC enthaltenen Informationen hervorgeht, dass es ▌offensichtlich missbräuchlich ist ***oder über den Zweck der Anordnung hinausgeht***, so übermittelt er das Formular in Anhang III auch der ***im EPOC angegebenen Anordnungsbehörde und*** Vollstreckungsbehörde***, wodurch eine aufschiebende Wirkung bezüglich der Übermittlung der angeforderten Daten eintritt***. In diesen Fällen kann die zuständige Vollstreckungsbehörde die Anordnungsbehörde entweder direkt oder über Eurojust oder das Europäische Justizielle Netz ***in Strafsachen*** um Klarstellungen zu der Europäischen Herausgabeanordnung ersuchen. ***Die Anordnungsbehörde reagiert umgehend, spätestens jedoch innerhalb von fünf Tagen. Die in den Absätzen 1a und 2 genannten Fristen gelten erst, wenn die Klarstellung erfolgt ist. Reagiert die Anordnungsbehörde nicht, wird die Anordnung als null und nichtig betrachtet.***

(6) ***Während des Verfahrens gemäß den Absätzen 1, 1a, 2, 2b, 2c, 3, 4 und 5*** sichert ***der Diensteanbieter*** die angeforderten Daten, ***soweit möglich***. Die Daten werden so lange gesichert, bis sie herausgegeben werden ***oder das EPOC zurückgezogen wird oder als null und nichtig zu betrachten ist***.

Artikel 10

Ausführung eines EPOC-PR

***(-1a) Ein EPOC-PR wird direkt und gleichzeitig gerichtet an***

***a) die Hauptniederlassung des Diensteanbieters oder gegebenenfalls den Sitz des gesetzlichen Vertreters; und***

***b) die Vollstreckungsbehörde.***

***Die gleichzeitige Unterrichtung der Vollstreckungsbehörde hat keine aufschiebende Wirkung bezüglich der Pflichten des Diensteanbieters gemäß Absatz 1.***

(1) Nach Erhalt des EPOC-PR ***wird der Diensteanbieter umgehend tätig, um*** die angeforderten Daten ***zu sichern***. Die Sicherung endet nach 60 Tagen, es sei denn, die Anordnungsbehörde bestätigt, dass das entsprechende Ersuchen um Herausgabe in die Wege geleitet wurde. ***Das EPOC-PR kann nur dann um weitere 30 Tage verlängert werden, wenn dies für eine weitere Bewertung der Relevanz der Daten erforderlich ist.***

(2) Wenn die Anordnungsbehörde innerhalb der in Absatz 1 genannten Frist ***die*** entsprechende ***Europäische Herausgabeanordnung erlässt***, sichert der ***Diensteanbieter*** die Daten so lange, wie dies ***für die Vollstreckung dieser Europäischen Herausgabeanordnung gemäß Artikel 8a oder 9*** erforderlich ist ▌.

(3) Wenn die Sicherung nicht mehr erforderlich ist, setzt die Anordnungsbehörde ***die*** Adressaten unverzüglich hiervon in Kenntnis***, und die Sicherung wird umgehend eingestellt***.

(4) Wenn ▌das ***EPOC-PR*** unvollständig ist, offensichtliche ***formale oder inhaltliche*** Fehler enthält oder keine ausreichenden Informationen zur Ausführung des EPOC-PR enthält, setzt ***der Diensteanbieter*** die im EPOC-PR angegebene Anordnungsbehörde ***und Vollstreckungsbehörde*** unverzüglich hiervon in Kenntnis und bittet unter Verwendung des Formulars in Anhang III um Klarstellung ***oder, sofern erforderlich, Berichtigung durch die Anordnungsbehörde***. Die Anordnungsbehörde reagiert umgehend, spätestens jedoch innerhalb von fünf Tagen. ***Die Adressaten stellen*** sicher, dass die erforderliche Klarstellung ▌entgegengenommen werden kann, damit ***der Diensteanbieter seinen*** Verpflichtungen gemäß ***den Absätzen*** 1***, 2 und 3*** nachkommen ***kann***. ***Reagiert die Anordnungsbehörde nicht, wird die Anordnung als null und nichtig betrachtet.***

(5) Wenn der ***Diensteanbieter*** seiner Verpflichtung aufgrund höherer Gewalt oder einer faktischen Unmöglichkeit ***infolge von Umständen***, die nicht ▌dem Diensteanbieter angelastet werden ***können***, nicht nachkommen kann, unter anderem weil die Person, deren Daten angefordert werden, kein Kunde ▌des Diensteanbieters ist oder weil die Daten vor Erhalt ***des EPOC-PR*** gelöscht wurden, setzt der ***Diensteanbieter*** die im EPOC-PR angegebene Anordnungsbehörde ***und Vollstreckungsbehörde*** unverzüglich hiervon in Kenntnis und legt unter Verwendung des Formulars in Anhang III die Gründe hierfür dar. Wenn ***die entsprechenden*** Voraussetzungen erfüllt sind, zieht die Anordnungsbehörde das EPOC-PR zurück ***und setzt die Adressaten von ihrer Entscheidung in Kenntnis***.

(6) In allen Fällen, in denen der ***Diensteanbieter*** die angeforderten Informationen aus anderen im Formular in Anhang III aufgeführten Gründen***, auch aus technischen oder betrieblichen Gründen,*** nicht sichert, setzt er die ***im EPOC-PR genannte*** Anordnungsbehörde ***und Vollstreckungsbehörde*** unverzüglich unter Verwendung des Formulars in Anhang III über die Gründe hierfür in Kenntnis. Die Anordnungsbehörde überprüft die Anordnung im Lichte der vom Diensteanbieter übermittelten Begründung.

***Ist der Diensteanbieter der Ansicht, dass das EPOC-PR nicht ausgeführt werden kann, weil ausschließlich aus den in dem EPOC-PR enthaltenen Informationen hervorgeht, dass es offensichtlich missbräuchlich ist oder über den Zweck der Anordnung hinausgeht, übermittelt er das Formular in Anhang III auch der im EPOC-PR genannten Anordnungsbehörde und Vollstreckungsbehörde. In diesen Fällen kann die zuständige Vollstreckungsbehörde die Anordnungsbehörde entweder direkt oder über Eurojust oder das Europäische Justizielle Netz in Strafsachen um Klarstellungen zu der Europäischen Sicherungsanordnung ersuchen. Die Anordnungsbehörde reagiert umgehend, spätestens jedoch innerhalb von fünf Tagen. Die in Absatz 1 genannte Frist gilt erst, wenn die Klarstellung erfolgt ist. Reagiert die Anordnungsbehörde nicht, wird die Anordnung als null und nichtig betrachtet.***

***Artikel 10a***

***Gründe für die Versagung der Anerkennung oder der Ausführung***

***(1) Unbeschadet des Artikels 1 Absatz 2 wird das EPOC, wenn es durch die Vollstreckungsbehörde bewertet wird, abgelehnt, wenn***

***a) die Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung gemäß Artikel 5 der vorliegenden Verordnung nicht erfüllt sind;***

***b) die Vollstreckung der Europäischen Herausgabeanordnung dem Grundsatz „ne bis in idem“ zuwiderläuft;***

***c) berechtigter Grund zu der Annahme besteht, dass die Ausführung der Europäischen Herausgabeanordnung mit den Verpflichtungen des Mitgliedstaats gemäß Artikel 6 EUV und der Charta unvereinbar wäre; oder***

***d) nach dem Recht des Vollstreckungsstaats Immunitäten, Vorrechte oder Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit im Zusammenhang mit der Pressefreiheit und der Freiheit der Meinungsäußerung in anderen Medien bestehen, die es unmöglich machen, die Europäische Herausgabeanordnung zu vollstrecken.***

***(2) Abgesehen von Absatz 1 kann die Vollstreckungsbehörde ein EPOC für Verkehrs- oder Inhaltsdaten ablehnen, wenn***

***a) die Vollstreckung der Europäischen Herausgabeanordnung wesentlichen nationalen Sicherheitsinteressen schaden, die Informationsquelle gefährden oder die Verwendung von Verschlusssachen über spezifische nachrichtendienstliche Tätigkeiten voraussetzen würde;***

***b) die Europäische Herausgabeanordnung sich auf eine Straftat bezieht, die mutmaßlich außerhalb des Hoheitsgebiets des Anordnungsstaats und ganz oder teilweise im Hoheitsgebiet des Vollstreckungsstaats begangen wurde, und die Handlung, aufgrund derer das EPOC ergangen ist, nach dem Recht des Vollstreckungsstaats keine Straftat darstellt; die Handlung, aufgrund derer das EPOC erlassen wurde, nach dem Recht des Vollstreckungsstaats keine Straftat darstellt, es sei denn, sie betrifft eine Straftat, die unter den in Anhang IIIa aufgeführten Kategorien von Straftaten genannt wird – wie von der Anordnungsbehörde im EPOC angegeben –, und sofern die Straftat im Anordnungsstaat mit einer Freiheitsstrafe oder freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist;***

***d) die Vollstreckung der Europäischen Herausgabeanordnung nach dem Recht des Vollstreckungsstaats auf eine Liste oder Kategorie von Straftaten oder auf Straftaten, die mit einem höherem Mindeststrafmaß bedroht sind, beschränkt ist; oder***

***e) die Befolgung einer Europäischen Herausgabeanordnung im Widerspruch zu den geltenden Rechtsvorschriften eines Drittstaats stehen würde, die die Offenlegung der betreffenden Daten verbieten.***

***(3) Absatz 2 Buchstabe e ist gemäß dem Verfahren nach Artikel 14a anzuwenden.***

***(4) Betrifft die Europäische Herausgabeanordnung eine Straftat in Verbindung mit Steuern oder Abgaben, Zöllen und Devisen, kann die Vollstreckungsbehörde die Anerkennung oder Ausführung nicht aus dem Grund verweigern, dass das Recht des Vollstreckungsstaats keine gleichartigen Steuern oder Abgaben vorschreibt oder keine gleichartige Steuer- oder Abgabe-, Zoll- und Devisenregelung enthält wie das Recht des Anordnungsstaats.***

***(5) Bevor die Vollstreckungsbehörde in den Fällen nach den Absätzen 1 und 2 entscheidet, eine Europäische Herausgabeanordnung ganz oder teilweise nicht anzuerkennen oder nicht auszuführen, konsultiert sie in geeigneter Weise die Anordnungsbehörde und ersucht sie gegebenenfalls um unverzügliche Übermittlung aller erforderlichen Angaben.***

***(6) Ist in einem Fall nach Absatz 1 Buchstabe d eine Behörde des Vollstreckungsstaats für die Aufhebung des Vorrechts oder der Immunität zuständig, ersucht die Vollstreckungsbehörde sie unverzüglich, die entsprechende Zuständigkeit wahrzunehmen. Ist eine Behörde eines anderen Staats oder eine internationale Organisation für die Aufhebung des Vorrechts oder der Immunität zuständig, ist es an der Anordnungsbehörde, die betreffende Behörde um Wahrnehmung dieser Zuständigkeit zu ersuchen.***

***(7) Die Vollstreckungsbehörde setzt die Anordnungsbehörde unter Verwendung des Formulars in Anhang III von der Inanspruchnahme einer der in den Absätzen 1 und 2 genannten Gründe für die Versagung der Anerkennung oder der Ausführung in Kenntnis.***

Artikel 11

▌Nutzerinformationen ***und Vertraulichkeit***

(1) ***Der Diensteanbieter unterrichtet die Person, deren Daten angefordert werden, unverzüglich.*** ***Der Diensteanbieter trifft*** die erforderlichen ***dem Stand der Technik entsprechenden betrieblichen und technischen*** Maßnahmen, um die Vertraulichkeit***, Geheimhaltung und Integrität*** des EPOC oder des EPOC-PR sowie der herausgegebenen oder gesicherten Daten zu gewährleisten.

***(1a) So lange wie dies notwendig und verhältnismäßig ist, um eine Behinderung des betreffenden Strafverfahrens zu vermeiden oder die Grundrechte einer anderen Person zu schützen, kann die Anordnungsbehörde unter gebührender Berücksichtigung der Auswirkungen der Maßnahme auf die Grundrechte der Person, deren Daten angefordert werden, den Diensteanbieter auf der Grundlage einer gerichtlichen Anordnung auffordern, davon abzusehen, die Person, deren Daten angefordert werden, hiervon in Kenntnis zu setzen.*** ***In einer solchen Anordnung, die ordnungsgemäß begründet sein muss, ist die Dauer der Geheimhaltungspflicht angegeben, und sie ist regelmäßig zu überprüfen.***

(2) Wenn die Anordnungsbehörde ***die*** Adressaten ***auf der Grundlage einer gerichtlichen Anordnung*** aufgefordert hat, die Person, deren Daten angefordert werden, nicht hiervon in Kenntnis zu setzen, unterrichtet die Anordnungsbehörde die Person, deren Daten mit dem EPOC ***oder dem EPOC-PR*** angefordert wurden, ohne unnötige Verzögerung über die Herausgabe ***bzw. Sicherung*** der Daten. Diese Unterrichtung kann ***unter Berücksichtigung der Rechte der verdächtigen oder beschuldigten Person und unbeschadet der Verteidigungsrechte und wirksamer Rechtsbehelfe*** so lange aufgeschoben werden, wie dies notwendig und verhältnismäßig ist, um eine Behinderung des betreffenden Strafverfahrens zu vermeiden.

(3) Bei der Unterrichtung der Person übermittelt die Anordnungsbehörde auch Informationen über alle verfügbaren Rechtsbehelfe gemäß Artikel 17.

***Artikel 11a***

***Beschränkungen für die Verwendung der eingeholten Informationen***

***Elektronische Informationen, die auf der Grundlage dieser Verordnung erlangt wurden, dürfen nicht für andere Verfahren als diejenigen verwendet werden, für die sie gemäß dieser Verordnung eingeholt wurden, es sei denn, es besteht eine unmittelbare Bedrohung für das Leben oder die körperliche Unversehrtheit einer Person.***

***Artikel 11b***

***Löschung von elektronischen Informationen***

***(1) Elektronische Informationen, die unter Verstoß gegen diese Verordnung eingeholt wurden, sind unverzüglich zu löschen.***

***(2) Elektronische Informationen, die für alle Phasen des Verfahrens, für das sie herausgegeben oder gesichert wurden, einschließlich für etwaige Rechtsbehelfe, nicht mehr benötigt werden, werden unverzüglich gelöscht, es sei denn, dies würde die Verteidigungsrechte des Verdächtigen oder Beschuldigten beeinträchtigen. Es wird festgelegt, dass regelmäßig überprüft wird, ob die elektronischen Informationen noch gespeichert werden müssen.***

***(3) Die Person, deren Daten angefordert wurden, wird unverzüglich über die Löschung unterrichtet.***

***Artikel 11c***

***Zulässigkeit elektronischer Informationen in Gerichtsverfahren***

***Elektronische Informationen, die unter Verstoß gegen diese Verordnung erlangt wurden, unter anderem, wenn die in dieser Verordnung festgelegten Kriterien nicht erfüllt waren, sind vor Gericht nicht zugelassen.*** ***Wurden elektronische Informationen erlangt, bevor ein in Artikel 10a (neu) genannter Grund für die Nichtanerkennung geltend gemacht wurde, sind sie vor Gericht ebenfalls nicht zugelassen.***

Artikel 12

Kostenerstattung

***Auf Antrag des Diensteanbieters erstattet der*** Anordnungsstaat ***die dem Diensteanbieter entstandenen gerechtfertigten Kosten im Zusammenhang mit der Ausführung der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung***. ***Aus praktischen Gründen kann der Diensteanbieter die Erstattung der Kosten vom Vollstreckungsstaat verlangen.*** ***Wenn der Diensteanbieter sich für den Vollstreckungsstaat entscheidet, erstattet der Anordnungsstaat dem Vollstreckungsstaat diese Kosten.*** ***Die Mitgliedstaaten teilen der Kommission die Vorschriften für die Kostenerstattung mit, und die Kommission veröffentlicht diese.***

Kapitel 3: Sanktionen***,*** ***Überprüfungsverfahren und Rechtsbehelfe***

Artikel 13

Sanktionen

(1) ▐ ***Die*** Mitgliedstaaten ***erlasse***n Vorschriften über ▐ Sanktionen, die bei Verstößen gegen die Verpflichtungen aus den Artikeln ***8a,*** 9, 10 und 11 ***in Bezug auf Diensteanbieter in ihrem Hoheitsgebiet*** zu verhängen sind, und treffen alle für die Anwendung finanzieller Sanktionen erforderlichen Maßnahmen. Die ***nach den nationalen Rechtsvorschriften des Mitgliedstaats*** vorgesehenen finanziellen Sanktionen müssen wirksam verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen sowie diesbezügliche spätere Änderungen unverzüglich mit.

***(1a) Ungeachtet der Datenschutzpflichten werden die Diensteanbieter in den Mitgliedstaaten nicht für die Konsequenzen der Befolgung eines EPOC oder eines EPOC-PR haftbar gemacht.***

Artikel 14

Vollstreckungsverfahren

(1) Leistet der ***Diensteanbieter*** ohne Angabe von Gründen, die von der Anordnungsbehörde akzeptiert werden, einem EPOC nicht fristgerecht oder einem EPOC-PR nicht Folge ***und hat die Vollstreckungsbehörde nicht einen der Gründe für die Versagung der Anerkennung oder der Ausführung gemäß Artikel 10a geltend gemacht,*** so kann die Anordnungsbehörde ***die zuständige*** Behörde im Vollstreckungsstaat ***darum ersuchen,*** die Europäische Herausgabeanordnung ▐ oder die Europäische Sicherungsanordnung ***zu vollstrecken▐***.

(2) ▐

(3) ▐ ***Die*** Vollstreckungsbehörde ▐ fordert ▐ den ***Diensteanbieter*** förmlich auf, der entsprechenden Verpflichtung nachzukommen, und setzt ihn davon, dass er unter Geltendmachung der in den ***Artikeln 8a, 9 und 10*** aufgeführten Gründe die ***Ausführung*** ablehnen kann, sowie von den bei Nichtbefolgung anwendbaren Sanktionen in Kenntnis und legt eine Frist für die Befolgung oder Ablehnung fest.

(4) ▐

(5) ▐

(6) Erhebt der ***Diensteanbieter*** Einwände, entscheidet die Vollstreckungsbehörde auf der Grundlage der von dem ***Diensteanbieter*** bereitgestellten Informationen und erforderlichenfalls der von der Anordnungsbehörde ▐ erhaltenen zusätzlichen Informationen, ob sie die Anordnung vollstreckt ***oder nicht anerkennt***. ***Die Vollstreckungsbehörde teilt ihre Entscheidung dem Dienst und der Anordnungsbehörde unverzüglich mit.***

(7) ▐

(8) ▐

(9) Erhält die Vollstreckungsbehörde die Daten von dem ***Diensteanbieter***, so übermittelt sie diese ***unverzüglich*** der Anordnungsbehörde ▐.

(10) Kommt der ***Diensteanbieter*** seinen Verpflichtungen ▐ nicht nach, so verhängt die ***Vollstreckungsbehörde*** eine ▐ Sanktion nach Maßgabe ***von Artikel 13***. Gegen den Beschluss zur Verhängung einer finanziellen Sanktion kann ein wirksamer Rechtsbehelf eingelegt werden.

***Artikel 14 a***

***Überprüfungsverfahren bei einander widersprechenden Verpflichtungen aus dem Recht eines Drittstaats***

***(1) Ist der Diensteanbieter oder die Vollstreckungsbehörde der Ansicht, dass die Befolgung einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung im Widerspruch zu den geltenden Rechtsvorschriften eines Drittstaats steht, die die Offenlegung der betreffenden Daten verbieten‚ so teilt er bzw. sie dies der Anordnungsbehörde und den einschlägigen Adressaten unverzüglich und spätestens innerhalb von zehn Tagen nach Eingang der Anordnung mit. In einem solchen Fall sollte die Ausführung der Anordnung ausgesetzt werden.***

***(2) Diese Mitteilung muss alle sachdienlichen Angaben zu den betreffenden Rechtsvorschriften des Drittstaats, zu ihrer Anwendbarkeit auf den vorliegenden Fall und zu der Art der widersprechenden Verpflichtung enthalten.***

***(3) Auf der Grundlage der folgenden Kriterien überprüft die zuständige Behörde des Anordnungsstaats die Europäische Herausgabeanordnung oder die Europäische Sicherungsanordnung und setzt die Adressaten innerhalb von 10 Tagen nach Eingang der Mitteilung in Kenntnis über:***

***a) die nach den einschlägigen Rechtsvorschriften des Drittstaats geschützten Interessen, einschließlich der Grundrechte und anderer Interessen, die eine Offenlegung der Daten verhindern, insbesondere wenn es um Interessen der nationalen Sicherheit des Drittstaats geht;***

***b) den Grad der Verbindung der Strafsache, wegen der die Anordnung erlassen wurde, zu dem Rechtssystem des Anordnungsstaats und des Drittstaats; hierfür maßgeblich sind unter anderem:***

***i) der Aufenthaltsort, die Staatsangehörigkeit und der Wohnsitz der Person, deren Daten angefordert werden, und/oder des Opfers beziehungsweise der Opfer;***

***ii) der Ort, an dem die betreffende Straftat begangen wurde;***

***c) den Grad der Verbindung zwischen dem Diensteanbieter und dem betreffenden Drittstaat;***

***d) die Interessen des Anordnungsstaats an der Einholung der betreffenden elektronischen Informationen aufgrund der Schwere der Straftat und der Bedeutung einer zügigen Einholung der elektronischen Informationen;***

***e) die möglichen Konsequenzen der Befolgung der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung für die Adressaten, einschließlich der möglicherweise nach den Rechtsvorschriften des Drittstaats gegen die Diensteanbieter zu verhängenden Sanktionen.***

***(4) Innerhalb von zehn Tagen nach Eingang der Mitteilung muss die Anordnungsbehörde die Anordnung zurückziehen, aufrechterhalten oder erforderlichenfalls anpassen, um diese Kriterien umzusetzen. Zu diesem Zweck holt die Anordnungsbehörde bei der zuständigen Behörde des Drittstaats im Einklang mit der Richtlinie (EU) 2016/680 Klarstellungen zu den geltenden Rechtsvorschriften ein, soweit dadurch die in dieser Verordnung vorgesehenen Fristen nicht behindert werden. Im Fall eines Rückzugs setzt die Anordnungsbehörde die Adressaten umgehend davon in Kenntnis.***

***(5) Beschließt die Anordnungsbehörde, die Anordnung aufrechtzuerhalten, so setzt sie die Adressaten von ihrem Beschluss in Kenntnis. Die Vollstreckungsbehörde fasst unter gebührender Berücksichtigung des Beschlusses der Anordnungsbehörde und darüber hinaus nach Konsultation der zuständigen Behörde des Drittstaats im Einklang mit der Richtlinie (EU) 2016/680 – soweit dadurch die in dieser Verordnung vorgesehenen Fristen nicht behindert werden – innerhalb von zehn Tagen nach Eingang des Beschlusses der Anordnungsbehörde einen endgültigen Beschluss auf der Grundlage der Kriterien gemäß Absatz 3 und setzt die Anordnungsbehörde, den Diensteanbieter und die zuständige Behörde des Drittstaats von ihrem endgültigen Beschluss in Kenntnis.***

***(6) Für die Dauer des Verfahrens gemäß Artikel 14a sichert der Diensteanbieter die angeforderten Daten.***

Artikel 15

▐

Artikel 16

▐

Artikel 17

***Wirksame Rechtsbehelfe***

(1) ***Personen***, deren Daten im Wege einer Europäischen Herausgabeanordnung ***oder einer Europäischen Sicherungsanordnung*** ***angefordert*** wurden, haben unbeschadet der nach der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 verfügbaren Rechtsbehelfe das Recht, ▐ wirksame Rechtsbehelfe gegen ***solche Anordnungen*** einzulegen.

(2) ▐

(3) Ein solches Recht auf Einlegung eines wirksamen Rechtsbehelfs wird vor einem Gericht des Anordnungsstaats ***oder des Vollstreckungsstaats*** nach ▐ nationalem Recht ausgeübt und beinhaltet die Möglichkeit, die Rechtmäßigkeit der Maßnahme, einschließlich ihrer Notwendigkeit und Verhältnismäßigkeit, anzufechten.

***(3a) Die sachlichen Gründe für den Erlass der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung werden im Anordnungsstaat angefochten; dies lässt die Garantien der Grundrechte im Vollstreckungsstaat unberührt.***

(4) Unbeschadet des Artikels 11 ergreifen die Anordnungsbehörde ***und die Vollstreckungsbehörde*** die geeigneten Maßnahmen, um zu gewährleisten, dass Informationen über die nach nationalem Recht bestehenden Möglichkeiten zur Einlegung von Rechtsbehelfen***, einschließlich des Zeitpunkts, zu dem diese Rechtsbehelfe gelten, rechtzeitig*** bereitgestellt werden, und sicherzustellen, dass die Rechtsbehelfe effektiv wahrgenommen werden können.

(5) Die Fristen oder sonstigen Bedingungen für die Einlegung eines Rechtsbehelfs entsprechen denen, die in vergleichbaren innerstaatlichen Fällen gelten, und werden in einer Weise angewendet, die die wirksame Ausübung dieser Rechtsbehelfe durch die betroffenen Personen gewährleistet.

(6) ▐

Artikel 18

▐

Kapitel 5: Schlussbestimmungen

Artikel 19

Monitoring und Berichterstattung

(1) Die Kommission erstellt spätestens am ***...*** *[Geltungsbeginn dieser Verordnung]* ein ausführliches Programm für das Monitoring der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung. In dem Monitoring-Programm werden die Instrumente benannt, mit denen Daten und sonstige erforderliche ***Informationen*** erfasst werden, 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 ***Informationen*** zu ergreifen haben.

(2) In jedem Fall führen die Mitgliedstaaten eine ausführliche Statistik, die sie anhand der bei den zuständigen Behörden erhobenen Daten erstellen. Die erhobenen Daten werden der Kommission jährlich bis zum 31. März für das vorhergehende Kalenderjahr übermittelt und umfassen:

a) die Zahl der ausgestellten EPOC und EPOC-PR, aufgeschlüsselt nach der Art der angeforderten Daten, ***den Adressaten*** und der jeweiligen Situation (Notfall oder nicht);

***aa) die Zahl der unter Ausnahmeregelungen für Notfälle ausgestellten EPOC, einschließlich Angaben zu den Umständen und möglichen Ergebnissen;***

***ab) die Zahl der ausgestellten EPOC und EPOC-PR, bei denen die Anordnungsbehörde Gebrauch von der Möglichkeit nach Artikel 11 Absatz 1a gemacht hat, den Diensteanbieter darum zu ersuchen, die Person, deren Daten angefordert werden, nicht hiervon in Kenntnis zu setzen, einschließlich Informationen zu den Umständen und einer möglichen späteren Unterrichtung nach Artikel 11 Absatz 2;***

b) die Zahl der EPOC ***und EPOC-PR***, denen Folge geleistet und denen nicht Folge geleistet wurde, aufgeschlüsselt nach der Art der angeforderten Daten, ***den*** ***Adressaten*** und der jeweiligen Situation (Notfall oder nicht);

***ba)*** ***die Zahl der EPOC, die abgelehnt wurden, aufgeschlüsselt nach der Art der angeforderten Daten, den Adressaten, der jeweiligen Situation (Notfall oder nicht) und den für die Versagung der Anerkennung oder der Vollstreckung geltend gemachten Gründe;***

c) im Falle von EPOC, denen Folge geleistet wurde, die bis zum Erhalt der angeforderten Daten durchschnittlich vergangene Zeit – vom Zeitpunkt der Ausstellung eines EPOC bis zum Zeitpunkt des Datenerhalts, aufgeschlüsselt nach der Art der angeforderten Daten, ***den Adressaten*** und der jeweiligen Situation (Notfall oder nicht)

***ca)*** ***im Falle von EPOC-PR, denen Folge geleistet wurde, die für das jeweilige EPOC-Verfahren im Anschluss an das EPOC-PR durchschnittlich vergangene Zeit – vom Zeitpunkt der Ausstellung des EPOC-PR bis zum Zeitpunkt der Ausstellung des EPOC, aufgeschlüsselt nach der Art der angeforderten Daten und den Adressaten;***

d) ▐;

e) die Zahl der Rechtsbehelfe, die gegen Europäische Herausgabeanordnungen ***und Europäische Sicherungsanordnungen*** im Anordnungsstaat und im Vollstreckungsstaat eingelegt wurden, aufgeschlüsselt nach der Art der angeforderten Daten***;***

***f) die verhängten Sanktionen gemäß Artikel 13, aufgeschlüsselt nach der Art der angeforderten Daten, den Adressaten, der jeweiligen Situation (Notfall oder nicht) und der Höhe der Sanktionen;***

***g) eine Übersicht über die von Diensteanbietern im Zusammenhang mit der Ausführung des EPOC oder des EPOC-PR geltend gemachten Kosten und die von den Anordnungsbehörden erstatteten Kosten;***

***h) die Zahl der eingeleiteten Vollstreckungsverfahren, aufgeschlüsselt nach der Art der angeforderten Daten, den Adressaten, der jeweiligen Situation (Notfall oder nicht) und dem Endergebnis.***

***(2a) Die Kommission veröffentlicht bis zum 30. Juni eines jeden Jahres einen Bericht, der die in Absatz 2 genannten Daten in zusammengefasster Form und nach Mitgliedstaaten aufgeschlüsselt enthält.***

Artikel 20

▐

Artikel 21

▐

Artikel 22

***Mitteilungen***

(1) Jeder Mitgliedstaat ***...***teilt der Kommission bis zum [***12 Monate vor dem*** *Geltungsbeginn dieser Verordnung*] Folgendes mit:

a) die Behörden, die im Einklang mit dem nationalen Recht gemäß Artikel 4 befugt sind, Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen zu erlassen und zu validieren;

b) die Vollstreckungsbehörde, ***an die das EPOC oder das EPOC-PR zur Ausführung oder*** ***Vollstreckung Europäischer*** Herausgabeanordnungen und ***Europäischer*** Sicherungsanordnungen ***übermittelt wird***;

***ba)*** ***wenn Diensteanbieter oder Mitgliedstaaten bereits spezielle Systeme oder andere gesicherte Kanäle für die Bearbeitung von Datenersuchen für Strafverfolgungszwecke eingerichtet haben, die Mittel und technischen Schnittstellen, die den zuständigen Behörden zur Verfügung stehen, um Daten zu empfangen oder abzurufen, die zwecks Verbindung mit dem System nach Artikel 7a erstellt wurden;***

c) ▐

***(1a) Bis zum selben Zeitpunkt unterrichten Diensteanbieter mit Niederlassungen in mehr als einem Mitgliedstaat die Kommission über den Ort ihrer Hauptniederlassung in der Union.***

(2) Die Kommission macht die nach Maßgabe dieses Artikels erhaltenen Informationen entweder auf einer eigens dafür eingerichteten Website oder auf der Website des Europäischen Justiziellen Netzes ***für Strafsachen***, auf die Artikel 9 des Beschlusses 2008/976/JI des Rates Bezug nimmt, öffentlich zugänglich[[22]](#footnote-22).

Artikel 23

Bezug zu Europäischen Ermittlungsanordnungen ***und Rechtshilfeverfahren***

Die Behörden der Mitgliedstaaten können weiterhin Europäische Ermittlungsanordnungen im Einklang mit der Richtlinie 2014/41/EU erlassen ***oder bestehende Rechtshilfeverfahren*** für die Erhebung von ***elektronischen Informationen anwenden***, die unter diese Verordnung fallen würden.

Artikel 24

Bewertung

Spätestens am ***...*** *[****zwei*** *Jahre nach dem Geltungsbeginn dieser Verordnung]* führt die Kommission eine Bewertung der Verordnung durch und legt dem Europäischen Parlament und dem Rat einen Bericht über das Funktionieren der Verordnung vor, in dessen Rahmen ***insbesondere auch die Zahl der Fälle bewertet wird, in denen die Ausnahmeregelung für Notfälle gemäß Artikel 9 Absatz 2 und die Ausnahmeregelung vom Grundsatz der Nutzerinformationen gemäß Artikel 11 Anwendung finden***.▐ ***Dem*** Bericht ***werden* *eine Bewertung des Funktionierens des gemeinsamen europäischen Austauschsystems sowie eine Bewertung des Funktionierens der Verordnung in Bezug auf die Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates*** beigefügt.Die Bewertung wird gemäß den Leitlinien der Kommission für eine bessere Rechtsetzung vorgenommen. Die Mitgliedstaaten übermitteln der Kommission die für die Ausarbeitung dieses Berichts erforderlichen Informationen.

Artikel 25

Inkrafttreten

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

Sie gilt ab dem … [***18*** Monate nach ihrem Inkrafttreten].

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt gemäß den Verträgen unmittelbar in den Mitgliedstaaten.

Geschehen zu ***Straßburg*** am […]

Im Namen des Europäischen Parlaments Im Namen des Rates

Der Präsident Der Präsident

ANHANG I

ZERTIFIKAT ÜBER EINE EUROPÄISCHE HERAUSGABEANORDNUNG (EPOC) ZUR

HERAUSGABE ELEKTRONISCHER ***INFORMATIONEN***

Gemäß der Verordnung (EU)… [1](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52018PC0225#footnote2) muss ***das Zertifikat*** über eine Europäische Herausgabeanordnung (EPOC) ***zu seiner Vollstreckung direkt und gleichzeitig an den Diensteanbieter und die Vollstreckungsbehörde gerichtet werden***. Werden die Daten nicht herausgegeben, ist der Adressat nach Erhalt des EPOC verpflichtet, die angeforderten Daten zu sichern, es sei denn, er kann diese Daten nicht anhand der Angaben im EPOC identifizieren. Die Daten werden bis zur Herausgabe gesichert, oder bis die Anordnungsbehörde oder gegebenenfalls die Vollstreckungsbehörde mitteilt, dass die Sicherung und Herausgabe von Daten nicht mehr erforderlich ist.

***Die Adressaten treffen*** die erforderlichen Maßnahmen, um die Vertraulichkeit des EPOC sowie der herausgegebenen oder gesicherten Daten sicherzustellen.

ABSCHNITT A:

Anordnungsstaat: ………………………………………………………………………………..

Hinweis: Nähere Informationen zur Anordnungsbehörde sind am Ende anzugeben (Abschnitte E und F).

***Adressaten (bitte kreuzen Sie das zutreffende Kästchen an):***

***– Diensteanbieter oder gegebenenfalls sein Vertreter:***

***– Vollstreckungsbehörde:***

ABSCHNITT B: Fristen

Die angeforderten Daten sind binnen folgender Fristen herauszugeben (Zutreffendes bitte ankreuzen und ggf. erläutern):

□ spätestens binnen 10 Tagen***, sofern die Vollstreckungsbehörde nicht einen der Gründe für die Versagung der Anerkennung oder der Vollstreckung geltend gemacht hat;***

□ spätestens binnen ***16 Stunden*** in einem Notfall***, sofern die Vollstreckungsbehörde nicht einen der Gründe für die Versagung der Anerkennung oder der Vollstreckung geltend gemacht hat***;

– einer unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit einer Person. Begründung▐:

▐

ABSCHNITT C: ***Informationen für den Nutzer***

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

□ der ***Diensteanbieter*** die Person, deren Daten ***auf der Grundlage einer gerichtlichen Entscheidung*** mit dem EPOC angefordert werden, hiervon nicht in Kenntnis setzen darf. ***Begründung: …***

ABSCHNITT D: Herauszugebende elektronische ***Informationen***

i) Dieses EPOC betrifft (Zutreffendes bitte ankreuzen):

□ Teilnehmerdaten▐:

□ Name, Anschrift, Geburtsdatum, Kontaktangaben (E-Mail-Adresse, Telefonnummer) und andere einschlägige Angaben zur Identität des Nutzers/Teilnehmers

□ Datum und Uhrzeit der ersten Registrierung/Anmeldung, Art der Registrierung/Anmeldung, Kopie des Vertrags, Methode der Identitätsüberprüfung zum Zeitpunkt der Registrierung/Anmeldung, Kopien der vom Teilnehmer vorgelegten Dokumente

□ Art des Dienstes, einschließlich Identifikator (Telefonnummer,▐ SIM-Kartennummer, MAC-Adresse) und zugehörige(s) Gerät/Geräte

□ Angaben zum Profil (Nutzername, Profilbild)

□ Daten über die Validierung der Nutzung des Dienstes, z. B. eine vom Nutzer/Teilnehmer angegebene alternative E-Mail-Adresse

▐

□ PUK-Codes

□ ***IP-Adresse zum einzigen Zweck der Identifizierung des Nutzers:***

***– IP-Adresse***

– IP-Verbindungsdaten/-protokolle zu Identifizierungszwecken

□ Verkehrsdaten▐:

a) für (Mobil-)Telefonie

□ ausgehende (A) und eingehende (B) Identifikatoren (Telefonnummer, IMSI, IMEI)

□ Zeit und Dauer der Verbindungen

□ Anrufversuche

□ ID der Basisstation, einschließlich geografischer Koordinaten (X/Y-Koordinaten) zum Zeitpunkt des Verbindungsaufbaus und -endes

□ genutzter Träger-/Teledienst (z. B. UMTS, GPRS)

b) für Internet:

□ Routing-Informationen (Quell-IP-Adresse, Ziel-IP-Adresse(n), Port-Nummer(n), Browser,▐ Message-ID)

□ ID der Basisstation, einschließlich geografischer Koordinaten (X/Y-Koordinaten) zum Zeitpunkt des Verbindungsaufbaus und -endes

□ Datenvolumen

c) für Hosting:

□ Protokolldateien

□ Tickets

□ Kaufhistorie

***– Historie über Prepaid-Aufladevorgänge***

▐

□ Inhaltsdaten▐:

***– Kontaktlisten***

□ (Web-)Mailbox-Dump

□ Online-Storage-Dump (vom Nutzer generierte Daten)

□ Pagedump

□ Message log/Backup

□ Voicemail-Dump

□ Server-Inhalte

□ Geräte-Backup

ii) ***Zusätzliche*** Informationen ▐ zur Ausführung des EPOC▐:

   IP-Adresse:…………………………………………………………………………..

   Telefonnummer:………………………………………………………………….

   E-Mail-Adresse:……………………………………………………………………...

   IMEI-Nummer:……………………………………………………………………….

   MAC-Adresse:……………………………………………………………………….

   Person(en), deren Daten angefordert werden:………………………….…………..

   Name des Dienstes: ………………………………………………………………..

   Sonstiges: ……………………………………………………………………………….

iii) ▐ ***Die*** Zeitspanne, für die die Herausgabe angefordert wird:

……..…………………………………………………………………………………………….

iv) Bitte beachten Sie, dass (bitte ankreuzen und ausfüllen, sofern zutreffend):

□ die angeforderten Daten aufgrund eines früheren Ersuchens um Datensicherung folgender Behörde gespeichert wurden: .………………………………………………......…… (Bitte die Behörde angeben und – sofern bekannt – das Datum der Übermittlung des Ersuchens sowie die Referenznummer). Diese Daten wurden übermittelt an: ………………………………………………..…………………………………………… (Bitte ***Adressaten*** angeben, an ▐ die das Ersuchen übermittelt wurde, sowie – falls bekannt – die vom Adressaten angegebene Referenznummer).

v) Art und rechtliche Würdigung der Straftat(en), die dem EPOC zugrunde liegen, und anwendbare Gesetzes-/Rechtsnorm:

……………………………………………..……………………………….……………………

Das vorliegende EPOC betrifft die Herausgabe von ***Verkehrs-*** und/oder Inhaltsdaten im Zusammenhang mit (sofern zutreffend, bitte ankreuzen):

    Straftat(en), die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet wird/werden;

folgende Straftat(en), wenn diese ganz oder teilweise mittels eines Informationssystems begangen wurde(n):

Straftat(en) im Sinne der Artikel 3, 4 und 5 des Rahmenbeschlusses 2001/413/JI des Rates;

Straftat(en) im Sinne der Artikel 3 bis 7 der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates;

Straftat(en) im Sinne der Artikel 3 bis 8 der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates;

Straftat(en) im Sinne der Artikel 3 bis 12 und 14 der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates.

vi) Bitte beachten Sie, dass (sofern zutreffend, bitte ankreuzen):

die angeforderten Daten als Teil einer Infrastruktur gespeichert oder verarbeitet werden, die ein Diensteanbieter für ein Unternehmen oder eine Einrichtung, die keine natürliche Person ist, bereitstellt, und das vorliegende EPOC an den Diensteanbieter gerichtet ist, da auf das Unternehmen oder die Einrichtung abzielende Ermittlungsmaßnahmen nicht geeignet sind, insbesondere weil sie die Ermittlung beeinträchtigen könnten.

vii) Sonstige sachdienliche Informationen:

………………………………………….……………………………….………………………

ABSCHNITT E: Angaben zur Behörde, die das EPOC ausgestellt hat

Art der Behörde, die das vorliegende EPOC ausgestellt hat (Zutreffendes bitte ankreuzen):

□ Richter, Gericht oder Ermittlungsrichter

□ Staatsanwalt (für Teilnehmer▐daten ***und IP-Adressen zum alleinigen Zweck der Bestimmung der Identität von Einzelpersonen***)

Staatsanwalt (für ***Verkehrs***- und Inhaltsdaten) → bitte auch Abschnitt F ausfüllen

□ andere vom Anordnungsstaat bezeichnete zuständige Behörde → bitte auch Abschnitt F ausfüllen

Angaben zur Anordnungsbehörde und/oder ihrem Vertreter zur Bescheinigung der inhaltlichen Richtigkeit des EPOC:

Name der Behörde:…………………………………..…………………………………………

Name ihres Vertreters:………….……………………...………………………………………..

Funktion (Titel/Amtsbezeichnung):……………………...…………………………………….

Dossier Nr.:….…………………………………………………………..……………………...

Anschrift:…………………………………………………………………..…………………....

Telefon: (Landesvorwahl) (Ortsvorwahl)………………………………………..…………….

Fax: (Landesvorwahl) (Ortsvorwahl)……………………………………..……………..…….

E-Mail:……………………………………………………………………………..…..……….

Datum:    ……………………………………………………………………………….………

Amtlicher Stempel (sofern vorhanden) und Unterschrift:………………………………...……

|  |
| --- |
| ABSCHNITT F: Nähere Angaben zur Behörde, die das EPOC validiert hatArt der Behörde, die das vorliegende EPOC validiert hat (Zutreffendes bitte ankreuzen):□ Richter, Gericht oder Ermittlungsrichter□ Staatsanwalt (für Teilnehmer▐daten ***und IP-Adressen zum alleinigen Zweck der Bestimmung der Identität von Einzelpersonen***)Angaben zur validierenden Behörde und/oder ihrem Vertreter zur Bestätigung der inhaltlichen Richtigkeit des EPOC:Name der Behörde:…………………………………..…………………………………………Name ihres Vertreters:………….……………………...………………………………………..Funktion (Titel/Amtsbezeichnung):……………………...…………………………………….Dossier Nr.:….…………………………………………………………..……………………...Anschrift: .…………………………………………………...……………………..…………..Telefon: (Landesvorwahl) (Ortsvorwahl)……………………………………..……………..…….Fax: (Landesvorwahl) (Ortsvorwahl)……………………………………..……………..…….E-Mail:……………………………………………………………………………..…..……….Datum:    ………………...…………………………………………………….………………….Amtlicher Stempel (sofern vorhanden) und Unterschrift:………………………………...…… |

ABSCHNITT G: Übermittlung von Daten und Kontaktangaben

i) Behörde, an die die Daten zu übermitteln sind (Zutreffendes bitte ankreuzen und ggf. erläutern):

□ Anordnungsbehörde

□ validierende Behörde

□ andere vom Anordnungsstaat bezeichnete zuständige Behörde:..............................

ii) Behörde/Ansprechpartner für Rückfragen im Zusammenhang mit der Ausführung des EPOC:...........................................................................................................................................

ANHANG II

ZERTIFIKAT ÜBER EINE EUROPÄISCHE SICHERUNGSANORDNUNG (EPOC-PR) ZUR

SICHERUNG ELEKTRONISCHER ***INFORMATIONEN***

Gemäß der Verordnung (EU)... [2](https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1524129181403&uri=COM%3A2018%3A225%3AFIN#footnote3) muss ***das Zertifikat*** über eine Europäische Sicherungsanordnung (EPOC-PR) ***zu seiner Vollstreckung direkt und gleichzeitig an den Diensteanbieter (oder gegebenenfalls seinen Vertreter) und*** die ***Vollstreckungsbehörde gerichtet werden***. Die Sicherung endet nach 60 Tagen, es sei denn, die Anordnungsbehörde bestätigt, dass ein entsprechendes Ersuchen um Herausgabe in die Wege geleitet wurde. Wenn die Anordnungsbehörde binnen dieser 60 Tage bestätigt, dass ein Ersuchen um Herausgabe in die Wege geleitet wurde, sichert der Adressat die Daten so lange, wie dies erforderlich ist, um die Daten nach Eingang des entsprechenden Ersuchens um Herausgabe herauszugeben.

***Die***Empfänger ***treffen*** die erforderlichen Maßnahmen, um die Vertraulichkeit des EPOC-PR sowie der gesicherten oder herausgegebenen Daten sicherzustellen.

ABSCHNITT A:

Anordnungsstaat: …………………………………………………………………………..…

   Hinweis: Informationen zur Anordnungsbehörde sind am Ende anzugeben (Abschnitte D und E).

***Adressaten (Zutreffendes bitte ankreuzen und ergänzen):***

***– Diensteanbieter oder gegebenenfalls sein Vertreter: ...***

***– Vollstreckungsbehörde: ...***

ABSCHNITT B: ***Informationen für den Nutzer***

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

□ der ***Diensteanbieter*** die Person, deren Daten ***auf der Grundlage einer gerichtlichen Entscheidung*** mit dem EPOC-PR angefordert werden, nicht hiervon in Kenntnis setzen darf. ***Begründung: …***

ABSCHNITT C: Zu sichernde elektronische ***Informationen***

i) Dieses EPOC-PR betrifft (Zutreffendes bitte ankreuzen):

□ Teilnehmerdaten▐:

□ Name, Anschrift, Geburtsdatum, Kontaktangaben (E-Mail-Adresse, Telefonnummer) und andere einschlägige Angaben zur Identität des Nutzers/Teilnehmers

□ Datum und Uhrzeit der ersten Registrierung/Anmeldung, Art der Registrierung/Anmeldung, Kopie des Vertrags, Methode der Identitätsüberprüfung zum Zeitpunkt der Registrierung/Anmeldung, Kopien der vom Teilnehmer vorgelegten Dokumente

□ Art des Dienstes, einschließlich Identifikator (Telefonnummer,▐ SIM-Kartennummer, MAC-Adresse) und zugehörige(s) Gerät/Geräte

□ Angaben zum Profil (Nutzername, Profilbild)

□ Daten über die Validierung der Nutzung des Dienstes, z. B. eine vom Nutzer/Teilnehmer angegebene alternative E-Mail-Adresse

▐

□ PUK-Codes

***IP-Adressen zum einzigen Zweck der Identifizierung des Nutzers:***

* ***IP-Adresse***
* IP-Verbindungsdaten/-protokolle zu Identifizierungszwecken

▐

□ Verkehrsdaten▐:

a) für (Mobil-)Telefonie

□ ausgehende (A) und eingehende (B) Identifikatoren (Telefonnummer, IMSI, IMEI)

□ Zeit und Dauer der Verbindungen

□ Anrufversuche

□ ID der Basisstation, einschließlich geografischer Koordinaten (X/Y-Koordinaten) zum Zeitpunkt des Verbindungsaufbaus und -endes

□ genutzter Träger-/Teledienst (z. B. UMTS, GPRS)

b) für Internet:

□ Routing-Informationen (Quell-IP-Adresse, Ziel-IP-Adresse(n), Port-Nummer(n), Browser,▐ Message-ID)

□ ID der Basisstation, einschließlich geografischer Koordinaten (X/Y-Koordinaten) zum Zeitpunkt des Verbindungsaufbaus und -endes

□ Datenvolumen

c) für Hosting:

□ Protokolldateien

□ Tickets

□ Kaufhistorie

□ sonstige ***Verkehrsdaten***▐:

□ Historie über Prepaid-Aufladevorgänge

▐ Inhaltsdaten▐:

***– Kontaktliste***

□ (Web-)Mailbox-Dump

□ Online-Storage-Dump (vom Nutzer generierte Daten)

□ Pagedump

□ Message log/Backup

□ Voicemail-Dump

□ Server-Inhalte

□ Geräte-Backup

ii) ***Zusätzliche*** Informationen ▐ zur Ausführung des EPOC-PR▐:

   IP-Adresse:………………………………………………………………………..

   Telefonnummer:…………………………………………………………….….….

   E-Mail-Adresse:……………………………………………………………....…...

   IMEI-Nummer:……………………………………………………………….…...

   MAC-Adresse:…………………………………………………………………….

   Person(en), deren Daten angefordert werden:…………………………….………..

   Name des Dienstes: ………………………………………………………………..

   Sonstiges: …………………………………………………….……………………

iii) ▐ ***Die*** Zeitspanne, für die die Sicherung angefordert wird:

……..…………………………………………………………………………………………….

iv) Art und rechtliche Würdigung der Straftat(en), die dem EPOC-PR zugrunde liegen, und anwendbare Gesetzes-/Rechtsnorm:

…………………………………………………………………………………..………….……

v) Sonstige sachdienliche Angaben:

…………………………………………………………………………………..………….……

ABSCHNITT D: Nähere Angaben zur Behörde, die das EPOC-PR ausgestellt hat

Art der Behörde, die das vorliegende EPOC-PR ausgestellt hat (Zutreffendes bitte ankreuzen):

□ Richter, Gericht oder Ermittlungsrichter

□ Staatsanwalt

□ andere vom Anordnungsstaat bezeichnete zuständige Behörde → bitte auch Abschnitt E ausfüllen

Angaben zur Anordnungsbehörde und/oder ihrem Vertreter zur Bescheinigung der inhaltlichen Richtigkeit des EPOC-PR:

Name der Behörde:…………………………………..…………………………………………

Name ihres Vertreters:………….……………………...………………………………………..

Funktion (Titel/Amtsbezeichnung):…...….

Dossier Nr.:….…………………………………………………………..……………………...

Anschrift:.…………………………………………………………….………………………..

Telefon: (Landesvorwahl) (Ortsvorwahl)…..….

Fax: (Landesvorwahl) (Ortsvorwahl)…..….

E-Mail:……………………………………………………………………………..…..……….

Datum:    …………………………………………………………………………………………

Amtlicher Stempel (sofern vorhanden) und Unterschrift:…...…

ABSCHNITT E: Nähere Angaben zur Behörde, die das EPOC-PR validiert hat

Art der Behörde, die das vorliegende EPOC-PR validiert hat (Zutreffendes bitte ankreuzen):

□ Richter, Gericht oder Ermittlungsrichter

□ Staatsanwalt

Angaben zur validierenden Behörde und/oder ihrem Vertreter zur Bestätigung der inhaltlichen Richtigkeit des EPOC-PR:

Name der Behörde:…………………………………..…………………………………………

Name ihres Vertreters:………….……………………...………………………………………..

Funktion (Titel/Amtsbezeichnung):…...….

Dossier Nr.:….…………………………………………………………..……………………...

Anschrift: ………………………………………………………………………………………..

Telefon: (Landesvorwahl) (Ortsvorwahl)…..….

Fax: (Landesvorwahl) (Ortsvorwahl)…..….

E-Mail:……………………………………………………………………………..…..……….

Datum:    …………………………………………………………………………………………..

Amtlicher Stempel (sofern vorhanden) und Unterschrift:…...…

|  |
| --- |
| ABSCHNITT F: KontaktangabenBehörde/Ansprechpartner für Rückfragen im Zusammenhang mit der Ausführung des EPOC-PR: ……………………………………………………………………………………………… |

ANHANG III

INFORMATIONEN ÜBER DIE UNMÖGLICHKEIT, DAS EPOC/EPOC-PR AUSZUFÜHREN***, ODER DIE VERSAGUNG DER ANERKENNUNG DES EPOC***

ABSCHNITT A:

Die nachfolgenden Informationen betreffen:

□ die Europäische Herausgabeanordnung (EPOC)

□ die Europäische Sicherungsanordnung (EPOC-PR)

ABSCHNITT B:

***Adressaten*** des EPOC/EPOC-PR:

***– Diensteanbieter oder gegebenenfalls sein Vertreter: ...***

***– Vollstreckungsbehörde: ...***

Behörde, die das EPOC/EPOC-PR ausgestellt hat: …………………………..…………………

Behörde, die das EPOC/EPOC-PR validiert hat (sofern zutreffend): ………………………….

ABSCHNITT C:

Referenznummer des Adressaten des EPOC/EPOC-PR: ……………………….…………….

Referenznummer der Anordnungsbehörde: ……………………………………………………

Referenznummer der validierenden Behörde ***(sofern zutreffend)***:

Datum der Übermittlung des EPOC/EPOC-PR ▐ : ………………...…………………

ABSCHNITT D: Gründe für die Unmöglichkeit der Ausführung ***des EPOC/EPOC-PR***

(i) Das EPOC/EPOC-PR kann aus folgendem Grund (folgenden Gründen) nicht ausgeführt werden oder nicht in der vorgeschriebenen Frist ausgeführt werden:

□ Das EPOC/EPOC-PR ist unvollständig.

□ Das EPOC/EPOC-PR enthält offensichtliche ***formale oder inhaltliche*** Fehler.

□ EPOC/EPOC-PR enthält keine ausreichenden Angaben.

□ Aufgrund höherer Gewalt oder einer ***durch die Umstände bedingten*** faktischen Unmöglichkeit, die dem Adressaten oder dem Diensteanbieter nicht angelastet werden ***können***.

□ Die Europäische Herausgabeanordnung wurde nicht von einer Anordnungsbehörde nach Artikel 4 der Verordnung (EU) … erlassen oder validiert.

□ Die Europäische Sicherungsanordnung wurde nicht von einer Anordnungsbehörde nach Artikel 4 der Verordnung (EU) … erlassen oder validiert.

□ Die Europäische Herausgabeanordnung wurde nicht wegen einer Straftat nach Artikel 5 Absatz 4 der Verordnung (EU) … erlassen.

□ Der ***Diensteanbieter*** fällt nicht unter die Verordnung (EU) … .

□ Die Europäische Herausgabeanordnung/Europäische Sicherungsanordnung betrifft keine Daten, die zum Zeitpunkt ***der Ausstellung*** des EPOC/EPOC-PR von einem Diensteanbieter oder in dessen Auftrag gespeichert wurden.

□ Ausschließlich aus den in dem EPOC/EPOC-PR enthaltenen Informationen geht hervor, dass das EPOC/EPOC-PR ▐ offensichtlich missbräuchlich ist ***oder über den Zweck der Anordnung hinausgeht***.

□ Die Befolgung der Europäischen Herausgabeanordnung ***bzw. der Europäischen Sicherungsanordnung*** würde im Widerspruch zu den geltenden Rechtsvorschriften eines Drittstaats stehen, die die Offenlegung der betreffenden Daten verbieten.

ii) Bitte erläutern Sie, weshalb das EPOC / EPOC-PR nicht ausgeführt wurde, und nennen Sie erforderlichenfalls weitere Gründe, die nicht unter Buchstabe i) dieses Abschnitts aufgeführt sind:

………………………………………………………………………………………………….

***ABSCHNITT Da:***

***Gründe für die Versagung der Anerkennung des EPOC oder die Unmöglichkeit, das EPOC auszuführen (Zutreffendes bitte ankreuzen):***

***Für alle EPOC:***

***□ Die Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung gemäß Artikel 5 der vorliegenden Verordnung sind nicht erfüllt;***

***□ die Ausführung der Europäischen Herausgabeanordnung würde dem Grundsatz „ne bis in idem“ zuwiderlaufen;***

***□ es bestehen berechtigte Gründe für die Annahme, dass die Ausführung der Europäischen Herausgabeanordnung mit den Verpflichtungen des Mitgliedstaats nach Artikel 6 EUV und der Charta unvereinbar wäre;***

***□ es bestehen nach dem Recht des Vollstreckungsstaats Immunitäten, Vorrechte oder Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit im Zusammenhang mit der Pressefreiheit und der Freiheit der Meinungsäußerung in anderen Medien, die es unmöglich machen, die Europäische Herausgabeanordnung auszuführen;***

***Im Falle eines EPOC für Verkehrs- und Inhaltsdaten:***

***□ Die Ausführung der Europäischen Herausgabeanordnung würde wesentliche nationale Sicherheitsinteressen beeinträchtigen, die Informationsquelle gefährden oder die Verwendung von Verschlusssachen über spezifische nachrichtendienstliche Tätigkeiten voraussetzen;***

***□ die Europäische Herausgabeanordnung bezieht sich auf eine Straftat, die mutmaßlich außerhalb des Hoheitsgebiets des Anordnungsstaats und ganz oder teilweise auf dem Hoheitsgebiet des Vollstreckungsstaats begangen wurde, und die Handlung, aufgrund derer das EPOC ergangen ist, stellt nach dem Recht des Vollstreckungsstaats keine Straftat dar;***

***□ die Handlung, aufgrund deren das EPOC erlassen wurde, stellt nach dem Recht des Vollstreckungsstaats keine Straftat dar, es sei denn, sie betrifft eine Straftat, die unter den in Anhang IIIa aufgeführten Kategorien von Straftaten genannt wird – wie von der Anordnungsbehörde im EPOC angegeben –, sofern diese Straftat im Anordnungsstaat mit einer Freiheitsstrafe oder freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist;***

***□ die Ausführung der Europäischen Herausgabeanordnung ist nach dem Recht des Vollstreckungsstaats auf eine Liste oder Kategorie von Straftaten oder auf Straftaten, die mit einem höherem Mindeststrafmaß bedroht sind, beschränkt;***

***□ die Befolgung einer Europäischen Herausgabeanordnung würde im Widerspruch zu den geltenden Rechtsvorschriften eines Drittstaats stehen, die die Offenlegung der betreffenden Daten verbieten.***

ABSCHNITT E: Einander widersprechende Verpflichtungen aufgrund von Rechtsvorschriften eines Drittstaats

Im Falle einander widersprechender Verpflichtungen aufgrund von Rechtsvorschriften eines Drittstaats bitte Folgendes angeben:

– Bezeichnung der Rechtsvorschrift(en) des Drittstaats, einschließlich der einschlägigen Bestimmung(en):

…………………………………………………………………….…………………………….

– Wortlaut der einschlägigen Bestimmung(en):

…………………………………………………..………………………………..…………….

– Art der einander widersprechenden Verpflichtungen, u. a. das nach Rechtsvorschriften des Drittstaats geschützte Interesse:

□ Grundrechte natürlicher Personen (bitte angeben):

……………………………………………………………………………….………………..

□ grundlegende Interessen des Drittstaats im Zusammenhang mit der nationalen Sicherheit oder Verteidigung (bitte angeben):

…………………………………………………………………………………………………..

□ andere Interessen (bitte angeben):

…………………………………………………..……………………………………………….

– Bitte erläutern Sie, weshalb die Rechtsvorschriften in diesem Fall Anwendung finden:

……………………………………………………………..………………….…..……………..

– Bitte erläutern Sie, weshalb in diesem Fall ein Widerspruch besteht:

……………………………………………………………………..……………………………

– Bitte erläutern Sie die Verbindung zwischen dem Diensteanbieter und dem betreffenden Drittstaat:

…………………………………………………………………………………….……………..

– Bitte erläutern Sie die möglichen Konsequenzen der Befolgung der Europäischen Herausgabeanordnung für den Adressaten, einschließlich der möglicherweise zu verhängenden Sanktionen:

……………………………………………………………………………...……………….…...

ABSCHNITT F: Angeforderte Informationen

Zur Ausführung des EPOC/EPOC-PR bedarf es weiterer Informationen seitens der Anordnungsbehörde (sofern zutreffend, bitte ausfüllen):

……………………………………………………………………………….…………………..

ABSCHNITT G: Datensicherung

Die angeforderten Daten (bitte Zutreffendes ankreuzen und ggf. ergänzen):

□ werden ***von der*** Anordnungsbehörde ***für die Dauer von fünf Tagen zur Klarstellung*** oder***, falls erforderlich, zur Korrektur*** gesichert;

□ werden nicht ***herausgegeben oder*** gesichert, da sie nicht anhand der Angaben im EPOC/EPOC-PR identifiziert werden können;

***□ werden nicht herausgegeben, da einer der Gründe für die Versagung der Anerkennung oder die Unmöglichkeit, das EPOC auszuführen, besteht.***

ABSCHNITT H: Angaben zum Diensteanbieter bzw. ***gegebenenfalls*** seinem Vertreter

Name des Diensteanbieters/Vertreters:….….…..

Name der bevollmächtigten Person:…

Amtlicher Stempel (sofern vorhanden) und Unterschrift:…...…

***ANHANG IIIa***

***Kategorien von Straftaten gemäß Artikel 10a Absatz 2 Buchstabe c***

– ***Beteiligung an einer kriminellen Vereinigung***

– ***Terrorismus***

– ***Menschenhandel***

– ***sexuelle Ausbeutung von Kindern und Kinderpornografie***

– ***illegaler Handel mit Drogen und psychotropen Stoffen***

– ***illegaler Handel mit Waffen, Munition und Sprengstoffen***

– ***Korruption***

– ***Betrugsdelikte, einschließlich des Betrugs zum Nachteil der finanziellen Interessen der Europäischen Union im Sinne des Übereinkommens vom 26. Juli 1995 über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften***

– ***Wäsche von Erträgen aus Straftaten***

– ***Geldfälschung einschließlich der Euro-Fälschung***

– ***Cyberkriminalität***

– ***Umweltkriminalität, einschließlich des illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten***

– ***Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt***

– ***Mord, schwere Körperverletzung***

– ***illegaler Handel mit menschlichen Organen und menschlichem Gewebe***

– ***Entführung, Freiheitsberaubung und Geiselnahme***

– ***Rassismus und Fremdenfeindlichkeit***

– ***Raub in organisierter Form oder mit Waffen***

– ***illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenständen***

– ***Betrug***

– ***Erpressung und Schutzgelderpressung***

– ***Nachahmung und Produktpiraterie***

– ***Fälschung von amtlichen Dokumenten und Handel damit***

– ***Fälschung von Zahlungsmitteln***

– ***Illegaler Handel mit Hormonen und anderen Wachstumsförderern***

– ***illegaler Handel mit nuklearen und radioaktiven Substanzen***

– ***Handel mit gestohlenen Kraftfahrzeugen***

– ***Vergewaltigung***

– ***Brandstiftung***

– ***Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen***

– ***Flugzeug- und Schiffsentführung***

– ***Sabotage***

VERFAHREN DES FEDERFÜHRENDEN AUSSCHUSSES

|  |  |
| --- | --- |
| **Titel** | Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen |
| **Bezugsdokumente – Verfahrensnummer** | COM(2018)0225 – C8-0155/2018 – 2018/0108(COD) |
| **Datum der Übermittlung an das EP** | 17.4.2018 |  |  |  |
| **Federführender Ausschuss**       Datum der Bekanntgabe im Plenum | LIBE31.5.2018 |  |  |  |
| **Mitberatende Ausschüsse**       Datum der Bekanntgabe im Plenum | IMCO31.5.2018 |  |  |  |
| **Nicht abgegebene Stellungnahme(n)**       Datum des Beschlusses | IMCO16.5.2018 |  |  |  |
| **Berichterstatter**       Datum der Benennung | Birgit Sippel4.9.2019 |  |  |  |
| **Prüfung im Ausschuss** | 11.11.2019 | 28.1.2020 | 7.12.2020 |  |
| **Datum der Annahme** | 7.12.2020 |  |  |  |
| **Ergebnis der Schlussabstimmung** | +:–:0: | 35227 |
| **Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder** | Magdalena Adamowicz, Konstantinos Arvanitis, Malik Azmani, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Nicolaus Fest, Jean-Paul Garraud, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Sophia in ‘t Veld, Patryk Jaki, Lívia Járóka, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Nuno Melo, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Jadwiga Wiśniewska, Javier Zarzalejos |
| **Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter** | Delara Burkhardt, Andor Deli, Leopoldo López Gil, Kostas Papadakis, Anne-Sophie Pelletier, Rob Rooken, Domènec Ruiz Devesa, Hilde Vautmans, Petar Vitanov |
| **Datum der Einreichung** | 11.12.2020 |

NAMENTLICHE SCHLUSSABSTIMMUNG IM FEDERFÜHRENDEN AUSSCHUSS

|  |  |
| --- | --- |
| 35 | + |
| PPE | Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Andrzej Halicki, Jeroen Lenaers, Leopoldo López Gil, Nuno Melo, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Tomas Tobé, Javier Zarzalejos |
| S&D | Katarina Barley, Pietro Bartolo, Delara Burkhardt, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Łukasz Kohut, Juan Fernando López Aguilar, Javier Moreno Sánchez, Domènec Ruiz Devesa, Birgit Sippel, Petar Vitanov, Bettina Vollath,  |
| GUE/NGL | Konstantinos Arvanitis, Pernando Barrena Arza, Cornelia Ernst, Anne-Sophie Pelletier |
| NI | Milan Uhrík |

|  |  |
| --- | --- |
| 22 | - |
| PPE | Andor Deli, Lívia Járóka |
| Renew | Malik Azmani, Anna Júlia Donáth, Sophia in ‘t Veld, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu, Hilde Vautmans |
| Verts/ALE | Patrick Breyer, Saskia Bricmont, Damien Carême, Alice Kuhnke, Tineke Strik |
| ECR | Jorge Buxadé Villalba, Patryk Jaki, Nicola Procaccini, Rob Rooken  |
| NI | Kostas Papadakis, Martin Sonneborn |

|  |  |
| --- | --- |
| 7 | 0 |
| ID | Nicolas Bay, Nicolaus Fest, Jean-Paul Garraud, Peter Kofod, Annalisa Tardino, Tom Vandendriessche |
| ECR | Assita Kanko |

Erklärung der benutzten Zeichen:

+ : dafür

– : dagegen

0 : Enthaltung

1. \* Textänderungen: Der neue bzw. geänderte Text wird durch Fett- und Kursivdruck gekennzeichnet; Streichungen werden durch das Symbol ▌gekennzeichnet. [↑](#footnote-ref-1)
2. ABl. C … vom …, S. … [↑](#footnote-ref-2)
3. ***Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen, ABl. L 130 vom 1.5.2014, S. 1.*** [↑](#footnote-ref-3)
4. ***Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).*** [↑](#footnote-ref-4)
5. ***Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der*** ***Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).*** [↑](#footnote-ref-5)
6. ***Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).*** [↑](#footnote-ref-6)
7. [Richtlinie 2010/64/EU](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32010L0064) des Europäischen Parlaments und des Rates vom 20. Oktober 2010 über das Recht auf Dolmetschleistungen und Übersetzungen in Strafverfahren (ABl. L 280 vom 26.10.2010, S. 1). [↑](#footnote-ref-7)
8. [Richtlinie 2012/13/EU](http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32012L0013) des Europäischen Parlaments und des Rates vom 22. Mai 2012 über das Recht auf Belehrung und Unterrichtung in Strafverfahren (ABl. L 142 vom 1.6.2012, S. 1). [↑](#footnote-ref-8)
9. [Richtlinie 2013/48/EU](http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32013L0048) des Europäischen Parlaments und des Rates vom 22. Oktober 2013 über das Recht auf Zugang zu einem Rechtsbeistand in Strafverfahren und in Verfahren zur Vollstreckung des Europäischen Haftbefehls sowie über das Recht auf Benachrichtigung eines Dritten bei Freiheitsentzug und das Recht auf Kommunikation mit Dritten und mit Konsularbehörden während des Freiheitsentzugs (ABl. L 294 vom 6.11.2013, S. 1). [↑](#footnote-ref-9)
10. [Richtlinie (EU) 2016/343](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016L0343) des Europäischen Parlaments und des Rates vom 9. März 2016 über die Stärkung bestimmter Aspekte der Unschuldsvermutung und des Rechts auf Anwesenheit in der Verhandlung in Strafverfahren (ABl. L 65 vom 11.3.2016, S. 1). [↑](#footnote-ref-10)
11. [Richtlinie (EU) 2016/800](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016L0800) des Europäischen Parlaments und des Rates vom 11. Mai 2016 über Verfahrensgarantien in Strafverfahren für Kinder, die Verdächtige oder beschuldigte Personen in Strafverfahren sind (ABl. L 132 vom 21.5.2016, S. 1). [↑](#footnote-ref-11)
12. [Richtlinie (EU) 2016/1919](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016L1919) des Europäischen Parlaments und des Rates vom 26. Oktober 2016 über Prozesskostenhilfe für Verdächtige und beschuldigte Personen in Strafverfahren sowie für gesuchte Personen in Verfahren zur Vollstreckung eines Europäischen Haftbefehls (ABl. L 297 vom 4.11.2016, S. 1). [↑](#footnote-ref-12)
13. ***Rahmenbeschluss 2009/948/JI des Rates vom 30. November 2009 zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren (ABl. L 328 vom 15.12.2009, S. 42).*** [↑](#footnote-ref-13)
14. ***. Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) (ABl. L 321 vom 17.12.2018, S. 36).*** [↑](#footnote-ref-14)
15. . ***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).*** [↑](#footnote-ref-15)
16. ***. Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. L 335 vom 17.12.2011, S. 1).*** [↑](#footnote-ref-16)
17. ***Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).*** [↑](#footnote-ref-17)
18. . ***Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).*** [↑](#footnote-ref-18)
19. ***. Stellungnahme 7/2019 des Europäischen Datenschutzbeauftragten zu den Vorschlägen über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (6. November 2019).*** [↑](#footnote-ref-19)
20. [Richtlinie (EU) 2015/1535](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32015L1535) 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). [↑](#footnote-ref-20)
21. [Richtlinie 2013/40/EU](https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32013L0040) des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8). [↑](#footnote-ref-21)
22. Beschluss 2008/976/JI des Rates vom 16. Dezember 2008 über das Europäische Justizielle Netz (ABl. L 348 vom 24.12.2008, S. 130). [↑](#footnote-ref-22)