Bundesrat **Drucksache 215/18**
24.05.18

EU - In - R - Wi

Unterrichtung
durch die Europäische Kommission

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

COM(2018) 225 final

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

Der Bundesrat wird über die Vorlage gemäß § 2 EUZBLG auch durch die Bundesregierung unterrichtet.
Der Europäische Wirtschafts- und Sozialausschuss wird an den Beratungen beteiligt.

EUROPÄISCHE
KOMMISSION

Straßburg, den 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen

{SWD(2018) 118 final} - {SWD(2018) 119 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Die Nutzung sozialer Medien, von Webmail, Nachrichtendiensten und Anwendungen („Apps“), um zu kommunizieren, zu arbeiten, Sozialkontakte zu pflegen und sich zu informieren, ist heute in vielen Teilen der Welt längst gang und gäbe. Diese Dienste verbinden mehrere hundert Millionen Nutzerinnen und Nutzer miteinander. Den Nutzern beschert dies innerhalb und außerhalb der Union für ihr wirtschaftliches und soziales Wohlergehen beträchtliche Vorteile. Kommunikationsmittel können jedoch auch missbraucht werden, um Straftaten zu begehen oder ihnen Vorschub zu leisten – darunter auch terroristische Anschläge. Wenn dies geschieht, dann sind diese Dienste und Apps häufig der einzige Ort, an dem die Ermittler Hinweise auf den Urheber einer Straftat finden und vor Gericht verwendbare Beweismittel einholen können.

Das Internet kennt keine Grenzen. Daher können derartige Dienste überall in der Welt bereitgestellt werden und erfordern nicht notwendigerweise eine physische Infrastruktur, eine Firmenpräsenz oder Mitarbeiter in den Mitgliedstaaten, in denen sie angeboten werden, oder am Binnenmarkt insgesamt. Daher bedarf es auch keines bestimmten Ortes für die Datenspeicherung, der vom Diensteanbieter oft auf Basis legitimer Erwägungen zur Datensicherheit, zu größenbedingten Kostenvorteilen und schnellem Zugang ausgewählt wird. Folglich ersuchen die Behörden der Mitgliedstaaten bei immer mehr Straftaten aller Art[1] um Zugang zu Daten, die als Beweismittel dienen könnten und die außerhalb des jeweiligen Mitgliedstaats und/oder von Diensteanbietern in anderen Mitgliedstaaten oder Drittstaaten gespeichert sind.

In Fällen, in denen sich entweder die Beweismittel andernorts befinden oder der Diensteanbieter andernorts ansässig ist, wurden bereits vor einigen Jahrzehnten Verfahren für die Zusammenarbeit zwischen den Ländern entwickelt.[2] Trotz regelmäßiger Reformen geraten diese Kooperationsverfahren immer stärker unter Druck, denn es gibt immer mehr Bedarf an raschem grenzüberschreitendem Zugang zu elektronischen Beweismitteln. Als Reaktion darauf bauen eine Reihe von Mitgliedstaaten und Drittstaaten ihre nationalen Instrumente aus. Die daraus resultierende Zersplitterung führt zu Rechtsunsicherheit und einander widersprechenden Verpflichtungen. Sie wirft Fragen über den Schutz der Grundrechte und Verfahrensgarantien für Menschen auf, die von solchen Ersuchen betroffen sind.

Der Rat forderte im Jahr 2016 konkrete Maßnahmen auf Grundlage eines gemeinsamen EU-Konzepts, um die Rechtshilfe effizienter zu gestalten, um die Zusammenarbeit zwischen den Behörden der Mitgliedstaaten und Diensteanbietern in Drittstaaten zu verbessern und um Lösungen in Zusammenhang mit der Bestimmung der Zuständigkeit für Ermittlungsmaßnahmen im Cyberspace und mit der entsprechenden Verfolgungszuständigkeit[3] vorzuschlagen.[4] Auch das Europäische Parlament wies darauf hin,

---

1 Siehe die Abschnitte 2.1.1 und 2.3 der Folgenabschätzung.

2 In der Union sind das Mechanismen zur gegenseitigen Anerkennung, die gegenwärtig auf der Richtlinie über die Europäische Ermittlungsanordnung basieren; in Drittstaaten handelt es sich um Rechtshilfemechanismen.

3 Im vorliegenden Dokument verweist der Begriff „Verfolgungszuständigkeit“ auf die Befugnis der zuständigen Behörden, eine Ermittlungsmaßnahme durchzuführen.

dass die derzeit fragmentierten rechtlichen Rahmenbedingungen ein Problem für Diensteanbieter sein können, die den Ersuchen von Strafverfolgungsbehörden Folge leisten wollen, und forderte einen europäischen Rechtsrahmen, der Garantien hinsichtlich der Rechte und Freiheiten aller Betroffenen umfasst.[5]

Der vorliegende Vorschlag nimmt das spezifische Problem ins Visier, das durch die Volatilität elektronischer Beweismittel und die internationale Dimension entsteht. Er zielt darauf ab, Kooperationsverfahren an das digitale Zeitalter anzupassen, der Justiz und der Strafverfolgung Instrumente für den Umgang mit den heutigen Kommunikationsmethoden von Straftätern an die Hand zu geben und gegen moderne Formen der Kriminalität vorzugehen. Voraussetzung für den Einsatz derartiger Instrumente ist, dass sie strengen Schutzmechanismen für die Grundrechte unterliegen. Mit diesem Vorschlag soll die Rechtssicherheit für Behörden, Diensteanbieter und betroffene Menschen verbessert und zugleich dafür gesorgt werden, dass Ersuchen von Strafverfolgungsbehörden weiterhin hohen Standards genügen und somit der Schutz der Grundrechte, Transparenz und Rechenschaftspflicht gewährleistet werden. Außerdem wird dadurch das Verfahren zur Sicherung und Einholung elektronischer Beweismittel beschleunigt, die in einem anderen Staat gespeichert wurden und/oder über die in einem anderen Staat niedergelassene Diensteanbieter verfügen. Dieses Instrument wird neben den derzeitigen Instrumenten zur justiziellen Zusammenarbeit bestehen, die weiterhin relevant sind, und kann nach Bedarf von den zuständigen Behörden eingesetzt werden. Parallel dazu arbeitet die Kommission daran, die bestehenden Verfahren zur justiziellen Zusammenarbeit durch bestimmte Maßnahmen zu stärken, etwa die Schaffung einer sicheren Plattform für den schnellen Austausch von Ersuchen zwischen Justizbehörden in der EU und die Investition von 1 Mio. EUR in die Rechtshilfe- und Kooperationsschulung von Praktikern aus allen EU-Mitgliedstaaten – wobei der Fokus auf den Vereinigten Staaten als dem Drittstaat liegt, bei dem die meisten Ersuchen aus der EU eingehen[6].

Zur Zustellung und Ausführung von Anordnungen im Rahmen dieses Instruments sollten die Behörden auf einen Vertreter zurückgreifen, der von den Diensteanbietern benannt wurde. Die Kommission legt heute einen Vorschlag vor, um sicherzustellen, dass diese Vertreter tatsächlich benannt werden. Der Vorschlag bietet eine gemeinsame, EU-weite Lösung, um mittels eines Vertreters gesetzmäßige Anordnungen an Diensteanbieter zu richten.

- **Kohärenz mit dem bestehenden EU-Rechtsrahmen in diesem Bereich und dem Budapester Übereinkommen des Europarats**

Der derzeitige EU-Rechtsrahmen besteht aus Instrumenten der Union für die Zusammenarbeit in Strafsachen wie der Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen[7] (EEA-Richtlinie), dem Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union[8], dem Beschluss 2002/187/JI des Rates

---

4 Schlussfolgerungen des Rates der Europäischen Union vom 9. Juni 2016 zur Verbesserung der Strafjustiz im Cyberspace, ST9579/16.

5 P8_TA(2017)0366.

6 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

7 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).

8 Rechtsakt des Rates vom 29. Mai 2000 über die Erstellung des Übereinkommens – gemäß Artikel 34 des Vertrags über die Europäische Union – über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union.

über die Errichtung von Eurojust[9], der Verordnung (EU) 2016/794 über Europol[10], dem Rahmenbeschluss 2002/465/JI des Rates über gemeinsame Ermittlungsgruppen[11] sowie aus bilateralen Abkommen zwischen der Union und Drittstaaten wie dem Abkommen zwischen der EU und den Vereinigten Staaten von Amerika über Rechtshilfe[12] und dem Abkommen zwischen der EU und Japan über Rechtshilfe[13].

Die Einführung Europäischer Herausgabeanordnungen und Europäischer Sicherungsanordnungen durch den Vorschlag macht es leichter, elektronische Beweismittel für Strafverfahren zu sichern und zu erheben, die von Diensteanbietern in einem anderen Staat gespeichert wurden oder über die diese verfügen. Die EEA-Richtlinie, die zu großen Teilen das Übereinkommen über die Rechtshilfe in Strafsachen ersetzt hat, deckt jede Ermittlungsmaßnahme ab[14]. Dies schließt den Zugang zu elektronischen Beweismitteln mit ein, jedoch enthält die EEA-Richtlinie keine besonderen Bestimmungen über diese Art von Beweismitteln[15]. Das neue Instrument wird die Europäische Ermittlungsanordnung (EEA) für das Einholen von Beweismitteln nicht ersetzen, gibt den Behörden aber ein zusätzliches Werkzeug an die Hand. Möglicherweise ergeben sich Situationen – beispielsweise wenn mehrere Ermittlungsmaßnahmen im vollstreckenden Mitgliedstaat durchgeführt werden müssen –, in denen die EEA für die Behörden die bevorzugte Option sein könnte. Ein neues Instrument für elektronische Beweismittel zu schaffen, ist eine bessere Alternative als die Änderung der EEA-Richtlinie, da mit dem Einholen elektronischer Beweismittel bestimmte Herausforderungen einhergehen, die bei den anderen unter die EEA-Richtlinie fallenden Ermittlungsmaßnahmen nicht bestehen.

Um das grenzüberschreitende Erheben elektronischer Beweismittel zu erleichtern, basiert das neue Instrument auf den Grundsätzen der gegenseitigen Anerkennung. Eine Behörde in dem Land, in dem der Adressat der Anordnung ansässig ist, muss nicht direkt in die Zustellung und Ausführung der Anordnung involviert sein, außer in Fällen von Nichteinhaltung: Dann ist Vollstreckung gefragt, und die zuständige Behörde in dem Land, in dem der Vertreter ansässig ist, wird tätig werden. Deshalb bedarf das Instrument robuster Garantien und Bestimmungen wie der Validierung durch eine Justizbehörde in jedem einzelnen Fall. So dürfen beispielsweise Europäische Herausgabeanordnungen zur Herausgabe von

---

9 Beschluss 2002/187/JI des Rates vom 28. Februar 2002 über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität. Im Jahr 2013 nahm die Kommission einen Vorschlag für eine Verordnung zur Reform von Eurojust an (Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates betreffend die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) (COM/2013/0535 final)).

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

11 Rahmenbeschluss 2002/465/JI des Rates vom 13. Juni 2002 über gemeinsame Ermittlungsgruppen.

12 Beschluss 2009/820/GASP des Rates vom 23. Oktober 2009 über den Abschluss im Namen der Europäischen Union des Abkommens über Auslieferung zwischen der Europäischen Union und den Vereinigten Staaten von Amerika und des Abkommens über Rechtshilfe zwischen der Europäischen Union und den Vereinigten Staaten von Amerika.

13 Beschluss 2010/616/EU des Rates vom 7. Oktober 2010 über den Abschluss des Abkommens zwischen der Europäischen Union und Japan über die Rechtshilfe in Strafsachen.

14 Mit Ausnahme der gemeinsamen Ermittlungsgruppen (siehe Artikel 3 der EEA-Richtlinie); nicht alle Mitgliedstaaten beteiligen sich an der EEA-Richtlinie (Irland, Dänemark).

15 Mit Ausnahme eines Verweises auf die Identifizierung eines Inhabers einer IP-Adresse in Artikel 10 Absatz 2 Buchstabe e, hier kann die beiderseitige Strafbarkeit nicht als Versagungsgrund für die Anerkennung oder Ausführung des Ersuchens herangezogen werden.

Transaktions- oder Inhaltsdaten (im Gegensatz zu Teilnehmer- und Zugangsdaten) nur erlassen werden, wenn Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden, vorliegen, oder aber bestimmte Straftaten, die mit dem Cyberspace zusammenhängen oder durch den Cyberspace möglich gemacht wurden oder in Zusammenhang mit Terrorismus stehen, wie dies im Vorschlag vorgesehen ist.

Die unter diesen Vorschlag fallenden personenbezogenen Daten sind geschützt und dürfen nur gemäß der Datenschutz-Grundverordnung[16] und der Richtlinie für den Datenschutz bei Polizei und Strafjustiz[17] verarbeitet werden. Die Datenschutz-Grundverordnung tritt am 25. Mai 2018 in Kraft, während die Richtlinie für den Datenschutz bei Polizei und Strafjustiz von den Mitgliedstaaten bis zum 6. Mai 2018 umgesetzt werden musste.

Das Budapester Übereinkommen des Europarats über Computerqualität (SEV Nr. 185), das von den meisten EU-Mitgliedstaaten ratifiziert wurde, legt internationale Kooperationsverfahren zur Bekämpfung der Cyberkriminalität fest.[18] Das Übereinkommen befasst sich mit Straftaten, die über das Internet und andere Computernetze verübt wurden. Zugleich verpflichtet es die Vertragsparteien, Befugnisse und Verfahren festzulegen, um elektronische Beweismittel einzuholen und gegenseitig Rechtshilfe zu leisten; dies ist nicht auf Cyberkriminalität beschränkt. Insbesondere sind die Vertragsparteien nach dem Übereinkommen verpflichtet, Herausgabeanordnungen einzuführen, um Computerdaten von Diensteanbietern in ihrem Hoheitsgebiet und Teilnehmerdaten von Diensteanbietern, die ihre Dienste in ihrem Hoheitsgebiet anbieten, einzuholen. Darüber hinaus sieht das Abkommen Sicherungsanordnungen vor, sofern Anlass zu der Annahme besteht, dass die Computerdaten besonders verlust- oder änderungsgefährdet sind. Die Zustellung und die Vollstreckbarkeit nationaler Herausgabeanordnungen bei Anbietern, die außerhalb des Hoheitsgebiets einer Vertragspartei des Übereinkommens niedergelassen sind, werfen weitere Fragen auf. In diesem Zusammenhang werden derzeit weitere Maßnahmen zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln in Betracht gezogen[19].

- **Zusammenfassung der vorgeschlagenen Verordnung**

Die vorgeschlagene Verordnung führt bindende Europäische Herausgabeanordnungen und Sicherungsanordnungen ein. Beide Anordnungen müssen von einer Justizbehörde eines

---

16 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.

17 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.

18 In der Cybersicherheitsstrategie der Europäischen Union aus dem Jahr 2013 wurde das Übereinkommen von Budapest als der zentrale multilaterale Rahmen für den Kampf gegen Cyberkriminalität anerkannt: Gemeinsame Mitteilung der Kommission und der Hohen Vertreterin der Europäischen Union über eine Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum, JOIN(2013) 1 final.

19 Bei seinem 17. Plenum (Juni 2017) übernahm der Ausschuss für das Übereinkommen über Computerkriminalität (T-CY) das Mandat für die Vorbereitung eines zweiten Zusatzprotokoll zum Übereinkommen (im Folgenden „zweites Zusatzprotokoll“), das vom Ausschuss bis Dezember 2019 vorzubereiten und abzuschließen ist. Ziel ist es, den Datenspeicherort nicht mehr als einen entscheidenden Faktor zu betrachten.

Mitgliedstaats erlassen oder validiert werden. Eine Anordnung kann zur Sicherung und Herausgabe von Daten erlassen werden, die von einem Diensteanbieter in einem anderen Staat gespeichert wurden und die als Beweismittel in strafrechtlichen Ermittlungen oder Strafverfahren erforderlich sind. Derartige Anordnungen dürfen nur erlassen werden, wenn in einer vergleichbaren innerstaatlichen Situation im Anordnungsstaat eine ähnliche Maßnahme für dieselbe Straftat zur Verfügung steht. Beide Anordnungen können Anbietern elektronischer Kommunikationsdienste, sozialer Netzwerke oder von Online-Marktplätzen, Anbietern anderer Hosting-Dienste und Anbietern von Internetinfrastruktur wie Registern von IP-Adressen und Domänennamen oder – wo es diese gibt – ihren Vertretern zugestellt werden. Die Europäische Sicherungsanordnung richtet sich – analog der Europäischen Herausgabeanordnung – an den Vertreter außerhalb des Rechtssystems des Anordnungsmitgliedstaats, um die Daten mit Blick auf ein späteres Ersuchen zur Herausgabe dieser Daten zu sichern, beispielsweise im Fall von Drittstaaten über Rechtshilfekanäle oder zwischen beteiligten Mitgliedstaaten über eine EEA. Anders als Überwachungsmaßnahmen oder gesetzlich festgelegte Verpflichtungen zur Vorratsdatenspeicherung, die nicht in dieser Verordnung vorgesehen sind, ist die Europäische Sicherungsanordnung eine Anordnung, die von einer Justizbehörde im Rahmen eines konkreten Strafverfahrens erlassen oder validiert wird, nachdem die Verhältnismäßigkeit und Notwendigkeit im Einzelfall geprüft wurde. Wie die Europäische Herausgabeanordnung bezieht sie sich auf bestimmte bekannte oder unbekannte Urheber einer Straftat, die bereits begangen wurde. Die Europäische Sicherungsanordnung erlaubt nur die Sicherung von Daten, die zum Zeitpunkt der Entgegennahme der Anordnung bereits gespeichert waren, und nicht den Zugang zu Daten zu einem späteren Zeitpunkt nach Entgegennahme der Europäischen Sicherungsanordnung.

Beide Anordnungen können ausschließlich in Strafverfahren verwendet werden – vom anfänglichen vorgerichtlichen Ermittlungsstadium bis zum Abschluss des Verfahrens durch ein Urteil oder eine andere Entscheidung. Die Anordnungen zur Herausgabe von Teilnehmer- und Zugangsdaten können für jede Art von Straftaten erlassen werden, während die Anordnung zur Herausgabe von Transaktions- und Inhaltsdaten nur für Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden, oder für bestimmte im Vorschlag angeführte Straftaten erlassen werden darf, bei denen eine bestimmte Verbindung zu elektronischen Tools und Straftaten besteht, die unter die Richtlinie (EU) 2017/541 zur Terrorismusbekämpfung fallen.

In Anbetracht der unterschiedlich starken Eingriffe im Verhältnis zu den erstrebten Daten werden in dem Vorschlag eine Reihe von Voraussetzungen und Garantien festgelegt. Dazu gehört die Verpflichtung, eine Ex-ante-Validierung der Anordnungen durch eine Justizbehörde zu erwirken. Der Vorschlag gilt nur für gespeicherte Daten. Die Echtzeit-Überwachung des Telekommunikationsverkehrs fällt nicht unter diesen Vorschlag. Die Maßnahme ist auf das beschränkt, was für die Zwecke relevanter Strafverfahren notwendig und verhältnismäßig ist. Sie ermöglicht es Diensteanbietern, von den Anordnungsbehörden bei Bedarf Erläuterungen einzuholen. Wenn diese Fragen nicht geklärt werden können und die Anordnungsbehörde beschließt, die Vollstreckung zu betreiben, können Diensteanbieter aus denselben Gründen die Vollstreckung durch die eigenen Behörden ablehnen. Zudem wird ein spezifisches Verfahren für Fälle eingerichtet, in denen die Pflicht zur Bereitstellung von Daten mit einer Verpflichtung kollidiert, die aus dem Recht eines Drittstaats erwächst.

Die Rechtsvorschriften der EU schützen die Rechte von Verdächtigen und Beschuldigten in Strafverfahren, auch gibt es schon Regelungen zum Schutz personenbezogener Daten. Für die Personen jedoch, um deren Daten ersucht wird, sehen diese im Vorschlag enthaltenen zusätzlichen Garantien Verfahrensrechte im Zuge oder außerhalb von Strafverfahren vor.

Dazu gehört die Möglichkeit, die Rechtmäßigkeit, Notwendigkeit oder Verhältnismäßigkeit der Anordnung anzufechten, ohne die Gründe für die Anfechtung gemäß nationalem Recht einzuschränken. Die nach dem Recht des Vollstreckungsstaats bestehenden Rechte werden vollständig durch die Gewährleistung gewahrt, dass den Immunitäten und Vorrechten, die die im Mitgliedstaat des Diensteanbieters angeforderten Daten schützen, im Anwendungsstaat Rechnung getragen wird. Das gilt insbesondere dann, wenn sie einen stärkeren Schutz gewähren als das Recht des Anordnungsstaats.

Die Anordnungen nach der vorgeschlagenen Verordnung sind in der gleichen Weise vollstreckbar wie vergleichbare innerstaatliche Anordnungen in dem Staat, in dem der Diensteanbieter die Anordnung entgegennimmt. In der Verordnung ist vorgesehen, dass die Mitgliedstaaten über wirksame und angemessene Sanktionen verfügen sollten.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄSSIGKEIT

- **Rechtsgrundlage**

Die Rechtsgrundlage für die Unterstützung von Maßnahmen in diesem Bereich ist Artikel 82 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Nach Artikel 82 Absatz 1 können Maßnahmen gemäß dem ordentlichen Gesetzgebungsverfahren erlassen werden, um Regeln und Verfahren festzulegen, mit denen die Anerkennung aller Arten von Urteilen und gerichtlichen Entscheidungen in der gesamten Union sichergestellt wird. Maßnahmen können auch erlassen werden, um die Zusammenarbeit zwischen den Justizbehörden oder entsprechenden Behörden der Mitgliedstaaten im Rahmen der Strafverfolgung sowie des Vollzugs und der Vollstreckung von Entscheidungen zu erleichtern.

Diese Rechtsgrundlage gilt für die Verfahren, die unter diese Verordnung fallen. Artikel 82 Absatz 1 gewährleistet die gegenseitige Anerkennung gerichtlicher Entscheidungen, die durch eine Justizbehörde im Anordnungsstaat an eine juristische Person in einem anderen Mitgliedstaat ergeht und mit der ihr sogar Verpflichtungen auferlegt werden können, ohne dass eine Justizbehörde in diesem anderen Mitgliedstaat vorher tätig geworden wäre. Die Europäische Herausgabeanordnung oder Sicherungsanordnung können zum Tätigwerden einer Justizbehörde des Vollstreckungsstaats führen, wenn dies zur Vollstreckung der Entscheidung notwendig ist.

- **Wahl des Instruments**

Artikel 82 Absatz 1 AEUV gibt dem Gesetzgeber der Union die Möglichkeit, Verordnungen und Richtlinien zu erlassen.

Da der Vorschlag grenzüberschreitende Verfahren betrifft, bei denen einheitliche Regeln notwendig sind, besteht keine Notwendigkeit, den Mitgliedstaaten einen Ermessensspielraum für die Umsetzung dieser Regeln zu lassen. Eine Verordnung gilt unmittelbar und sorgt für Klarheit und mehr Rechtssicherheit, zudem werden durch eine Verordnung die unterschiedliche Auslegung durch die Mitgliedstaaten und andere Umsetzungsprobleme vermieden, die in Zusammenhang mit den Rahmenbeschlüssen über die gegenseitige Anerkennung von Urteilen und gerichtlichen Entscheidungen aufgetreten sind. Darüber hinaus gestattet eine Verordnung, dieselbe Verpflichtung in der Union einheitlich aufzuerlegen. Aus diesen Gründen wird eine Verordnung als die am besten geeignete Form für dieses Instrument für die gegenseitige Anerkennung erachtet.

- **Subsidiarität**

Angesicht der grenzüberschreitenden Dimension der hier behandelten Probleme müssen die in den Vorschlag aufgenommenen Maßnahmen auf Unionsebene erlassen werden, um die Ziele zu erreichen. Bei den Straftaten, für die es elektronische Beweismittel gibt, kommt es häufig vor, dass die Infrastruktur, in der die elektronischen Beweismittel gespeichert sind, und der Diensteanbieter, der die Infrastruktur betreibt, unter einen anderen nationalen Rechtsrahmen innerhalb oder außerhalb der Union fallen als das Opfer oder der Straftäter. In der Folge kann es für das zuständige Land sehr zeitaufwendig und schwierig werden, sich ohne gemeinsame Mindestvorschriften über Grenzen hinweg Zugang zu elektronischen Beweismitteln zu verschaffen. Mitgliedstaaten, die allein handeln, stünden dann bei folgenden Aspekten vor Problemen:

- der Zersplitterung der mitgliedstaatlichen Rechtsrahmen. Dies wird von Diensteanbietern, die auf unterschiedlichen nationalen Rechtsvorschriften basierenden Ersuchen Folge leisten wollen, als besonders große Herausforderung angesehen;
- einer zweckmäßigeren justiziellen Zusammenarbeit auf Grundlage des geltenden Unionsrechts, vor allem mittels der EEA.

Angesichts der verschiedenartigen Rechtsordnungen, der Zahl der betroffenen Politikbereiche (Sicherheit, Grundrechte einschließlich der Verfahrensrechte und des Schutzes personenbezogener Daten, Wirtschaftsangelegenheiten) und des breiten Spektrums von Interessenträgern sind Rechtsvorschriften auf Unionsebene das am besten geeignete Mittel, um die Schwierigkeiten anzugehen.

- **Verhältnismäßigkeit**

Mit dem Vorschlag werden die Regeln festgelegt, nach denen eine zuständige Behörde in der Union einen Diensteanbieter, der in der Union Dienstleistungen anbietet und nicht im selben Mitgliedstaat ansässig ist, anweisen kann, elektronische Beweismittel herauszugeben oder zu sichern. Zentrale Aspekte des Vorschlags wie etwa der sachliche Anwendungsbereich der Europäischen Herausgabeanordnung, die Voraussetzungen zur Gewährleistung entgegenkommenden Verhaltens, der Sanktionsmechanismus und das System von Garantien und Rechtsbehelfen beschränken den Vorschlag auf das, was zum Erreichen der wichtigsten Ziele notwendig ist. Der Vorschlag ist insbesondere auf Ersuchen um gespeicherte Daten (Daten aus der Echtzeit-Überwachung des Telekommunikationsverkehrs gehören nicht dazu) und auf Anordnungen im Zuge von Strafverfahren begrenzt, bei denen es um Ermittlungen in einer bestimmten Straftat geht. Die Verhütung von Straftaten oder andere Arten von Verfahren oder Verstößen (wie etwa Verwaltungsverfahren wegen Zuwiderhandlung gegen Rechtsvorschriften) fallen nicht unter diesen Vorschlag. Der Vorschlag verpflichtet Anbieter auch nicht, systematisch mehr Daten zu sammeln oder zu speichern als aus geschäftlichen Gründen oder zur Einhaltung anderer rechtlicher Verpflichtungen notwendig. Darüber hinaus kann die Anordnung zur Herausgabe von Transaktions- und Inhaltsdaten nur für Straftaten erlassen werden, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden, oder für bestimmte im Vorschlag definierte Straftaten, die mit dem Cyberspace zusammenhängen oder durch den Cyberspace ermöglicht wurden, sowie für Straftaten mit einem terroristischen Hintergrund. Anordnungen zur Herausgabe von Teilnehmer- und Zugangsdaten können unterdessen für jede Art von Straftat erlassen werden. Schließlich werden mit dem Vorschlag noch die beim grenzüberschreitenden Zugang zu elektronischen Beweismitteln geltenden Verfahrensvorschriften und Garantien

geklärt; der Vorschlag geht jedoch nicht so weit, innerstaatliche Maßnahmen zu harmonisieren. Er bleibt auf das beschränkt, was notwendig und verhältnismäßig ist, um den Bedürfnissen der Strafverfolgungs- und Justizbehörden im digitalen Zeitalter Rechnung zu tragen.

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

• Konsultation der Interessenträger

Die Kommission hat rund anderthalb Jahre lang alle einschlägigen Interessenträger konsultiert, um Probleme zu ermitteln und gangbare Wege aufzuzeigen. Dies geschah mittels Erhebungen, die von öffentlichen Konsultationen bis hin gezielten Umfragen bei den einschlägigen Behörden reichten. Zudem wurden Sitzungen von Sachverständigengruppen und bilaterale Treffen organisiert, um die potenziellen Auswirkungen von EU-Rechtsvorschriften zu diskutieren. Konferenzen zum grenzüberschreitenden Zugang zu elektronischen Beweismitteln dienten auch dazu, Feedback für die Initiative zu sammeln.

Insgesamt betrachteten die Umfrageteilnehmer die zunehmende Nutzung von Informationsdiensten als Herausforderung für die Strafverfolgung, da die zuständigen Behörden oft nur schlecht für den Umgang mit Online-Beweismitteln gerüstet sind. Auch wurde das langwierige Verfahren zum Einholen von Beweismitteln als eine der zentralen Hürden anerkannt. Als weitere entscheidende Themen führten die Behörden an, dass es an verlässlicher Zusammenarbeit mit den Diensteanbietern und Transparenz mangelt und dass Rechtsunsicherheit in Bezug auf die Zuständigkeit für Ermittlungsmaßnahmen herrscht. Eine direkte grenzüberschreitende Zusammenarbeit zwischen Strafverfolgungsbehörden und Anbietern digitaler Dienste wurde als Zusatznutzen bei strafrechtlichen Ermittlungen gewertet. Diensteanbieter und einige zivilgesellschaftliche Organisationen wiesen auf die Notwendigkeit hin, bei der Zusammenarbeit mit den Behörden Rechtssicherheit zu gewährleisten und Gesetzeskollisionen zu vermeiden. Im Hinblick auf Bedenken, wie sich neue EU-Rechtsvorschriften auf Rechte auswirken könnten, vertraten die Interessenträger die Auffassung, dass als notwendige Voraussetzung für ein grenzüberschreitendes Instrument bestimmte Garantien gegeben werden sollten.

Das Feedback aus der Folgenabschätzung in der Anfangsphase zeigte, dass die Interessenträger davon ausgehen, dass eine Behebung der Mängel des gegenwärtigen Rechtshilfesystems es wirksamer machen und die Rechtssicherheit verbessern würde. Einige zivilgesellschaftliche Organisationen sprachen sich gegen Rechtvorschriften auf EU-Ebene zur direkten Zusammenarbeit aus. Sie hätten EU-Maßnahmen bevorzugt, die sich auf verbesserte Rechtshilfeverfahren beschränken. Dieser Gedanke wird als Teil der vom Rat im Juni 2016 gebilligten praktischen Maßnahmen weiterverfolgt werden.

Durch eine gezielte Umfrage bei Behörden in den Mitgliedstaaten zeigte sich auch, dass es keinen gemeinsamen Ansatz gibt, um grenzüberschreitenden Zugang zu elektronischen Beweismitteln zu erlangen, da jeder Mitgliedstaat seine eigene Praxis hat. Diensteanbieter reagieren auch unterschiedlich auf Ersuchen ausländischer Strafverfolgungsbehörden; je nach ersuchendem Mitgliedstaat variiert die Reaktionszeit. Dies schafft für alle betroffenen Interessenträger Rechtsuntersicherheit.

Insgesamt ergab die Konsultation der Interessenträger, dass der gegenwärtige Rechtsrahmen zersplittert und komplex ist. Dies kann in der Ausführungsphase zu Verzögerungen und einer

wenig effektiven Ermittlung und Verfolgung von Straftaten führen, sofern dies mit dem grenzüberschreitenden Zugang zu elektronischen Beweismitteln einhergeht.

- **Folgenabschätzung**

Der Ausschuss für Regulierungskontrolle hat eine befürwortende Stellungnahme über die Folgenabschätzung abgegeben, die diesen Vorschlag unterstützt[20], und hat verschiedene Verbesserungsvorschläge unterbreitet[21]. Die Folgenabschätzung wurde infolge der Stellungnahme geändert, um weiter über Grundrechtefragen in Zusammenhang mit dem grenzüberschreitenden Datenaustausch zu beraten, insbesondere über die Verbindungen zwischen den verschiedenen Maßnahmen, die Bestandteil der bevorzugten Option sind. Die Bewertung wurde ebenfalls abgeändert, um den Sichtweisen der Interessenträger und Mitgliedstaaten und der Art und Weise, wie diese berücksichtigt werden, besser Rechnung zu tragen. Darüber hinaus wurde der politische Kontext überprüft, um zusätzliche Verweise auf verschiedene Aspekte aufzunehmen – beispielsweise auf die Beratungen in den Sachverständigengruppen, die zur Gestaltung der Initiative beigetragen haben. Die wechselseitige Ergänzung verschiedener Maßnahmen (insbesondere die EEA-Richtlinie, die Verhandlungen eines Zusatzprotokolls zum Budapester Übereinkommen und die gemeinsame Überprüfung des Rechtshilfeabkommens zwischen der EU und den USA) wurde präzisiert, was Anwendungsbereich, Zeitplan und Tiefe angeht. Zudem wurde das Basisszenario überprüft, um Entwicklungen besser zu berücksichtigen, die sich unabhängig von der Annahme der vorgeschlagenen Maßnahmen einstellen dürften. Und schließlich wurden Flussdiagramme hinzugefügt, um den Arbeitsablauf beim Datenaustausch besser darzustellen.

Abgesehen vom Basisszenario (Option O) wurden vier zentrale politische Optionen erwogen: eine Reihe praktischer Maßnahmen, um sowohl die Verfahren bei der justiziellen Zusammenarbeit und die direkte Zusammenarbeit zwischen Behörden und Diensteanbietern zu verbessern (Option A: nichtlegislativ); eine Option, die die praktischen Maßnahmen von Option A mit internationalen Lösungsansätzen auf bilateraler oder multilateraler Ebene kombiniert (Option B: legislativ); eine Option, die die vorhergehenden in Option B enthaltenen Maßnahmen mit einer Europäischen Herausgabeanordnung und einer Maßnahme für besseren Zugang zu Datenbanken kombiniert, die auf Abfragebasis Teilnehmerinformationen liefern, wie etwa die Whois-Abfrage für Domänennamen (Option C: legislativ) und eine Option, die alle vorhergehenden in Option C enthaltenen Maßnahmen mit Gesetzgebung zum direkten Zugang zu extern gespeicherten Daten kombiniert (Option D: legislativ)[22].

---

20 Arbeitsunterlage der Kommissionsdienststellen – Folgenabschätzung zum Vorschlag für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und den Vorschlag für eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren, SWD(2018) 118.

21 Europäische Kommission – Stellungnahme des Ausschusses für Regulierungskontrolle zur Folgenabschätzung – Vorschlag für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und Vorschlag für eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren, SWD(2018) 199.

22 Für Einzelheiten: Arbeitsunterlage der Kommissionsdienststellen – Folgenabschätzung zum Vorschlag für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und den Vorschlag für eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren, SWD(2018) 118.

Werden keine Maßnahmen ergriffen (Option O), wird eine wachsende Zahl von Ersuchen die Situation verschlechtern. Alle anderen Optionen tragen dazu bei, die Ziele der Initiative zu erreichen – allerdings in unterschiedlichem Maße. Option A würde die Effizienz der gegenwärtigen Verfahren erhöhen, beispielsweise durch eine verbesserte Qualität der Ersuchen. Allerdings wäre der Spielraum für Verbesserungen wegen der strukturellen Mängel des derzeitigen Systems eingeschränkt.

Option B würde durch international akzeptierte Lösungsansätze mehr Verbesserungen bewirken, allerdings würde es zum großen Teil von Drittstaaten abhängen, welche Ergebnisse diese internationalen Ansätze zeitigen können. Die Lösungen sind deshalb unsicher, und es ist unwahrscheinlich, dass sie so wirksam wären und so viele Garantien bieten würden wie eine Lösung auf Unionsebene.

Option C würde verglichen mit den vorangegangenen Optionen klar Mehrwert liefern, da hier auch ein EU-internes Instrument zur direkten Zusammenarbeit mit Diensteanbietern vorgesehen ist. Dadurch ließen sich die meisten der identifizierten Probleme lösen, wenn ein Diensteanbieter im Besitz der betreffenden Daten ist.

Option D liefert das umfassendste Lösungspaket. Zusätzlich zu den vorhergehenden Maßnahmen umfasst sie eine legislative Maßnahme für den direkten Zugang in Situationen, in denen die Beteiligung eines Diensteanbieters nicht notwendig ist.

Die vorliegende von der Kommission vorgeschlagene Legislativinitiative fußt auf den Ergebnissen der Folgenabschätzung. Diese Gesetzgebung wird wie in der Folgenabschätzung beschrieben durch die praktischen Maßnahmen und durch die weitere Arbeit an einem Zusatzprotokoll zum Budapester Übereinkommen ergänzt. Auf Basis ihres Legislativvorschlags wird die Kommission auch mit den Vereinigten Staaten und anderen Drittstaaten über die Möglichkeit künftiger bilateraler oder multilateraler Übereinkommen zum grenzüberschreitenden Zugang zu elektronischen Beweismitteln mit begleitenden Garantien beraten. Für Maßnahmen zum direkten Zugang und zum Zugang zu Datenbanken, die Bestandteil von Option D sind, schlägt die Kommission derzeit keine Gesetzgebung vor. Sie wird aber weiterhin über den besten Lösungsansatz für diese beiden Probleme reflektieren.

Die Initiative dürfte zu wirksamerer und effizienterer Ermittlungsarbeit und Strafverfolgung führen und zugleich Transparenz und Rechenschaftspflicht erhöhen und die Achtung der Grundrechte gewährleisten. Auch dürfte sie das Vertrauen in den digitalen Binnenmarkt stärken, indem die Sicherheit erhöht und dem Eindruck von Straflosigkeit entgegengewirkt wird, wenn es um Straftaten auf oder mittels vernetzten Geräten geht.

Für die Behörden würde der Vorstoß anfangs voraussichtlich Umsetzungskosten generieren, diese dürften aber langfristig durch Einsparungen bei wiederkehrenden Kosten aufgewogen werden. Mitarbeiter nationaler Behörden müssten sich auf neue Verfahren einstellen und Schulungen besuchen. Im Anschluss jedoch würden die Behörden von der Straffung und Zentralisierung sowie vom klaren Rechtsrahmen, der Ersuchen um Datenzugang regelt, profitieren, da dies alles zu Effizienzgewinn führen dürfte. Ebenso dürften Länder, die Ersuchen erhalten, eine sinkende Zahl von Ersuchen registrieren, die sie bearbeiten müssen, da mit der bevorzugten Option die Kanäle zur justiziellen Zusammenarbeit entlastet würden.

Diensteanbieter müssten sich auf einen neuen Rechtsrahmen einstellen, indem sie (neue) Verfahren einführen und ihre Mitarbeiter schulen. Andererseits könnte ein harmonisierter

Rahmen die Lasten für jene Anbieter mindern, die derzeit auf Ersuchen für Nichtinhaltsdaten reagieren und die diese nach den unterschiedlichen Gesetzen aller Mitgliedstaaten zu prüfen haben. Rechtssicherheit und eine Standardisierung von Verfahren dürften sich auch positiv auf kleine und mittlere Unternehmen auswirken, da dies die bürokratische Last verringerte und den Wettbewerb in Schwung brächte. Aufs Ganze gesehen ist zudem zu erwarten, dass die Initiative ihnen Einsparungen ermöglicht.

- **Grundrechte**

Der Vorschlag könnte potenziell Auswirkungen auf eine Reihe von Grundrechten haben:

- Rechte des Individuums, auf dessen Daten zugegriffen wird: das Recht auf den Schutz personenbezogener Daten; das Recht auf Achtung des Privat- und Familienlebens; das Recht auf freie Meinungsäußerung; Verteidigungsrechte; das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren;
- Rechte des Diensteanbieters: das Recht auf unternehmerische Freiheit; das Recht auf einen wirksamen Rechtsbehelf;
- Rechte aller Bürger: das Recht auf Freiheit und Sicherheit.

Die vorgeschlagene Verordnung umfasst unter Berücksichtigung des einschlägigen Besitzstands im Bereich Datenschutz ausreichende und wichtige Garantien, um sicherzustellen, dass die Rechte dieser Personen geschützt werden.

Da die Anordnungen nur in Strafverfahren und nur bei Bestehen vergleichbarer innerstaatlicher Situationen sowohl im Ermittlungs- als auch im Gerichtsverfahren erlassen werden können, gelten alle strafrechtlichen Verfahrensgarantien. Dazu gehört insbesondere das in Artikel 6 der Europäischen Menschenrechtskonvention und in den Artikeln 47 und 48 der Charta der Grundrechte festgeschriebene Recht auf ein faires Verfahren. Ferner gehören die einschlägigen Rechtsvorschriften auf EU-Ebene über Verfahrensrechte in Strafverfahren dazu: Richtlinie 2010/64/EU über das Recht auf Dolmetschleistungen und Übersetzungen in Strafverfahren, Richtlinie 2012/13/EU über das Recht auf Belehrung und Unterrichtung in Strafverfahren, Richtlinie 2013/48/EU über das Recht auf Zugang zu einem Rechtsbeistand und auf Kommunikation mit Dritten während des Freiheitsentzugs, Richtlinie (EU) 2016/343 über die Stärkung bestimmter Aspekte der Unschuldsvermutung und des Rechts auf Anwesenheit in der Verhandlung, Richtlinie (EU) 2016/800 über Verfahrensgarantien für Kinder und Richtlinie (EU) 2016/1919 über Prozesskostenhilfe für Verdächtige und beschuldigte Personen in Strafverfahren sowie für gesuchte Personen in Verfahren zur Vollstreckung eines Europäischen Haftbefehls.

Insbesondere gewährleistet das vorherige Einschalten einer Justizbehörde beim Erlass der Anordnung, dass die Rechtmäßigkeit der Maßnahme, ihre Notwendigkeit und Verhältnismäßigkeit im Hinblick auf den betreffenden Fall überprüft wurde. Dies stellt auch sicher, dass die Anordnung sich nicht unzulässig auf die Grundrechte einschließlich Rechtsgrundsätze wie die Vertraulichkeit der anwaltlichen Korrespondenz auswirkt. Die Anordnungsbehörde ist verpflichtet im Einzelfall sicherzustellen, dass die Maßnahme auch im Hinblick auf die Schwere der Straftat, die Gegenstand der Ermittlungen ist, notwendig und verhältnismäßig ist. Der Vorschlag enthält zudem ein Mindeststrafmaß für Transaktions- und Inhaltsdaten, was gewährleistet, dass die Europäische Herausgabeanordnung nur für schwerwiegendere Straftaten in Bezug auf solche Daten verwendet wird.

Auch das Recht auf einen wirksamen Rechtsbehelf für Menschen, um deren Daten ersucht wird, wird ausdrücklich behandelt. Immunitäten und Vorrechte, die bestimmten

Berufsgruppen wie Rechtsanwälten gewährt werden, und grundlegende Interessen in Bezug auf die nationale Sicherheit oder Verteidigung im Staat des Adressaten müssen während des Verfahrens im Anordnungsstaat ebenfalls berücksichtigt werden. Die Nachprüfung durch ein Gericht dient hier als eine weitere Garantie.

Da die Anordnung eine verbindliche Maßnahme ist, wirkt sie sich auch auf die Rechte der Diensteanbieter, insbesondere das Recht auf unternehmerische Freiheit, aus. Der Vorschlag umfasst ein Anrecht des Diensteanbieters, bestimmte Ansprüche im Anordnungsmitgliedstaat geltend zu machen, beispielsweise wenn die Anordnung nicht von einer Justizbehörde erlassen oder validiert wurde. Wenn die Anordnung zwecks Vollstreckung an den Vollstreckungsstaat übermittelt wird, kann die Vollstreckungsbehörde beschließen, die Anordnung nach Konsultation der Anordnungsbehörde bei Vorliegen zulässiger Ablehnungsgründe nicht anzuerkennen oder nicht zu vollstrecken. Sollte das Vollstreckungsverfahren eingeleitet werden, kann zudem der Adressat selbst die Anordnung noch vor der Vollstreckungsbehörde aufgrund solcher zulässiger Ablehnungsgründe ablehnen. Das gilt beispielsweise auch für Fälle, in denen es offensichtlich ist, dass die Anordnung nicht von einer zuständigen Behörde erlassen oder validiert wurde oder in denen durch die Einhaltung offenkundig gegen die Charta verstoßen würde oder die Einhaltung offensichtlich missbräuchlich wäre. Dies schließt nicht das Recht des Adressaten auf einen wirksamen gerichtlichen Rechtsbehelf gegen eine Entscheidung über die Verhängung einer Sanktion aus.

Ein potenzielles Problem in Zusammenhang mit EU-Maßnahmen in diesem Bereich ist, dass Drittstaaten dazu bewogen werden könnten, Verpflichtungen für EU-Diensteanbieter einzuführen, die nicht mit den EU-Grundrechten in Einklang stehen und damit auch nicht mit dem hohen Maß an Datenschutz, das durch den EU-Besitzstand gewährleistet wird. Der Vorschlag behandelt diese Problematik auf zweierlei Weise: zum einen dadurch, dass eine Maßnahme vorgesehen ist, die starke Garantien und ausdrückliche Verweise auf die dem EU-Besitzstand bereits zugrundeliegenden Voraussetzungen und Garantien enthält, was Modellcharakter für die ausländische Gesetzgebung hat; zum anderen durch die Aufnahme einer spezifischen Klausel zu einander widersprechenden Verpflichtungen. Diese ermöglicht es Diensteanbietern, einander widersprechende Verpflichtungen zu identifizieren und zu thematisieren, mit denen sie sich konfrontiert sehen, was wiederum eine gerichtliche Überprüfung in Gang setzt. Diese Klausel wurde geschaffen, um die Einhaltung zweier Arten von Gesetzen sicherzustellen: einerseits von generell blockierenden Gesetzen (blocking statutes) wie etwa dem US-amerikanischen Electronic Communications Privacy Act (ECPA) – der Offenlegung in Zusammenhang mit Inhaltsdaten innerhalb seines geografischen Geltungsbereich außer unter bestimmten Voraussetzungen verbietet –, andererseits von Gesetzen, durch die Offenlegung nicht generell, sondern gegebenenfalls in Einzelfällen verboten wird. Für Fälle in Zusammenhang mit dem ECPA kann derzeit in bestimmten Situationen der Zugang zu Inhaltsdaten verweigert werden, deshalb sollte die Rechtshilfe das zentrale Instrument für den Zugang zu diesen Daten bleiben. Mit den Änderungen durch die Verabschiedung des Gesetzes zur Regelung der rechtmäßigen Verwendung von Daten im Ausland (Clarifying Lawful Overseas Use of Data Act; CLOUD Act)[23] in den Vereinigten Staaten könnte das blockierende Gesetz aufgehoben werden, wenn die EU ein Übereinkommen mit den USA schlössen. Zusätzliche internationale Übereinkommen mit anderen Schlüsselpartnern könnten das Risiko von Gesetzeskollisionen weiter senken.

[23] Der CLOUD Act wurde am 23. März 2018 in den Vereinigten Staaten verabschiedet. Das Gesetz kann hier eingesehen werden.

Aus den vorstehenden Ausführungen kann geschlossen werden, dass die in diesem Vorschlag genannten Maßnahmen mit den Grundrechten vereinbar sind.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

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

5. WEITERE ANGABEN

- **Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

Die Verordnung gilt in der Union unmittelbar. Sie wird von den Angehörigen der entsprechenden Berufsgruppen unmittelbar angewandt, eine Änderung innerstaatlicher Rechtssysteme ist nicht notwendig.

Die Verordnung wird bewertet, und die Kommission wird dem Europäischen Parlament und dem Rat spätestens 5 Jahre nach ihrem Inkrafttreten einen Bericht vorlegen. Auf Grundlage der Ergebnisse dieses Berichts, insbesondere zu der Frage, ob die Verordnung mit Blick auf die Praxis lückenhaft ist, und unter Berücksichtigung technologischer Entwicklungen wird die Kommission die Notwendigkeit eines erweiterten Anwendungsbereichs der Verordnung bewerten. Im Bedarfsfall wird die Kommission Vorschläge unterbreiten, um die Verordnung anzupassen. Die Mitgliedstaaten übermitteln der Kommission alle erforderlichen Angaben zur Ausarbeitung des Berichts. Sie sammeln die zur jährlichen Überwachung der Verordnung erforderlichen Daten.

Bei Bedarf wird die Kommission für Diensteanbieter Leitlinien zur Einhaltung der Verpflichtungen gemäß der Verordnung vorlegen.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

	VERORDNUNG	
	Artikel	**Erwägungsgrund**
I. Gegenstand, Begriffsbestimmungen und Anwendungsbereich	1. Gegenstand	1-15
	2. Begriffsbestimmungen	16-23
	3. Anwendungsbereich	24-27
II. Europäische Herausgabeanordnung, Europäische Sicherungsanordnung und Zertifikate, Vertreter	4. Anordnungsbehörde	30
	5. Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung	28-29, 31-35
	6. Voraussetzungen für den Erlass einer Europäischen Sicherungsanordnung	36

	7. Adressat einer Europäischen Herausgabeanordnung und einer Europäischen Sicherungsanordnung	37
	8. Zertifikate über eine Europäische Herausgabe- oder Sicherungsanordnung	38-39
	9. Ausführung eines EPOC	40-41
	10. Ausführung eines EPOC-PR	42
	11. Vertraulichkeit und Nutzerinformationen	43
	12. Kostenerstattung	entfällt
III. Sanktionen und Vollstreckung	13. Sanktionen	entfällt
	14. Vollstreckungsverfahren	44-45, 55
IV. Rechtsbehelfe	15. und 16. Überprüfungsverfahren bei einander widersprechenden Verpflichtungen aus dem Recht eines Drittstaats	47-53
	17. Wirksame Rechtsbehelfe	54
	18. Gewährleistung von Immunitäten und Vorrechten nach dem Recht des Vollstreckungsstaats	35
V. Schlussbestimmungen	19. Monitoring und Berichterstattung	58
	20. Änderungen der Zertifikate und Formulare	59-60
	21. Ausübung der Befugnisübertragung	60
	22. Mitteilungen	entfällt
	23. Bezug zu Europäischen Ermittlungsanordnungen	61
	24. Bewertung	62
	25. Inkrafttreten	entfällt

Kapitel 1: Gegenstand, Begriffsbestimmungen und Anwendungsbereich

Artikel 1: Gegenstand

In diesem Artikel werden der allgemeine Anwendungsbereich und das Ziel des Vorschlags festgelegt, die Regeln aufzustellen, nach denen eine zuständige Justizbehörde in der Europäischen Union mittels einer Europäischen Herausgabe- oder Sicherungsanordnung von einem Diensteanbieter, der in der Union Dienstleistungen anbietet, verlangen kann, elektronische Beweismittel herauszugeben oder zu sichern. Diese Instrumente können nur in

grenzüberschreitenden Fällen angewendet werden, also in Fällen, in denen der Diensteanbieter in einem anderen Mitgliedstaat niedergelassen oder vertreten ist.

Diese Verordnung gibt den untersuchenden Behörden zusätzliche Instrumente zur Einholung elektronischer Beweismittel an die Hand – ohne die bereits in den nationalen Rechtsvorschriften vorgesehenen Befugnisse zu beschränken –, um in ihrem Hoheitsgebiet niedergelassene oder vertretene Diensteanbieter in die Pflicht zu nehmen. Wenn der Diensteanbieter im selben Mitgliedstaat niedergelassen oder vertreten ist, nutzen die Behörden dieses Mitgliedstaats deshalb nationale Maßnahmen, um den Diensteanbieter in die Pflicht zu nehmen.

Die durch eine Europäische Herausgabeanordnung angeforderten Daten sollten den Behörden direkt zur Verfügung gestellt werden – ohne Mitwirkung der Behörden des Mitgliedstaates, in dem der Diensteanbieter niedergelassen oder vertreten ist. Die Verordnung bewegt sich auch weg vom Datenort als einem entscheidenden Anknüpfungspunkt, da die Datenspeicherung normalerweise zu einer Kontrolle durch den Staat führt, in dessen Hoheitsgebiet die Daten gespeichert sind. Eine solche Speicherung wird in den meisten Fällen aufgrund unternehmerischer Erwägungen durch den Anbieter selbst bestimmt[24].

Darüber hinaus gilt die Verordnung auch dann, wenn die Diensteanbieter zwar nicht in der Union niedergelassen oder vertreten sind, wohl aber ihre Dienste in der Union anbieten. Dem wird in Artikel 3 Absatz 1 Rechnung getragen.

Wenn der Vorschlag sich auf einen Diensteanbieter bezieht, der über einen benannten Vertreter in einem Mitgliedstaat niedergelassen oder vertreten ist, dann ergibt sich allein aus der Benennung eines Vertreters keine Niederlassung des Diensteanbieters im Sinne dieser Verordnung.

In Artikel 1 Absatz 2 wird darauf hingewiesen, dass diese Verordnung nicht die Pflicht berührt, die Grundrechte und allgemeinen Rechtsgrundätze, wie sie in Artikel 6 des Vertrags über die Europäische Union niedergelegt sind, zu achten.

Artikel 2: Begriffsbestimmungen

In diesem Artikel werden die für das Instrument geltenden Begriffsbestimmungen festgelegt.

Die folgenden Diensteanbieter fallen in den Anwendungsbereich der Verordnung: Anbieter elektronischer Kommunikationsdienste, Anbieter von Diensten der Informationsgesellschaft, für die die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung ist, einschließlich sozialer Netzwerke, soweit sie nicht als elektronische Kommunikationsdienste gelten, Online-Marktplätze, die Transaktionen zwischen ihren Nutzern (wie Verbrauchern oder Unternehmen) vereinfachen, und Anbieter anderer Hosting-Dienste sowie Anbieter von Internetdomänennamen und IP-Adressendiensten.

Der Anwendungsbereich der Verordnung deckt Anbieter elektronischer Kommunikationsdienste gemäß der Definition [in der Richtlinie über den europäischen Kodex für die elektronische Kommunikation] ab. Für traditionelle Telekommunikationsdienste, Verbraucher und Unternehmen werden neue internetgestützte

[24] Die Folgenabschätzung enthält weitere Erläuterungen.

Dienste, die interpersonelle Kommunikationsdienste wie Internet-Telefondienste („Voice over IP“), die Übermittlung von Sofortnachrichten und E-Mail-Dienste möglich machen, zunehmend wichtiger als traditionelle Kommunikationsdienste. Diese Dienste sowie soziale Netzwerke wie Twitter und Facebook, die den Nutzern den Austausch von Inhalten ermöglichen, sollten daher mit diesem Vorschlag abgedeckt werden.

In vielen Fällen werden Daten nicht mehr auf dem Gerät eines Nutzers gespeichert, sondern über eine Cloud-Infrastruktur grundsätzlich für den Zugang von jedem beliebigen Ort aus zur Verfügung gestellt. Diensteanbieter müssen nicht in jedem Staat niedergelassen sein oder dort Server unterhalten, sondern können vielmehr eine zentrale Verwaltung und dezentrale Systeme nutzen, um Daten zu speichern und ihre Dienste anzubieten. Sie tun dies, um den Lastausgleich zu optimieren und um schneller auf Ersuchen der Nutzer um Daten zu reagieren. Inhalt verteilende Netze (content delivery networks, CDN) werden in der Regel eingesetzt, um das Bereitstellen von Inhalten durch das Kopieren von Inhalten auf verschiedene Server in aller Welt zu beschleunigen. Damit können Unternehmen Inhalte von dem Server liefern, der dem Nutzer am nächsten ist oder der die Kommunikation durch ein schwächer frequentiertes Netzwerk leiten kann. Um dieser Entwicklung Rechnung zu tragen, umfasst die Definition Cloud- und anderen Hosting-Dienste, die vielfältige Informatikressourcen wie Netzwerke, Server oder andere Infrastruktur, Datenspeicherung, Apps und Dienste bereitstellen, die das Speichern von Daten für verschiedene Zwecke ermöglichen. Das Instrument gilt auch für digitale Marktplätze, an denen Verbraucher und/oder Unternehmen Geschäfte über Online-Verkäufe oder Dienstleistungsverträge abschließen können. Diese Transaktionen erfolgten entweder auf der Website des Online-Marktplatzes oder auf der Website eines Händlers, der vom Online-Marktplatz bereitgestellte Informatikdienste nutzt. Daher sind auf diesem Marktplatz elektronische Beweismittel zu finden, die im Verlauf eines Strafverfahrens nötig werden könnten.

Dienste, für die die Speicherung von Daten kein bestimmendes Element ist, fallen nicht unter den Vorschlag. Obwohl die meisten von Anbietern bereitgestellten Dienste in irgendeiner Form die Speicherung von Daten beinhalten, insbesondere wenn sie online aus der Ferne erbracht werden, lassen sich Dienste identifizieren, für die das Speichern von Daten kein zentrales Merkmal und daher nur ein nebensächliches Element ist, darunter online erbrachte Rechts-, Architektur, Ingenieur- und Buchführungsleistungen.

Daten im Besitz von Anbietern von Internet-Infrastrukturdiensten wie Domänennamen-Registrierstellen und -Registern und Datenschutz- und Proxy-Diensteanbieter oder regionale Internetregister für IP-Adressen können in Strafverfahren wichtig werden, da sie Spuren zur Identifizierung von an strafbaren Handlungen beteiligten Personen oder Einrichtungen liefern können.

Zu den Datenkategorien, die von den zuständigen Behörden mit einer Europäischen Herausgabeanordnung eingeholt werden können, gehören Teilnehmerdaten, Zugangsdaten, Transaktionsdaten (diese drei Kategorien werden als „Nichtinhaltsdaten“ bezeichnet) und gespeicherte Inhaltsdaten. Diese Unterscheidung ist – abgesehen von den Zugangsdaten – in den Rechtsordnungen vieler Mitgliedstaaten und auch in den Rechtsrahmen von Drittstaaten vorgesehen.

Alle Kategorien enthalten personenbezogene Daten und fallen somit unter die Garantien im Rahmen der Datenschutzvorschriften der EU. Die Intensität der Auswirkungen auf die Grundrechte variiert, insbesondere zwischen Teilnehmerdaten einerseits und Transaktions- und Inhaltsdaten andererseits. Es ist entscheidend, dass all diese Kategorien unter das

Instrument fallen: Teilnehmer- und Zugangsdaten sind oft der Ausgangspunkt, um bei einer Untersuchung erste Hinweise auf die Identität eines Verdächtigen zu erhalten. Transaktions- und Inhaltsdaten können sich unterdessen in Sachen Beweismittel als relevanteste Daten erweisen. Wegen des unterschiedlich starken Eingriffs in die Grundrechte ist es gerechtfertigt, den Teilnehmerdaten einerseits und den Transaktions- und Inhaltsdaten andererseits unterschiedliche Voraussetzungen zuzumessen, wie dies auch in mehreren Bestimmungen der Verordnung der Fall ist.

Zugangsdaten sollten in dieser Verordnung als gesonderte Datenkategorie betrachtet werden. Die Beschaffung von Zugangsdaten im hier definierten Sinn wird für dasselbe Ziel angestrebt wie die Beschaffung von Teilnehmerdaten, d. h. zur Identifizierung des Nutzers, und das Ausmaß des Eingriffs in die Grundrechte ist ähnlich. Daher sollten sie denselben Voraussetzungen unterliegen wie Teilnehmerdaten. Daher wird mit diesem Vorschlag eine neue Datenkategorie eingeführt, die wie Teilnehmerdaten zu behandeln ist, wenn dasselbe Ziel verfolgt wird.

Artikel 2 definiert die Mitgliedstaaten und die Behörden, die an dem Verfahren beteiligt sein könnten. Eine Definition der Anordnungsbehörde wurde in Artikel 4 aufgenommen.

Notfälle sind außergewöhnliche Umstände, die regelmäßig eine rasche Reaktion der Diensteanbieter erfordern und für die besondere Voraussetzungen gelten. Sie werden deshalb in diesem Artikel gesondert definiert.

Artikel 3: Anwendungsbereich

Dieser Artikel legt den Anwendungsbereich des Vorschlags fest. Die Verordnung gilt für alle Diensteanbieter, die Dienste in der Union anbieten, darunter auch Diensteanbieter, die nicht in der Union niedergelassen sind. Das aktive Angebot von Diensten in der Union mitsamt allen daraus erwachsenden Vorteilen rechtfertigt, dass diese Diensteanbieter ebenfalls der Verordnung unterliegen, und schafft gleiche Ausgangsbedingungen für Teilnehmer an denselben Märkten. Darüber hinaus entstünde eine Lücke, wenn diese Diensteanbieter nicht einbezogen würden, und Straftätern würde es leicht gemacht, den Anwendungsbereich der Verordnung zu umgehen.

Damit festgestellt werden kann, ob Dienstleistungen angeboten werden, müssen die Behörden prüfen, ob der Diensteanbieter juristische oder natürliche Personen in einem oder mehreren Mitgliedstaaten befähigt, seine Dienste zu nutzen. Allerdings sollte die bloße Zugänglichkeit des Dienstes (die auch aus der Zugänglichkeit der Website des Dienstleisters oder eines Vermittlers oder einer E-Mail-Adresse oder anderer Kontaktdaten erwachsen könnte) keine ausreichende Voraussetzung für die Anwendung dieser Verordnung sein. Deshalb ist eine wesentliche Verbindung zu diesen Mitgliedstaaten erforderlich, um eine ausreichende Verbindung zwischen dem Anbieter und dem Hoheitsgebiet, in dem er seine Dienste anbietet, festzustellen. Eine solche wesentliche Verbindung besteht, wenn ein Diensteanbieter eine Niederlassung in einem oder mehreren Mitgliedstaaten hat. Besteht keine Niederlassung in der Union, 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 lässt sich anhand aller relevanten Umstände, einschließlich Faktoren wie der Verwendung einer in einem Mitgliedstaat allgemein verwendeten Sprache oder Währung bestimmen. Ferner ließe sich die Ausrichtung von Tätigkeiten auf einen Mitgliedstaat auch aus der Verfügbarkeit einer App im jeweiligen

nationalen App-Store, aus lokaler Werbung oder Werbung in der in einem Mitgliedstaat verwendeten Sprache, aus der Nutzung von Informationen von Personen in den Mitgliedstaaten im Zuge der Aktivitäten oder aus dem Management der Kundenbeziehungen, z. B. durch die Bereitstellung von Kundendiensten in der in einem Mitgliedstaat allgemein verwendeten Sprache, ableiten. Von einer wesentlichen Verbindung ist auch dann auszugehen, wenn ein Diensteanbieter seine Tätigkeit gemäß Artikel 17 Absatz 1 Buchstabe c der Verordnung 1215/2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen auf einen oder mehrere Mitgliedstaaten ausrichtet.

Die Europäische Herausgabeanordnung und die Europäische Sicherungsanordnung sind Ermittlungsmaßnahmen, die nur im Rahmen von strafrechtlichen Ermittlungen oder Strafverfahren für konkrete Straftaten erlassen werden können. Die Verbindung zu einer konkreten Ermittlung unterscheidet sie von vorbeugenden Maßnahmen oder gesetzlich festgelegten Verpflichtungen zur Vorratsdatenspeicherung und gewährleistet die Anwendung der für Strafverfahren geltenden Verfahrensrechte. Die Befugnis, Ermittlungen in einer bestimmten Straftat einzuleiten, ist daher eine Voraussetzung, um die Verordnung heranziehen zu können.

Als zusätzliches Erfordernis müssen die angeforderten Daten in Zusammenhang mit den Diensten des Anbieters in der Union stehen.

Kapitel 2: Europäische Herausgabeanordnung, Europäische Sicherungsanordnung und Zertifikate

Artikel 4: Anordnungsbehörde

Wenn eine Europäische Herausgabeanordnung oder Sicherungsanordnung erlassen wird, muss stets eine Justizbehörde entweder als anordnende oder als validierende Behörde beteiligt sein. Für Anordnungen zur Herausgabe von Transaktions- oder Inhaltsdaten ist ein Richter oder ein Gericht erforderlich. Bei Teilnehmer- oder Zugangsdaten kann dies auch von einem Staatsanwalt übernommen werden.

Artikel 5: Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung

In Artikel 5 sind die Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung festgelegt. Sie müssen von der anordnenden Justizbehörde geprüft werden.

Die Europäische Herausgabeanordnung darf nur erlassen werden, wenn dies im Einzelfall notwendig und verhältnismäßig ist. Darüber hinaus sollte sie nur erlassen werden, wenn im Anordnungsstaat in einer vergleichbaren innerstaatlichen Situation eine ähnliche Maßnahme zur Verfügung stünde.

Anordnungen zur Herausgabe von Teilnehmer- und Zugangsdaten können für jede Straftat erlassen werden. Transaktions- und Inhaltsdaten sollten strengeren Anforderungen unterliegen, um dem sensibleren Charakter solcher Daten und der im Vergleich zu Teilnehmer- und Zugangsdaten entsprechend höheren Invasivität von Anordnungen bezüglich derartiger Daten Rechnung zu tragen. Anordnungen können daher nur für Straftaten erlassen werden, die mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden. Die Festlegung eines Mindeststrafmaßes auf Basis einer Freiheitsstrafe im Höchstmaß ermöglicht ein verhältnismäßigeres Vorgehen; ferner sind eine Reihe weiterer Ex-

ante- und Ex-post-Voraussetzungen und Garantien vorgesehen, die für die Wahrung der Verhältnismäßigkeit und der Rechte der betroffenen Personen sorgen sollen.

Zugleich sollte ein Mindeststrafmaß die Wirksamkeit des Instruments und seine Anwendung durch die Praktiker nicht unterlaufen. Die Mitgliedstaaten wenden je nach nationalem System unterschiedliche Höchstmaße für Strafen an. Das Strafrecht der einzelnen Länder variiert und ist nicht harmonisiert. Dies gilt sowohl für die Straftaten als auch für die zu verhängenden Sanktionen. Auch die nationalen Prozessordnungen unterscheiden sich hinsichtlich des Mindeststrafmaßes für das Einholen von Transaktions- oder Inhaltsdaten: In manchen Mitgliedstaaten wurde kein spezifisches Mindeststrafmaß festgelegt, in anderen gibt es eine Auflistung der Straftaten. Ein Mindeststrafmaß von drei Jahren begrenzt den Anwendungsbereich des Instruments auf schwerere Straftaten, ohne die Möglichkeiten seiner Anwendung durch die Praktiker übermäßig einzuschränken. Dieses Maß nimmt abhängig vom Strafgesetzbuch des Mitgliedstaats ein breites Spektrum von Straftaten vom Anwendungsbereich aus (in einigen Mitgliedstaaten beispielsweise die Beteiligung an den Aktivitäten einer kriminellen Vereinigung und Entführung, aber auch Straftaten wie einfacher Diebstahl, Betrug und tätliche Angriffe, für die eine grenzüberschreitende Anordnung zur Herausgabe sensiblerer Daten als unverhältnismäßig gelten könnte). Andererseits sind mit der Obergrenze von drei Jahren Straftaten erfasst, die ein wirksameres Vorgehen erfordern wie die Mitgliedschaft in einer kriminellen Vereinigung, die Finanzierung terroristischer Gruppen, die Unterstützung oder Werbung für eine kriminelle Vereinigung, die Ausbildung zur Ausführung terroristischer Straftaten, bestimmte Straftaten, die aus terroristischen Motiven begangen werden, und die Vorbereitung einer Straftat, die aus terroristischer Motivation verübt werden soll, oder die Vorbereitung einer Geiselnahme; diese Straftaten wären je nach Mitgliedstaat bei einem höheren Mindeststrafmaß ausgenommen. Dieses Mindeststrafmaß wurde gewählt, um für alle Mitgliedstaaten ein Gleichgewicht zwischen effizienten strafrechtlichen Ermittlungen sowie dem Schutz der Rechte und Verhältnismäßigkeit zu sorgen. Ein Mindeststrafmaß hat zudem den Vorteil, in der Praxis leicht anwendbar zu sein.

Zudem können Anordnungen zur Herausgabe von Transaktions- oder Inhaltsdaten auch für spezifische in der Bestimmung aufgeführte harmonisierte Straftaten erlassen werden, für die Beweismittel in der Regel meistens lediglich in elektronischer Form verfügbar sind. Dies rechtfertigt die Anwendung der Verordnung auch in Fällen, in denen die Freiheitsstrafe im Höchstmaß unter dem vorgenannten Mindeststrafmaß liegt; andernfalls könnte bei diesen Straftaten nicht ordnungsgemäß ermittelt werden, was zu Straffreiheit führen könnte. Die Straftaten sind besondere Bestimmungen von: (i) Rahmenbeschluss 2001/413/JI des Rates zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, (ii) Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates und (iii) Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates. Anordnungen können auch für Straftaten erlassen werden, die in der Richtlinie (EU) 2017/541 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates aufgelistet sind. Einige dieser Straftaten haben ein Höchststrafmaß von mindestens einem Jahr, andere von zwei Jahren, keines aber liegt unter einem Höchststrafmaß von einem Jahr.

In dem Artikel sind zudem obligatorische Angaben festgelegt, die in der Europäischen Herausgabeanordnung enthalten sein müssen, damit der Diensteanbieter die angeforderten Daten identifizieren und herausgeben kann. Die Begründung in Bezug auf die Notwendigkeit

und Verhältnismäßigkeit dieser Maßnahme ist ebenfalls Bestandteil der Europäischen Herausgabeanordnung.

Die Europäische Herausgabeanordnung wird durch den Erlass eines Zertifikats über eine Europäische Herausgabeanordnung (EPOC) (siehe Artikel 8) umgesetzt, die übersetzt und dem Diensteanbieter übermittelt wird. Das Zertifikat enthält dieselben obligatorischen Angaben wie die Anordnung mit Ausnahme der Gründe für die Notwendigkeit und Verhältnismäßigkeit der Maßnahme oder weiteren Einzelheiten zu dem Fall.

In Fällen, in denen die angeforderten Daten als Teil einer Infrastruktur gespeichert oder verarbeitet werden, die ein Diensteanbieter für ein Unternehmen – in der Regel für Hosting- oder Softwaredienste – bereitstellt, sollte das Unternehmen selbst der primäre Adressat eines Ersuchens der untersuchenden Behörden sein. In Fällen, in denen das Unternehmen kein in den Anwendungsbereich dieser Verordnung fallender Diensteanbieter ist, kann hierfür eine EEA oder ein Rechtshilfeverfahren erforderlich sein. Der Diensteanbieter kann nur dann Adressat einer Europäischen Herausgabeanordnung sein, wenn es nicht angemessen wäre, das Ersuchen an das Unternehmen zu richten, insbesondere in Fällen, in denen dadurch die Ermittlungen gefährdet werden könnten – beispielsweise, wenn das Unternehmen selbst Gegenstand von Ermittlungen ist.

Vor dem Erlass einer Europäischen Herausgabeanordnung muss die Anordnungsbehörde auch potenzielle Immunitäten und Vorrechte nach dem Recht des Mitgliedstaats des Diensteanbieters oder Auswirkungen auf grundlegende Interessen dieses Mitgliedstaats wie nationale Sicherheit und Verteidigung berücksichtigen. Ziel dieser Bestimmung ist es zu gewährleisten, dass die Immunitäten und Vorrechte, die die im Mitgliedstaat des Diensteanbieters angeforderten Daten schützen, im Anordnungsstaat berücksichtigt werden, insbesondere, wenn sie einen höheren Schutz vorsehen als das Recht des Anordnungsstaats.

Artikel 6: Voraussetzungen für den Erlass einer Europäischen Sicherungsanordnung

Eine Europäische Sicherungsanordnung unterliegt ähnlichen Voraussetzungen wie die Europäische Herausgabeanordnung. Sie kann gemäß den anderen in Artikel 6 genannten Voraussetzungen für jede Straftat erlassen werden. Sie zielt darauf ab, die Entfernung, Löschung oder Änderung relevanter Daten in Situationen zu verhindern, in denen mehr Zeit benötigt wird, um die Herausgabe dieser Daten zu erwirken – zum Beispiel, weil Kanäle für die justizielle Zusammenarbeit genutzt werden. Da beispielsweise die EEA generell für jede Straftat ohne Beschränkung auf ein Mindeststrafmaß erlassen werden kann, wird auch die Europäische Sicherungsanordnung nicht beschränkt. Andernfalls wäre dieses Instrument nicht wirksam. Damit die untersuchenden Behörden schnell handeln können und da das relevante Ersuchen das spätere Ersuchen um Herausgabe der Daten ist, für das alle Voraussetzungen nochmals geprüft werden, können Europäische Sicherungsanordnungen auch von einem Staatsanwalt erlassen oder validiert werden.

Artikel 7: Adressat einer Europäischen Herausgabeanordnung und einer Europäischen Sicherungsanordnung

Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen sollten an einen Vertreter gerichtet werden, den der Diensteanbieter zum Zweck der Beweismittelerhebung in Strafverfahren im Einklang mit der Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren benannt hat. Die Übermittlung erfolgt gemäß Artikel 8 in Form eines

Zertifikats über eine Europäische Herausgabeanordnung (EPOC) oder eines Zertifikats über eine Europäische Sicherungsanordnung (EPOC-PR). Dieser Vertreter ist für ihre Entgegennahme und die rasche und vollständige Ausführung verantwortlich. Damit haben Diensteanbieter die Wahl, wie sie sich hinsichtlich der von mitgliedstaatlichen Behörden angeordneten Herausgabe von Daten organisieren wollen.

Wenn kein Vertreter benannt wurde, können Anordnungen an jede Niederlassung des Diensteanbieters in der Union gerichtet werden. Diese Alternative dient dazu, die Wirksamkeit des Systems für den Fall zu gewährleisten, dass der Diensteanbieter (noch) keinen bestimmten Vertreter benannt hat, beispielsweise, wenn es nach der Richtlinie keine Pflicht zur Benennung eines Vertreters gibt, weil Diensteanbieter in nur einem Mitgliedstaat niedergelassen und tätig sind, oder in Fällen, in denen eine Verpflichtung zur Benennung eines Vertreters vor der Umsetzungsfrist der Richtlinie noch nicht besteht.

Im Falle der Nichteinhaltung durch den Vertreter kann die Anordnungsbehörde sich in zwei Fällen an jede Niederlassung des Diensteanbieters in der Union wenden: In Notfällen gemäß Artikel 9 Absatz 2 und in Fällen, in denen der Vertreter seinen Verpflichtungen nach den Artikeln 9 und 10 nicht nachkommt und in denen die Anordnungsbehörde klare Risiken eines Datenverlusts sieht.

Artikel 8: Zertifikate über eine Europäische Herausgabe- oder Sicherungsanordnung

Das EPOC und das EPOC-PR dienen der Übermittlung der Anordnungen an den in Artikel 7 definierten Adressaten. Muster für beide Zertifikate sind in den Anhängen I und II der Verordnung enthalten; sie müssen in eine der Amtssprachen des Mitgliedstaats übersetzt werden, in dem der Adressat ansässig ist. Der Diensteanbieter kann erklären, dass Anordnungen auch in anderen Amtssprachen der Union akzeptiert werden. Zweck der Zertifikate ist es, alle notwendigen Informationen bereitzustellen, die dem Adressaten dann in einem standardisierten Format übermittelt werden, Fehlerquellen zu minimieren, eine unkomplizierte Identifizierung der Daten zu ermöglichen, Freitext so weit wie möglich zu vermeiden und so die Übersetzungskosten zu senken. Die komplette Begründung in Bezug auf die Notwendigkeit und Verhältnismäßigkeit oder weitere Einzelheiten zu dem Fall sind nicht Bestandteil des Zertifikats, um die Ermittlungen nicht zu gefährden. Sie ist lediglich als Bestandteil der eigentlichen Anordnung notwendig, damit der Verdächtige sie später während des Strafverfahrens anfechten kann.

Einige Diensteanbieter haben bereits Plattformen eingerichtet, damit Strafverfolgungsbehörden Ersuchen einreichen können. Die Plattformnutzung wird durch die Verordnung nicht unterbunden, da sie viele Vorteile bietet – beispielsweise die Möglichkeit einer unkomplizierten Authentifizierung oder einer sicheren Datenübermittlung. Es muss jedoch möglich sein, über diese Plattformen das EPOC und das EPOC-PR in dem in den Anhängen I und II festgelegten Format einzureichen, ohne zusätzliche die Anordnung betreffende Daten anzufordern.

Plattformen der Mitgliedstaaten oder von Einrichtungen der Union können ebenfalls sichere Optionen zur Übermittlung und zur vereinfachten Authentifizierung der Anordnungen sowie für statistische Erhebungen darstellen. Es sollte erwogen werden, die eCodex- und SIRIUS-Plattformen mit dem Ziel einer sicheren Verbindung zu Diensteanbietern für die Übermittlung des EPOC und des EPOC-PR sowie gegebenenfalls für die Antworten der Diensteanbieter zu erweitern.

Artikel 9: Ausführung eines EPOC

Nach Artikel 9 sind die Adressaten verpflichtet, auf EPOC zu antworten; der Artikel enthält verbindliche Fristen. Die normale Frist beläuft sich auf zehn Tage, in gerechtfertigten Fällen können die Behörden jedoch auch eine kürzere Frist setzen. Darüber hinaus beträgt die Frist in Notfällen – definiert als Situation, in der Leib und Leben oder die körperliche Unversehrtheit einer Person oder eine kritische Infrastruktur unmittelbar bedroht sind – sechs Stunden.

Mit der Bestimmung wird auch die Möglichkeit eines Dialogs zwischen Adressat und Anordnungsbehörde gewährleistet. Wenn das EPOC unvollständig oder offensichtlich falsch ist oder dem Diensteanbieter nur unzureichende Informationen zur Ausführung des Zertifikats liefert, kontaktiert der Adressat die Anordnungsbehörde und versucht mit Hilfe des Formulars in Anhang III den Sachverhalt zu klären. Auch unterrichtet der Adressat die Anordnungsbehörde in Fällen, in denen er die Daten wegen höherer Gewalt oder faktischer Unmöglichkeiten nicht bereitstellen kann. Dies ist der Fall, wenn beispielsweise eine Person, deren Daten angefordert werden, weder Kunde dieses Dienstes war oder die Daten – etwa wegen anderer Auflagen zum Schutz der Privatsphäre – rechtmäßig durch den Diensteanbieter gelöscht wurden, bevor dieser oder sein Vertreter die Anordnung erhielten. Die Anordnungsbehörde müsste diese Umstände kennen, um schnell reagieren zu können und beispielsweise elektronische Beweismittel von einem anderen Diensteanbieter einzuholen und zu verhindern, dass die Behörde ein in dieser Situation sinnloses Vollstreckungsverfahren einleitet.

Wenn der Adressat die Informationen aus anderen als den vorgenannten Gründen gar nicht oder nicht erschöpfend oder zeitnah bereitstellt, muss er die Anordnungsbehörde mit dem Formular in Anhang III über die Gründe unterrichten. Adressaten können daher jedes Problem in Zusammenhang mit der EPOC-Ausführung mit der Anordnungsbehörde thematisieren. Der Anordnungsbehörde wird so ermöglicht, das EPOC in einem frühen Stadium – noch vor der Vollstreckungsphase – zu korrigieren oder zu überdenken.

In Fällen, in denen keine unverzügliche Herausgabe der Daten erfolgt – insbesondere wenn ein Dialog zwischen Adressat und Anordnungsbehörde eingeleitet wird, womit die Fristen nach Artikel 9 Absatz 1 nicht mehr eingehalten werden können –, ist der Diensteanbieter mit Entgegennahme des EPOC verpflichtet, die Daten, sofern sie sich identifizieren lassen, zur Vermeidung eines Verlusts zu sichern. Die Sicherung kann für das präzisierte EPOC oder ein späteres Ersuchen um Rechtshilfe oder eine EEA erfolgen, die anstelle des ursprünglichen EPOC übermittelt werden.

Artikel 10: Ausführung eines EPOC-PR

Die Ausführung eines EPOC-PR erfordert die Sicherung der zum Zeitpunkt der Entgegennahme der Anordnung verfügbaren Daten. Diensteanbieter sollten die Daten so lange wie nötig sichern, um die Daten auf Verlangen herauszugeben, vorausgesetzt, die Anordnungsbehörde bestätigt binnen 60 Tagen nach Erlass der Anordnung, dass sie das spätere Ersuchen um Herausgabe in die Wege geleitet hat. Dies setzt voraus, dass zumindest einige formelle Schritte unternommen wurden, dass als etwa die Übersetzung eines Rechtshilfeersuchens in Auftrag gegeben wurde.

Andererseits sollten Sicherungsanordnungen nur ergehen oder aufrechterhalten werden, so lange sie notwendig sind, um ein späteres Ersuchen um Herausgabe dieser Daten zu

ermöglichen. Um eine unnötige oder übermäßig lange Sicherung zu vermeiden, informiert die Behörde, die die Europäische Sicherungsanordnung erlassen hat, den Adressaten, sobald entschieden wurde, vom Erlass einer Herausgabeanordnung oder eines Ersuchens um justizielle Zusammenarbeit abzusehen oder die Anordnung bzw. das Ersuchen aufzuheben.

Mit der Bestimmung wird analog zu den Bestimmungen in Artikel 9 ebenfalls die Möglichkeit eines Dialogs zwischen Adressat und Anordnungsbehörde gewährleistet. Wenn das EPOC-PR unvollständig oder offensichtlich falsch ist oder dem Diensteanbieter nur unzureichende Informationen zur Ausführung des Zertifikats liefert, kontaktiert der Adressat die Anordnungsbehörde und versucht mit Hilfe des Formulars in Anhang III den Sachverhalt zu klären. Auch unterrichtet der Adressat die Anordnungsbehörde, wenn er die Daten unter Umständen, die als höhere Gewalt anzusehen sind, oder wegen faktischer Unmöglichkeit oder aus anderen Gründen nicht bereitstellen kann.

Artikel 11: Vertraulichkeit und Nutzerinformationen

Die Vertraulichkeit der laufenden Ermittlungen einschließlich der Tatsache, dass eine Anordnung zur Einholung relevanter Daten ergangen ist, muss gewahrt bleiben. Dieser Artikel orientiert sich an Artikel 19 der EEA-Richtlinie. Er schreibt die Verpflichtung des Adressaten oder, falls abweichend, des Diensteanbieters fest, die Vertraulichkeit des EPOC oder des EPOC-PR zu wahren, insbesondere indem gemäß Artikel 23 der Datenschutz-Grundverordnung zur Sicherstellung der Ermittlung von Straftaten auf Aufforderung der Anordnungsbehörde davon abgesehen wird, die Person, deren Daten angefordert werden, hiervon in Kenntnis zu setzen.

Anderseits ist es auch zur Ausübung von Rechtsbehelfen wichtig, die Person, deren Daten angefordert werden, zu unterrichten. Wo dies auf Aufforderung der Anordnungsbehörde nicht durch den Diensteanbieter geschieht, unterrichtet die Anordnungsbehörde die Person gemäß Artikel 13 der Richtlinie für den Datenschutz bei Polizei und Strafjustiz, sobald kein Risiko mehr besteht, dass die Ermittlung gefährdet wird, und übermittelt auch Informationen über verfügbare Rechtsbehelfe. Wegen des geringfügigeren Eingriffs in die betreffenden Rechte werden solche Informationen nicht im Fall einer Europäischen Sicherungsanordnung, sondern nur für Europäische Herausgabeinformationen bereitgestellt.

Artikel 12: Kostenerstattung

Sofern die nationalen Rechtsvorschriften des Anordnungsstaats dies für innerstaatliche Anordnungen in ähnlichen innerstaatlichen Fällen vorsehen, können Diensteanbieter gemäß den Rechtsvorschriften des Anordnungsstaats eine Erstattung ihrer Kosten durch diesen Staat geltend machen. Dies gewährleistet die Gleichbehandlung von Diensteanbietern, an die eine innerstaatliche Anordnung gerichtet wurde, und von Diensteanbietern, an die ein EPOC durch denselben Mitgliedstaat gerichtet wurde, wenn dieser Mitgliedstaat die Kostenerstattung für bestimmte Diensteanbieter beschlossen hat. Andererseits vereinheitlicht die vorgeschlagene Verordnung die Kostenerstattung nicht, da die Mitgliedstaaten in dieser Hinsicht unterschiedlich entschieden haben.

Die Kosten können entweder direkt durch den Diensteanbieter oder über seinen Vertreter geltend gemacht werden. Die Erstattung kann nur einmal erfolgen.

Kapitel 3: Sanktionen und Vollstreckung

Artikel 13: Sanktionen

Die Mitgliedstaaten gewährleisten, dass wirksame, verhältnismäßige und abschreckende finanzielle Sanktionen zur Verfügung stehen, wenn Diensteanbieter ihren Verpflichtungen nach Artikel 9, 10 oder 11 nicht nachkommen. Nationale Rechtsvorschriften über die Verhängung strafrechtlicher Sanktionen in derartigen Fällen bleiben davon unberührt.

Artikel 14: Vollstreckungsverfahren

In Artikel 14 ist für den Fall der Nichteinhaltung ein Verfahren zur Vollstreckung der Anordnungen mit Hilfe des Mitgliedstaats vorgesehen, in dem der Adressat des übermittelten Zertifikats ansässig ist. Abhängig vom ursprünglichen Adressaten ist dies entweder der Mitgliedstaat des Diensteanbieters oder der Mitgliedstaat des Vertreters. Die Anordnungsbehörde übermittelt die vollständige Anordnung einschließlich der Begründung in Bezug auf Notwendigkeit und Verhältnismäßigkeit sowie das entsprechende Zertifikat an die zuständige Behörde des Vollstreckungsstaats, die es im Einklang mit dem nationalen Recht vollstreckt und sich dabei gegebenenfalls der in Artikel 13 genannten Sanktionen bedient. Wenn die Anordnung zwecks Vollstreckung an den Vollstreckungsstaat übermittelt wird, kann die Vollstreckungsbehörde beschließen, die Anordnung nach Konsultation der Anordnungsbehörde bei Vorliegen bestimmter Gründe nicht anzuerkennen oder nicht zu vollstrecken. Sollte das Vollstreckungsverfahren eingeleitet werden, kann zudem der Adressat selbst die Anordnung vor der Vollstreckungsbehörde ablehnen. Der Adressat kann dies auf Basis derartiger Gründe unter Ausschluss von Immunitäten und Vorrechten, jedoch unter Einbeziehung von Fällen tun, in denen es offensichtlich ist, dass die Anordnung nicht von einer zuständigen Behörde erlassen oder validiert wurde oder in der durch die Einhaltung offenkundig gegen die Charta der Grundrechte der Europäischen Union verstoßen würde oder die Einhaltung offensichtlich missbräuchlich wäre. So würde beispielsweise eine Anordnung zur Herausgabe von Inhaltsdaten, die eine nicht definierte Personengruppe in einem geografischen Gebiet betreffen oder in keinem Zusammenhang zu einem konkreten Strafverfahren stehen, ganz offensichtlich die in dieser Verordnung festgeschriebenen Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung missachten, was bereits aus dem Inhalt des Zertifikats hervorginge. Andere Gründe können nur von der Person geltend gemacht werden, deren Daten angefordert werden, und zwar im Rahmen der eigenen Rechtsbehelfe im Anordnungsstaat (siehe Artikel 17). Zudem verfügen Diensteanbieter über einen Rechtsbehelf gegen die Entscheidung der Vollstreckungsbehörde, eine Sanktion gegen sie zu verhängen.

Das Vollstreckungsverfahren enthält mehrere Fristen für die Vollstreckungs- und für die Anordnungsbehörde, um weitere Verzögerungen in diesem Verfahren zu vermeiden.

Kapitel 4: Rechtsbehelfe

Artikel 15 und 16: Überprüfungsverfahren bei einander widersprechenden Verpflichtungen aus dem Recht eines Drittstaats

In den Artikeln 15 und 16 ist ein Überprüfungsverfahren für den Fall vorgesehen, dass sich Diensteanbieter mit Hauptsitz in Drittstaaten mit einander widersprechenden Verpflichtungen konfrontiert sehen. Diese Bestimmungen sind auch sehr wichtig, um den Schutz individueller Rechte und der diplomatischen Gepflogenheiten zu gewährleisten. Die Festlegung eines hohen Niveaus hat den Zweck, Drittstaaten zu motivieren, für einen ähnlich hohen Schutz zu

sorgen. Im umgekehrten Fall, in dem Behörden aus Drittstaaten bei einem EU-Diensteanbieter Daten eines EU-Bürgers anfordern, können die Rechtsvorschriften der Union oder der Mitgliedstaaten zum Schutz der Grundrechte wie etwa der Besitzstand im Bereich des Datenschutzes gleichfalls die Offenlegung verhindern. Die Europäische Union erwartet von Drittländern, ihrerseits derartige Verbote zu respektieren, wie in diesem Vorschlag geschehen.

Das Verfahren nach Artikel 15 kann vom Adressaten ausgelöst werden, wenn die Einhaltung einer Europäischen Herausgabeanordnung einen Verstoß gegen die Rechtsvorschriften eines Drittstaats verursachen würde, die die Offenlegung von Daten mit der Begründung verbieten, dass dies notwendig ist, um entweder die Grundrechte der betroffenen Personen oder die grundlegenden Interessen des betreffenden Drittstaats im Zusammenhang mit der nationalen Sicherheit oder Verteidigung zu schützen. Der Adressat ist verpflichtet, die Anordnungsbehörde durch einen begründeten Einwand über die Gründe für seine Schlussfolgerung zu unterrichten, dass einander widersprechende Verpflichtungen vorliegen. Ein solcher begründeter Einwand kann nicht allein auf der Tatsache basieren, dass im Recht des Drittstaats keine vergleichbaren Bestimmungen existieren, und auch nicht darauf, dass die Daten in einem Drittstaat gespeichert sind. Der begründete Einwand wird nach dem Verfahren des Artikels 9 Absatz 5 zur Mitteilung einer beabsichtigten Nichtbefolgung und unter Verwendung des Formulars in Anhang III erhoben.

Auf Grundlage dieses begründeten Einwands überprüft die Anordnungsbehörde ihre eigene Anordnung. Entscheidet die Anordnungsbehörde, die Anordnung zurückzuziehen, ist das Verfahren beendet. Will die Behörde an der Anordnung festhalten, wird der Fall an das zuständige Gericht in ihrem Mitgliedstaat übermittelt. Das Gericht prüft dann auf Basis des begründeten Einwands und unter Berücksichtigung aller für den Fall relevanten Fakten, ob die Rechtsvorschriften des Drittstaats in dem vorliegenden Fall gelten und, sofern sie gelten, ob in diesem Fall ein Konflikt besteht. Bei dieser Prüfung sollte das Gericht berücksichtigen, ob die Rechtsvorschrift des Drittstaats nicht weniger dem Schutz der Grundrechte oder der grundlegenden Interessen des Drittstaats in Zusammenhang mit der nationalen Sicherheit oder Verteidigung dient, sondern viel mehr offensichtlich darauf abzielt, andere Interessen zu schützen, oder dazu genutzt wird, rechtswidrige Handlungen vor Ersuchen von Strafverfolgungsbehörden im Rahmen strafrechtlicher Ermittlungen abzuschirmen.

Wenn das Gericht zu dem Schluss gelangt, dass tatsächlich ein Konflikt mit Verpflichtungen besteht, die aus Rechtsvorschriften zum Schutz der Grundrechte von Individuen oder grundlegenden Interessen des Drittstaats in Zusammenhang mit der nationalen Sicherheit oder Verteidigung erwachsen, muss das Gericht über die nationalen Zentralbehörden des betreffenden Drittstaats eine Stellungnahme des Drittstaats anfordern. Wenn der konsultierte Drittstaat das Bestehen des Konflikts bestätigt und Einwände gegen die Ausführung der Anordnung hat, muss das Gericht die Anordnung zurückziehen.

Wenn der Konflikt auf der Grundlage anderweitiger drittstaatlicher Rechtsvorschriften entsteht, die nicht entweder dem Schutz der Grundrechte von Individuen oder grundlegenden Interessen des Drittstaats in Zusammenhang mit der nationalen Sicherheit oder Verteidigung dienen, entscheidet das Gericht, indem es die Interessen abwägt, die für oder gegen die Aufrechterhaltung der Anordnung sprechen.

Die in Artikel 9 genannten Voraussetzungen, insbesondere die in Artikel 9 Absatz 6 beschriebenen Sicherungsverpflichtungen, gelten auch dann, wenn sich aus dem Recht eines Drittstaats Verpflichtungen ergeben, die einander widersprechen. Wenn das Gericht zu dem Schluss kommt, dass die Anordnung aufrechtzuerhalten ist, werden die Anordnungsbehörde und der Diensteanbieter im Hinblick auf die beginnende Ausführung der Anordnung informiert. Wird die Anordnung aufgehoben, kann eine getrennte europäische

Sicherungsanordnung erlassen werden, um die Verfügbarkeit der Daten zu gewährleisten, wenn diese über ein Ersuchen um Rechtshilfe eingeholt werden könnten.

Da die Europäische Sicherungsanordnung selbst nicht zur Offenlegung von Daten führt und daher kein Anlass zu vergleichbaren Bedenken besteht, ist das Überprüfungsverfahren auf die Europäische Herausgabeanordnung beschränkt.

Artikel 17: Wirksame Rechtsbehelfe

Diese Bestimmung stellt sicher, dass von der Europäischen Herausgabeanordnung betroffenen Personen wirksame Rechtsbehelfe zur Verfügung stehen. Diese Rechtsbehelfe werden im Anordnungsstaat im Einklang mit dem nationalen Recht ausgeübt. Für Verdächtige und Beschuldigte werden Rechtsbehelfe üblicherweise während des Strafverfahrens ausgeübt. Für die Europäische Sicherungsanordnung, die an sich keine Offenlegung von Daten ermöglicht, stehen keine spezifischen Rechtsbehelfe zur Verfügung; anders ist der Fall gelagert, wenn auf die Sicherungsanordnung eine Europäische Herausgabeanordnung oder ein anderes zur Offenlegung führendes Instrument folgen, woraus sich spezifische Rechtsbehelfe ergeben.

Personen, deren Daten angefordert wurden, bei denen es sich aber nicht um Verdächtige oder Beschuldigte in einem Strafverfahren handelt, haben ebenfalls ein Recht auf einen Rechtsbehelf im Anordnungsstaat. All diese Rechte lassen nach der Richtlinie für den Datenschutz bei Polizei und Strafjustiz und der Datenschutz-Grundverordnung verfügbare Rechtsbehelfe unberührt.

Anders als bei den Bestimmungen für Diensteanbieter sind für all diese Personen gemäß der Verordnung die möglichen Gründe, die Rechtmäßigkeit der Anordnung anzufechten, nicht beschränkt. Zu diesen Gründen zählen die Notwendigkeit und Verhältnismäßigkeit der Anordnung.

Die Ausübung von Rechtsbehelfen im Anordnungsstaat belastet Betroffene nicht unverhältnismäßig. Wie dies bei Anordnungen der Fall ist, die durch andere Formen der justiziellen Zusammenarbeit vollstreckt werden, sind die Gerichte des Anordnungsstaats am besten dazu in der Lage, die Rechtmäßigkeit der von den eigenen Behörden erlassenen Europäischen Herausgabeanordnungen zu überprüfen und ihre Vereinbarkeit mit dem jeweiligen nationalen Recht zu bewerten. Zudem können Adressaten während der Vollstreckungsphase auf Grundlage einer in der Verordnung veröffentlichten Liste von Gründen (siehe Artikel 14) separat die Vollstreckung des EPOC oder des EPOC-PR in ihrem Aufnahmemitgliedstaat ablehnen.

Artikel 18: Gewährleistung von Immunitäten und Vorrechten nach dem Recht des Vollstreckungsstaats

Diese Bestimmung hat wie Artikel 5 Absatz 7 das Ziel zu gewährleisten, dass die Immunitäten und Vorrechte, die die im Mitgliedstaat des Diensteanbieters angeforderten Daten schützen, im Anordnungsstaat berücksichtigt werden, insbesondere, wenn zwischen diesen Mitgliedstaaten Unterschiede bestehen und es um grundlegende Interessen dieses Mitgliedstaats wie nationale Sicherheit und Verteidigung geht. Nach Artikel 18 muss das Gericht im Anordnungsstaat diese so berücksichtigen, als wären sie im nationalen Recht vorgesehen. Wegen der Unterschiede zwischen Mitgliedstaaten bei der Bewertung der Relevanz und Zulässigkeit von Beweismitteln gewährt die Bestimmung den Gerichten Flexibilität, wie dem Rechnung zu tragen ist.

Kapitel 5: Schlussbestimmungen

Artikel 19: Monitoring und Berichterstattung

Nach diesem Artikel sind die Mitgliedstaaten verpflichtet, spezifische Angaben in Zusammenhang mit der Anwendung der Verordnung zur Unterstützung der Kommission bei der Wahrnehmung ihrer Aufgaben nach Artikel 24 zu übermitteln. Die Kommission erstellt ein detailliertes Programm zur Überwachung der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung.

Artikel 20: Änderungen der Zertifikate und Formulare

Die Zertifikate und die Formulare, die in den Anhängen I, II und III dieses Vorschlags enthalten sind, vereinfachen die Ausführung eines EPOC und eines EPOC-PR. Deshalb ist es künftig nötig, so schnell wie möglichen auf potenziellen inhaltlichen Verbesserungsbedarf der Zertifikate und der Formulare reagieren zu können. Es entspricht nicht dieser Anforderung, die drei Anhänge nach dem ordentlichen Gesetzgebungsverfahren zu ändern, zudem stellen sie keine wesentlichen Elemente der Rechtsakte dar; die zentralen Elemente sind in Artikel 8 definiert. Deshalb ist in Artikel 20 ein schnelleres und flexibleres Verfahren für Änderungen durch delegierte Rechtsakte festgelegt.

Artikel 21: Ausübung der Befugnisübertragung

In diesem Artikel wird festgelegt, unter welchen Bedingungen die Kommission befugt ist, delegierte Rechtsakte zu erlassen, um notwendige Änderungen an dem Zertifikat und den Formularen im Anhang des Vorschlags vorzunehmen. Festgelegt wird ein Standardverfahren für die Annahme solcher delegierter Rechtsakte.

Artikel 22: Mitteilungen

Mitgliedstaaten sind verpflichtet, die Kommission über die zuständigen Anordnungs- und Vollstreckungsbehörden sowie darüber zu unterrichten, welche Gerichte dafür zuständig sind, sich mit begründeten Einwänden von Diensteanbietern im Fall einer Gesetzeskollision zu befassen.

Artikel 23: Bezug zu Europäischen Ermittlungsanordnungen

Diese Bestimmung stellt klar, dass die Verordnung mitgliedstaatliche Behörden nicht daran hindert, gemäß der Richtlinie 2014/41/EU Europäische Ermittlungsanordnungen zu erlassen, um elektronische Beweismittel einzuholen.

Artikel 24: Bewertung

Gemäß dieser Bestimmung führt die Kommission eine Bewertung dieser Verordnung im Einklang mit den Leitlinien der Kommission für eine bessere Rechtsetzung und gemäß Nummer 22 der Interinstitutionellen Vereinbarung vom 13. April 2016[25] durch. Die Kommission wird dem Europäischen Parlament und dem Rat fünf Jahre nach dem Inkrafttreten der vorgeschlagenen Verordnung Bericht über die Ergebnisse der Bewertung erstatten, dies schließt eine Prüfung der Notwendigkeit mit ein, ihren Anwendungsbereich auf noch nicht erfasste Dienste zu erweitern, die für Ermittlungen wichtiger werden könnten.

Artikel 25: Inkrafttreten

Die vorgeschlagene Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt in Kraft. Diese Verordnung gilt sechs Monate nach dem Datum des Inkrafttretens.

[25] Interinstitutionelle Vereinbarung zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Europäischen Kommission über bessere Rechtsetzung vom 13. April 2016 (ABl. L 123 vom 12.5.2016, S. 1).

2018/0108 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen

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[26],

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 Beweismittel immer wichtiger. Wirksame Verfahren zur Einholung elektronischer Beweismittel sind für die Bekämpfung von Kriminalität unerlässlich, unterliegen jedoch bestimmten Bedingungen, welche die uneingeschränkte Einhaltung der in der Charta der Grundrechte der Europäischen Union anerkannten und in den Verträgen verankerten Grundrechte und Grundsätze sicherstellen, insbesondere der Grundsätze der Notwendigkeit und Verhältnismäßigkeit, des ordnungsgemäßen Verfahrens, des Datenschutzes, des Briefgeheimnisses und des Schutzes der Privatsphäre.

(3) In der Gemeinsamen Erklärung der Minister für Justiz und Inneres und der Vertreter der Organe der Union vom 22. März 2016 zu den Terroranschlägen in Brüssel wurde betont, dass vorrangig Wege gefunden werden müssen, um elektronische Beweismittel schneller und wirksamer zu sichern und zu erlangen, und dass konkrete Maßnahmen bezüglich dieser Frage ermittelt werden müssen.

(4) In den Schlussfolgerungen des Rates vom 9. Juni 2016 wurden die zunehmende Bedeutung elektronischer Beweismittel in Strafverfahren und der Tatsache, dass der Schutz des Cyberspace vor Missbrauch und kriminellen Aktivitäten maßgeblich für

[26] ABl. C vom , S. .

das Wohl der Volkswirtschaften und Gesellschaften ist und die Strafverfolgungs- und Justizbehörden daher über wirksame Instrumente für die Ermittlung und Verfolgung von Straftaten im Zusammenhang mit dem Cyberspace verfügen müssen, hervorgehoben.

(5) In der Gemeinsamen Mitteilung „Abwehrfähigkeit, Abschreckung und Abwehr“ vom 13. September 2017[27] betonte die Kommission, dass wirksame Ermittlungen und eine wirksame Verfolgung der durch den Cyberraum ermöglichten Kriminalität einen wesentlichen Abschreckungsfaktor darstellen, der bestehende Verfahrensrahmen jedoch besser an das Internetzeitalter angepasst werden muss. Die aktuellen Verfahren könnten mitunter nicht mit der Geschwindigkeit von Cyber-Angriffen Schritt halten, weshalb insbesondere eine zügige grenzüberschreitende Zusammenarbeit erforderlich sei.

(6) Das Europäische Parlament griff diese Bedenken in seiner Entschließung zur Bekämpfung der Cyberkriminalität vom 3. Oktober 2017[28] auf und betonte, dass die derzeit fragmentierten rechtlichen Rahmenbedingungen ein Problem für Diensteanbieter sein können, die darum bemüht sind, den Ersuchen von Strafverfolgungsbehörden nachzukommen, und forderte die Kommission auf, einen Vorschlag für einen EU-Rechtsrahmen für elektronische Beweismittel mit ausreichenden Garantien hinsichtlich der Rechte und Freiheiten aller Betroffenen vorzulegen.

(7) Netzbasierte Dienstleistungen können von einem beliebigen Ort aus erbracht werden und erfordern keine physische Infrastruktur, Räumlichkeiten oder Personal in dem betreffenden Land. Folglich werden relevante Beweismittel häufig außerhalb des ermittelnden Staates oder von einem außerhalb dieses Staates niedergelassenen Diensteanbieter gespeichert. Häufig besteht keine weitere Verbindung zwischen dem untersuchten Fall in dem betreffenden Staat und dem Staat, in dem die Daten gespeichert sind oder die Hauptniederlassung des Diensteanbieters liegt.

(8) Aufgrund dieser fehlenden Verbindung werden Ersuchen um justizielle Zusammenarbeit häufig an Staaten gerichtet, in denen viele Diensteanbieter niedergelassen sind, die aber keinen anderen Bezug zu dem jeweiligen Fall haben. Zudem hat sich die Zahl der Ersuchen angesichts der immer stärker genutzten Netzdienste, die naturgemäß keine Grenzen kennen, vervielfacht. Dies hat dazu geführt, dass die Einholung elektronischer Beweismittel über Kanäle der justiziellen Zusammenarbeit häufig lange dauert – länger als die sich daraus ergebenden Indizien unter Umständen zur Verfügung stehen. Zudem gibt es keinen klaren 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 nach Möglichkeit auf den Kanal für die Zusammenarbeit mit Diensteanbietern, wobei sie unterschiedliche nationale Instrumente, Bedingungen und Verfahren zugrunde legen. In Bezug auf Inhaltsdaten haben einige Mitgliedstaaten ferner einseitige Maßnahmen ergriffen, wohingegen andere sich weiterhin auf die justizielle Zusammenarbeit verlassen.

(9) Der fragmentierte Rechtsrahmen stellt die Diensteanbieter, die Ersuchen von Strafverfolgungsbehörden Folge leisten wollen, vor Probleme. Daher muss ein

---

27 JOIN(2017) 450 final.

28 2017/2068 (INI).

europäischer Rechtsrahmen für elektronische Beweismittel geschaffen werden, mit dem Diensteanbieter im Anwendungsbereich des Instruments verpflichtet werden, Behörden direkt zu antworten, ohne dass die Einschaltung einer Justizbehörde im Mitgliedstaat des Diensteanbieters erforderlich ist.

(10) Anordnungen gemäß dieser Verordnung sollten an die zu diesem Zweck benannten Vertreter von Diensteanbietern gerichtet werden. Wenn ein in der Union niedergelassener Diensteanbieter keinen Vertreter benannt hat, können die Anordnungen an eine beliebige Niederlassung dieses Diensteanbieters in der Union gerichtet werden. Diese Ausweichoption soll die Wirksamkeit des Systems in den Fällen sicherstellen, in denen der Diensteanbieter (noch) keinen speziellen Vertreter benannt hat.

(11) Der Mechanismus der Europäischen Herausgabeanordnung und der Europäischen Sicherungsanordnung für elektronische Beweismittel in Strafsachen kann nur auf der Grundlage eines großen gegenseitigen Vertrauens zwischen den Mitgliedstaaten funktionieren; dies ist eine wesentliche Voraussetzung für das ordnungsgemäße Funktionieren dieses Instruments.

(12) Diese Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden. Dazu gehören das Recht auf Freiheit und Sicherheit, die Achtung des Privat- und Familienlebens, der Schutz personenbezogener Daten, die unternehmerische Freiheit, das Recht auf Eigentum, 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. Hat der Anordnungsmitgliedstaat Hinweise darauf, dass in einem anderen Mitgliedstaat möglicherweise ein paralleles Strafverfahren läuft, so konsultiert er die Behörden dieses Mitgliedstaats gemäß dem Rahmenbeschluss 2009/948/JI des Rates[29].

(13) Um die uneingeschränkte Achtung der Grundrechte zu gewährleisten, nimmt diese Verordnung ausdrücklich Bezug auf die erforderlichen Normen für die Einholung personenbezogener Daten, die Verarbeitung solcher Daten, die gerichtliche Überprüfung der Verwendung der in diesem Instrument vorgesehenen Ermittlungsmaßnahme und die verfügbaren Rechtsbehelfe.

(14) Diese Verordnung sollte unbeschadet der in den Richtlinien 2010/64/EU[30], 2012/13/EU[31], 2013/48/EU[32], (EU) 2016/343[33], (EU) 2016/800[34] und (EU)

---

29 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).

30 Richtlinie 2010/64/EU 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).

31 Richtlinie 2012/13/EU 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).

32 Richtlinie 2013/48/EU 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).

33 Richtlinie (EU) 2016/343 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).

2016/1919[35] des Europäischen Parlaments und des Rates dargelegten Verfahrensrechte in Strafverfahren angewandt werden.

(15) Mit diesem Instrument werden die Regeln festgelegt, nach denen eine zuständige Justizbehörde in der Europäischen Union mittels einer Europäischen Herausgabe- oder Sicherungsanordnung von einem Diensteanbieter, der in der Union Dienstleistungen anbietet, verlangen kann, elektronische Beweismittel herauszugeben oder zu sichern. Diese Verordnung gilt in allen Fällen, in denen der Diensteanbieter in einem anderen Mitgliedstaat niedergelassen oder vertreten ist. In rein innerstaatlichen Fällen, in denen die in dieser Verordnung genannten Instrumente nicht verwendet werden können, sollte die Verordnung die bereits in den nationalen Rechtsvorschriften vorgesehenen Befugnisse der zuständigen nationalen Behörden, Diensteanbieter, die in dem betreffenden Hoheitsgebiet niedergelassen oder vertreten sind, zu bestimmten Maßnahmen zu verpflichten, nicht beschränken.

(16) Die für Strafverfahren wichtigsten Diensteanbieter sind Anbieter elektronischer Kommunikationsdienste und bestimmte Anbieter von Diensten der Informationsgesellschaft, welche die Interaktion zwischen Nutzern erleichtern. Daher sollten beide Gruppen unter diese Verordnung fallen. Elektronische Kommunikationsdienste sind im Vorschlag für eine Richtlinie über den europäischen Kodex für die elektronische Kommunikation 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 hier 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. Dienste der Informationsgesellschaft, bei denen die Speicherung von Daten kein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung, sondern nur ein Nebenprodukt ist, wie online erbrachte Rechts-, Architektur-, Ingenieur- und Buchführungsleistungen, sollten vom Anwendungsbereich dieser Verordnung ausgenommen werden, selbst wenn sie unter die Definition der Dienste der Informationsgesellschaft im Sinne der Richtlinie (EU) 2015/1535 fallen.

(17) In vielen Fällen werden die Daten nicht mehr auf dem Gerät eines Nutzers gespeichert oder verarbeitet, sondern über eine Cloud-Infrastruktur für den Zugang von jedem beliebigen Ort zur Verfügung gestellt. Um diese Dienste betreiben zu können, benötigen Diensteanbieter weder eine Niederlassung noch Server in einem bestimmten Staat. Daher sollte die Anwendung dieser Verordnung nicht vom tatsächlichen Standort der Niederlassung des Diensteanbieters oder der Datenverarbeitungs- oder -speicherungseinrichtung abhängen.

---

34 Richtlinie (EU) 2016/800 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).

35 Richtlinie (EU) 2016/1919 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).

(18) Anbieter von Internetinfrastrukturdiensten im Zusammenhang mit der Zuweisung von Namen und Nummern wie Domänennamen-Registrierungsstellen und -Register sowie Datenschutz- und 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 für Strafverfahren von besonderer Bedeutung sind, da sie die Identifizierung einer Person oder Einrichtung hinter einer für kriminelle Aktivitäten verwendeten Website oder – im Falle einer kompromittierten Website, die von Kriminellen gekapert wurde – des Opfers der kriminellen Aktivität ermöglichen.

(19) Diese Verordnung regelt nur die Erhebung gespeicherter Daten, das heißt derjenigen Daten, die ein Diensteanbieter zum Zeitpunkt des Erhalts des Zertifikats über die Europäische Herausgabe- oder Sicherungsanordnung besitzt. 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 Erhalt eines Zertifikats über eine Herausgabe- oder Sicherungsanordnung gespeichert werden, genehmigt. Daten sollten unabhängig davon bereitgestellt werden, ob sie verschlüsselt sind oder nicht.

(20) Zu den Datenkategorien, die unter diese Verordnung fallen, gehören Teilnehmerdaten, Zugangsdaten, Transaktionsdaten (diese drei Kategorien werden als „Nichtinhaltsdaten“ bezeichnet) und Inhaltsdaten. Diese Unterscheidung ist – abgesehen von den Zugangsdaten – in den Rechtsvorschriften vieler Mitgliedstaaten und auch im derzeitigen Rechtsrahmen der USA vorgesehen, der es den Diensteanbietern ermöglicht, Nichtinhaltsdaten freiwillig an ausländische Strafverfolgungsbehörden weiterzugeben.

(21) Zugangsdaten sollten in dieser Verordnung als gesonderte Datenkategorie betrachtet werden. Die Beschaffung von Zugangsdaten wird zu demselben Zweck angestrebt wie die Beschaffung von Teilnehmerdaten, nämlich zur Identifizierung des betreffenden Nutzers, und das Ausmaß des Eingriffs in die Grundrechte entspricht weitgehend dem bei Teilnehmerdaten. Zugangsdaten werden üblicherweise im Rahmen einer Aufzeichnung von Ereignissen (das heißt einem Server-Protokoll) erfasst, um den Beginn und die Beendigung der Zugangssitzung eines Nutzers in Bezug auf einen Dienst anzuzeigen. Welche Netzschnittstelle während der Zugangssitzung verwendet wird, wird häufig durch eine individuelle (statische oder dynamische) IP-Adresse oder eine andere Kennung gekennzeichnet. Wenn der Nutzer unbekannt ist, müssen häufig diese Daten eingeholt werden, bevor die mit der betreffenden Kennung verbundenen Teilnehmerdaten von dem Diensteanbieter angefordert werden können.

(22) Die Einholung von Transaktionsdaten hingegen wird in der Regel angestrebt, um Informationen über die Kontakte und den Aufenthaltsort des Nutzers zu erhalten; diese Daten können zur Erstellung eines Profils einer Person herangezogen werden. Zugangsdaten allein können nicht einem ähnlichen Zweck dienen; beispielsweise liefern sie keine Informationen zu Gesprächspartnern des betreffenden Nutzers. Daher wird mit diesem Vorschlag eine neue Datenkategorie eingeführt, die wie Teilnehmerdaten zu behandeln ist, wenn mit der Einholung dieser Daten ein ähnliches Ziel verfolgt wird.

(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, insbesondere zwischen den Teilnehmer- und Zugangsdaten einerseits und den Transaktions- und Inhaltsdaten

andererseits. Während Teilnehmer- und Zugangsdaten nützlich sind, um bei einer Untersuchung erste Hinweise zur Identität eines Verdächtigen zu erhalten, sind Transaktions- und Inhaltsdaten am relevantesten als Beweismittel. 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 Bedingungen für die Einholung von Teilnehmer- und Zugangsdaten einerseits und von Transaktions- und Inhaltsdaten andererseits festgelegt.

(24) Die Europäische Herausgabeanordnung und die Europäische Sicherungsanordnung sind Ermittlungsmaßnahmen, die nur im Rahmen eines bestimmten Strafverfahrens gegen bestimmte bekannte oder noch unbekannte Urheber einer konkreten, bereits begangenen Straftat und nach einer individuellen Bewertung der Verhältnismäßigkeit und der Notwendigkeit in jedem Einzelfall erlassen werden sollten.

(25) Diese Verordnung lässt die Ermittlungsbefugnisse der Behörden in Zivil- oder Verwaltungsverfahren unberührt, auch wenn solche Verfahren zu Sanktionen führen können.

(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, selbst wenn der Diensteanbieter in der Union niedergelassen ist.

(27) Damit festgestellt werden kann, ob ein Diensteanbieter Dienstleistungen in der Union anbietet, muss geprüft werden, ob der Diensteanbieter juristische oder natürliche Personen in einem oder mehreren Mitgliedstaaten in die Lage versetzt, seine Dienste in Anspruch zu nehmen. Allerdings sollte die bloße Zugänglichkeit einer Online-Schnittstelle, beispielsweise die Zugänglichkeit der Website des Diensteanbieters oder eines Vermittlers, einer E-Mail-Adresse oder anderer Kontaktdaten in einem oder mehreren Mitgliedstaaten, für sich genommen keine ausreichende Voraussetzung für die Anwendung dieser Verordnung sein.

(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 lässt sich anhand aller relevanten Umstände, einschließlich Faktoren wie der Verwendung einer in dem betreffenden Mitgliedstaat gebräuchlichen Sprache oder Währung oder der Möglichkeit, Waren oder Dienstleistungen zu bestellen, bestimmen. Ferner ließe sich die Ausrichtung von Tätigkeiten auf einen Mitgliedstaat auch von der Verfügbarkeit einer Anwendung („App“) im jeweiligen nationalen App-Store, von der Schaltung lokaler Werbung oder Werbung in der in dem betreffenden Mitgliedstaat verwendeten Sprache oder vom Management der Kundenbeziehungen, zum Beispiel durch die Bereitstellung eines Kundendienstes in der in dem betreffenden Mitgliedstaat gebräuchlichen Sprache, ableiten. Das Vorhandensein einer wesentlichen Verbindung wird auch dann angenommen, wenn ein Diensteanbieter seine Tätigkeit gemäß Artikel 17 Absatz 1 Buchstabe c der Verordnung (EU) Nr. 1215/2012 über die

gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen[36] auf einen oder mehrere Mitgliedstaaten ausrichtet. Andererseits kann die Erbringung der Dienstleistung zum Zwecke der bloßen Einhaltung des in der Verordnung (EU) 2018/302[37] festgelegten Verbots der Diskriminierung nicht allein aus diesem Grund als Ausrichtung von Tätigkeiten auf ein bestimmtes Gebiet innerhalb der Union betrachtet werden.

(29) Eine Europäische Herausgabeanordnung sollte nur erlassen werden, wenn dies notwendig und verhältnismäßig ist. Bei der Prüfung dieser Frage sollte berücksichtigt werden, ob die Anordnung auf das Maß beschränkt ist, das 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.

(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 Transaktions- 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 Teilnehmer- und Zugangsdaten weniger sensibel sind, können Europäische Herausgabeanordnungen für deren Offenlegung auch von den zuständigen Staatsanwälten erlassen oder validiert werden.

(31) Aus dem gleichen Grund muss in Bezug auf den sachlichen Anwendungsbereich dieser Verordnung folgende Unterscheidung getroffen werden: Anordnungen zur Herausgabe von Teilnehmerdaten und Zugangsdaten können wegen jeder Straftat erlassen werden, wohingegen für den Zugang zu Transaktions- 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 Beweismittel in der Regel ausschließlich in elektronischer und somit naturgemäß in nicht dauerhafter Form zur

---

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

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

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 ist ein Höchststrafmaß von mindestens drei Jahren nicht erforderlich.

(33) Des Weiteren muss vorgesehen werden, dass eine Europäische Herausgabeanordnung nur dann erlassen werden darf, wenn in einer vergleichbaren innerstaatlichen Situation im Anordnungsstaat eine ähnliche Anordnung für dieselbe Straftat zur Verfügung stünde.

(34) Wenn die angeforderten Daten als Teil einer Infrastruktur gespeichert oder verarbeitet werden, die ein Diensteanbieter für ein Unternehmen oder eine Einrichtung, die keine natürlichen Personen sind, bereitstellt, üblicherweise im Falle von Hosting-Diensten, sollte die Europäische Herausgabeanordnung nur dann verwendet werden, wenn andere auf das Unternehmen oder die Einrichtung abzielende Ermittlungsmaßnahmen nicht geeignet sind, insbesondere wenn dadurch Ermittlungen beeinträchtigt werden könnten. Dies ist insbesondere dann von Belang, wenn es um größere Einheiten wie Kapitalgesellschaften oder staatliche Stellen geht, die die Dienste von Diensteanbietern für die Bereitstellung ihrer gesamten IT-Infrastruktur oder für die Erbringung von IT-Dienstleistungen oder für beides in Anspruch nehmen. Der erste Adressat einer Europäischen Herausgabeanordnung sollte in solchen Fällen das Unternehmen beziehungsweise die Einrichtung sein. Dieses Unternehmen beziehungsweise diese Einrichtung muss kein Diensteanbieter sein, der in den Anwendungsbereich dieser Verordnung fällt. In Fällen, in denen es nicht sinnvoll ist, sich an dieses Unternehmen oder diese Einrichtung zu wenden, beispielsweise weil der Verdacht auf Beteiligung an dem betreffenden Fall besteht oder es Hinweise auf Absprachen mit dem Ziel der Ermittlung gibt, sollten sich die zuständigen Behörden jedoch an den Diensteanbieter, der die betreffende Infrastruktur bereitstellt, wenden und von diesem die Übermittlung der angeforderten Daten verlangen können. Diese Bestimmung berührt nicht das Recht, vom Diensteanbieter die Sicherung der Daten zu verlangen.

(35) Auf Immunitäten und Vorrechte für Personengruppen (wie Diplomaten) oder besonders geschützte Beziehungen (wie das Recht auf Vertraulichkeit der Kommunikation zwischen Anwalt und Mandant) wird in anderen Instrumenten zur gegenseitigen Anerkennung wie der Europäischen Ermittlungsanordnung Bezug genommen. Ihr Umfang und ihre Auswirkungen unterscheiden sich je nach dem geltenden nationalen Recht, das bei Erlass der Anordnung zu berücksichtigen ist, da die Anordnungsbehörde die Anordnung nur dann erlassen darf, wenn in einer vergleichbaren innerstaatlichen Situation eine ähnliche Anordnung erlassen werden könnte. Zusätzlich zu diesem Grundprinzip sollten die Immunitäten und Vorrechte, die Zugangs-, Transaktions- oder Inhaltsdaten im Mitgliedstaat des Diensteanbieters schützen, im Anordnungsstaat nach Möglichkeit genauso berücksichtigt werden als wären sie im nationalen Recht des Anordnungsstaats vorgesehen. Dies gilt insbesondere, wenn das Recht des Mitgliedstaats, in dem die Anordnung an den

Diensteanbieter oder seinen Vertreter gerichtet wird, einen höheren Schutz vorsieht als das Recht des Anordnungsstaats. Ferner gewährleistet die Bestimmung, dass Fälle Berücksichtigung finden, in denen sich die Offenlegung der Daten auf grundlegende Interessen des betreffenden Mitgliedstaats wie die nationale Sicherheit und Verteidigung auswirken kann. Als zusätzliche Schutzmaßnahme sollten diese Aspekte nicht nur beim Erlass der Anordnung berücksichtigt werden, sondern auch zu einem späteren Zeitpunkt bei der Prüfung der Relevanz und Zulässigkeit der betreffenden Daten in der jeweiligen Phase des Strafverfahrens und im Falle eines Vollstreckungsverfahrens durch die vollstreckende Behörde.

(36) Die Europäische Sicherungsanordnung kann wegen jeder Straftat erlassen werden. Ihr Ziel besteht darin, die Entfernung, Löschung oder Änderung relevanter Daten in Situationen zu verhindern, in denen mehr Zeit für die Erwirkung der Herausgabe dieser Daten benötigt wird, zum Beispiel weil Kanäle für die justizielle Zusammenarbeit genutzt werden.

(37) Europäische Herausgabe- und Sicherungsanordnungen sollten an den vom Diensteanbieter benannten Vertreter gerichtet werden. Wenn kein Vertreter benannt wurde, können Anordnungen an eine Niederlassung des Diensteanbieters in der Union gerichtet werden. Dies kann dann der Fall sein, wenn der Diensteanbieter nicht gesetzlich verpflichtet ist, einen Vertreter zu benennen. Im Falle der Nichtbefolgung durch den Vertreter in Notfällen kann die Übermittlung der Europäischen Herausgabe- oder Sicherungsanordnung an den Diensteanbieter auch zusätzlich zu der oder anstatt der Betreibung der Vollstreckung der ursprünglichen Anordnung gemäß Artikel 14 erfolgen. Im Falle der Nichtbefolgung durch den Vertreter in einer Situation, die keinen Notfall darstellt, in der aber eindeutige Risiken eines Datenverlusts bestehen, kann eine Europäische Herausgabe- oder Sicherungsanordnung auch an eine beliebige Niederlassung des Diensteanbieters in der Union gerichtet werden. Aufgrund dieser verschiedenen möglichen Szenarien wird in den Bestimmungen der allgemeine Begriff „Adressat“ verwendet. Gilt eine Verpflichtung, zum Beispiel zur Wahrung der Vertraulichkeit, nicht nur für den Adressaten, sondern auch für den Diensteanbieter, wenn dieser nicht der Adressat ist, so ist dies in der entsprechenden Bestimmung angegeben.

(38) Europäische Herausgabe- und Sicherungsanordnungen sollten dem Diensteanbieter 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; diese Zertifikate sollten übersetzt werden. Die Zertifikate sollten dieselben obligatorischen Angaben enthalten wie die Anordnungen, mit Ausnahme der Gründe für die Notwendigkeit und Verhältnismäßigkeit der Maßnahme und weiterer Einzelheiten zu dem Fall, um eine Gefährdung der Ermittlungen zu vermeiden. Da sie jedoch Teil der eigentlichen Anordnung sind, können sie von der betreffenden verdächtigen Person später während des Strafverfahrens angefochten werden. Erforderlichenfalls muss ein Zertifikat in eine der Amtssprachen des Mitgliedstaats des Adressaten oder in eine andere Amtssprache, der der Diensteanbieter zugestimmt hat, übersetzt werden.

(39) Die zuständige Anordnungsbehörde sollte das EPOC oder das EPOC-PR im Einklang mit den Vorschriften zum Schutz personenbezogener Daten direkt an den Adressaten übermitteln, und zwar in einer Form, die einen schriftlichen Nachweis unter Bedingungen ermöglicht, die dem Diensteanbieter die Feststellung der Echtheit gestatten, zum Beispiel per Einschreiben, über ein gesichertes E-Mail-System und

Plattformen oder sonstige gesicherte Kanäle, einschließlich der vom Diensteanbieter zur Verfügung gestellten.

(40) Die angeforderten Daten sollten den Behörden spätestens innerhalb von zehn Tagen nach Erhalt des EPOC übermittelt werden. In Notfällen und wenn die Anordnungsbehörde andere Gründe für eine Abweichung von der Zehn-Tage-Frist nennt, sollten Diensteanbieter auch kürzere Fristen einhalten. Neben der unmittelbaren Gefahr einer Löschung der angeforderten Daten könnten solche Gründe auch Umstände umfassen, die im Zusammenhang mit einer laufenden Untersuchung stehen, zum Beispiel wenn die angeforderten Daten mit anderen dringenden Ermittlungsmaßnahmen verbunden sind, die ohne die fehlenden Daten nicht durchgeführt werden können oder auf andere Weise von ihnen abhängig sind.

(41) Damit Diensteanbieter formale Probleme lösen können, muss ein Verfahren für die Kommunikation zwischen dem Diensteanbieter und der anordnenden Justizbehörde festgelegt werden für die Fälle, in denen das EPOC möglicherweise unvollständig ist oder offensichtliche Fehler oder keine ausreichenden Informationen zur Ausführung der Anordnung enthält. Sollte der Diensteanbieter die Informationen zudem aus anderen Gründen nicht vollständig oder fristgerecht übermitteln, beispielsweise weil er der Ansicht ist, dass ein Widerspruch zu einer Verpflichtung nach dem Recht eines Drittstaats besteht oder dass die Europäische Herausgabeanordnung nicht gemäß den in dieser Verordnung festgelegten Bedingungen erlassen wurde, so sollte er sich an die Anordnungsbehörden wenden und seine Ansicht angemessen begründen. Das Kommunikationsverfahren sollte allgemein die Berichtigung oder erneute Prüfung des EPOC durch die Anordnungsbehörde in einem frühen Stadium ermöglichen. Um die Verfügbarkeit der Daten zu gewährleisten, sollte der Diensteanbieter die Daten sichern, wenn er die angeforderten Daten identifizieren kann.

(42) Nach Erhalt eines EPOC-PR sollte der Diensteanbieter die angeforderten Daten für höchstens 60 Tage sichern, es sei denn, die Anordnungsbehörde teilt ihm mit, dass sie das Verfahren für die Stellung eines entsprechenden Ersuchens um Herausgabe eingeleitet hat; in diesem Fall sollte die Sicherung der Daten fortgesetzt werden. Die 60-Tage-Frist wird berechnet, um die Stellung eines offiziellen Ersuchens zu ermöglichen. Dies setzt voraus, dass zumindest einige formelle Schritte unternommen wurden, beispielsweise die Übersetzung eines Rechtshilfeersuchens in Auftrag gegeben wurde. Nach Erhalt dieser Informationen sollten die Daten so lange gesichert werden, bis sie im Rahmen eines späteren Ersuchens um Herausgabe herausgegeben werden.

(43) Diensteanbieter und ihre Vertreter sollten Vertraulichkeit gewährleisten und auf Ersuchen der Anordnungsbehörde davon absehen, die Person, deren Daten angefordert werden, hierüber zu informieren, um gemäß Artikel 23 der Verordnung (EU) 2016/679[38] die Ermittlung von Straftaten sicherzustellen. Nutzerinformationen tragen jedoch maßgeblich zur Ermöglichung von Überprüfungen und Rechtsbehelfen bei und sollten im Einklang mit der nationalen Maßnahme zur Umsetzung des Artikels 13 der Richtlinie (EU) 2016/680[39] von der Behörde bereitgestellt werden,

---

38 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).

39 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

wenn der Diensteanbieter aufgefordert wurde, den Nutzer nicht zu informieren, sofern keine Gefahr besteht, dass laufende Ermittlungen gefährdet werden.

(44) Im Falle der Nichtbefolgung durch den Adressaten kann die Anordnungsbehörde die vollständige Anordnung, einschließlich der Begründung in Bezug auf die Notwendigkeit und Verhältnismäßigkeit, sowie das entsprechende Zertifikat an die zuständige Behörde des Mitgliedstaats übermitteln, in dem der Adressat des Zertifikats ansässig oder niedergelassen ist. Dieser Mitgliedstaat sollte die Anordnung gemäß seinen nationalen Rechtsvorschriften vollstrecken. Die Mitgliedstaaten sollten dafür sorgen, dass bei Verstößen gegen die Verpflichtungen aus dieser Verordnung wirksame, verhältnismäßige und abschreckende finanzielle Sanktionen verhängt werden.

(45) Das Vollstreckungsverfahren ist ein Verfahren, bei dem der Adressat die Vollstreckung aus bestimmten beschränkten Gründen ablehnen kann. Die Vollstreckungsbehörde kann die Anerkennung und Vollstreckung der Anordnung ablehnen, entweder aus denselben Gründen oder wenn Immunitäten und Vorrechte gemäß den betreffenden nationalen Rechtsvorschriften gelten oder wenn die Offenlegung Auswirkungen auf grundlegende Interessen wie die nationale Sicherheit und Verteidigung haben könnte. Bevor die Vollstreckungsbehörde die Anerkennung oder Vollstreckung der Anordnung aus diesen Gründen ablehnt, sollte sie die Anordnungsbehörde konsultieren. Im Falle der Nichtbefolgung können die Behörden Sanktionen verhängen. Diese Sanktionen sollten auch angesichts bestimmter Umstände wie einer wiederholten oder systematischen Nichtbefolgung verhältnismäßig sein.

(46) Ungeachtet ihrer Datenschutzpflichten sollten die Diensteanbieter in den Mitgliedstaaten nicht für Schäden haftbar gemacht werden, die ihren Nutzern oder Dritten ausschließlich aufgrund der Befolgung eines EPOC oder eines EPOC-PR in guter Absicht entstehen.

(47) Neben den Personen, deren Daten angefordert werden, können auch die Diensteanbieter und Drittstaaten von der Ermittlungsmaßnahme betroffen sein. 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 gerichtliche Überprüfung vorgesehen, wenn die Befolgung einer Europäischen Herausgabeanordnung Diensteanbieter daran hindern würde, ihren aus dem Recht eines Drittstaats erwachsenden rechtlichen Verpflichtungen nachzukommen.

(48) Zu diesem Zweck sollte der Adressat, wenn er der Auffassung ist, dass die Europäische Herausgabeanordnung im konkreten Fall eine Verletzung einer aus dem Recht eines Drittstaats erwachsenden Verpflichtung zur Folge hätte, die Anordnungsbehörde durch einen unter Verwendung der vorgesehenen Formulare erstellten begründeten Einwand hiervon in Kenntnis setzen. Die Anordnungsbehörde sollte dann die Europäische Herausgabeanordnung im Lichte des begründeten Einwands überprüfen und hierbei dieselben Kriterien berücksichtigen, die das zuständige Gericht zugrunde legen müsste. Beschließt die Behörde, die Anordnung

---

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).

aufrechtzuerhalten, sollte das Verfahren an das vom betreffenden Mitgliedstaat benannte zuständige Gericht verwiesen werden, das die Anordnung dann überprüft.

(49) Bei der Prüfung, ob in dem betreffenden Fall ein Widerspruch zwischen verschiedenen Verpflichtungen besteht, sollte sich das zuständige Gericht gegebenenfalls auf angemessenes externes Fachwissen stützen, beispielsweise wenn die Überprüfung Fragen zur Auslegung des Rechts des betreffenden Drittstaats aufwirft. In diesem Zusammenhang können auch die zentralen Behörden des betreffenden Staates konsultiert werden.

(50) Das Fachwissen über die Auslegung könnte gegebenenfalls auch durch Sachverständigengutachten eingeholt werden. Informationen und die Rechtsprechung zur Auslegung von Rechtsvorschriften von Drittstaaten 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. Auf diese Weise könnten die Gerichte von den Erfahrungen und dem Fachwissen anderer Gerichte zu denselben oder ähnlichen Fragen profitieren. Eine erneute Konsultation des Drittstaats sollte gegebenenfalls aber dennoch möglich sein.

(51) Wenn einander widersprechende Verpflichtungen bestehen, sollte das Gericht prüfen, ob die widersprüchlichen Bestimmungen des Drittstaats die Offenlegung der betreffenden Daten mit der Begründung verbieten, dass dies notwendig ist, um entweder die Grundrechte der betroffenen Personen oder die grundlegenden Interessen des betreffenden Drittstaats im Zusammenhang mit der nationalen Sicherheit oder Verteidigung zu schützen. Bei dieser Prüfung sollte das Gericht berücksichtigen, ob die betreffenden Rechtsvorschriften des Drittstaats nicht weniger dem Schutz der Grundrechte oder der grundlegenden Interessen des Drittstaats im Zusammenhang mit der nationalen Sicherheit oder Verteidigung dienen, sondern vielmehr offensichtlich darauf abzielen, andere Interessen zu schützen, oder dazu genutzt werden, rechtswidrige Handlungen vor Ersuchen von Strafverfolgungsbehörden im Rahmen strafrechtlicher Ermittlungen abzuschirmen. Wenn das Gericht zu dem Schluss gelangt, dass die widersprüchlichen Bestimmungen des Drittstaats die Offenlegung der betreffenden Daten mit der Begründung verbieten, dass dies zum Schutz der Grundrechte der betroffenen Personen oder der grundlegenden Interessen des Drittstaats im Zusammenhang mit der nationalen Sicherheit oder Verteidigung notwendig ist, sollte es den Drittstaat über seine zentralen Behörden, die bereits für Rechtshilfezwecke in den meisten Teilen der Welt eingerichtet sind, konsultieren. Ferner sollte das Gericht eine Frist festlegen, innerhalb deren der Drittstaat Einwände gegen die Ausführung der Europäischen Herausgabeanordnung erheben kann; wenn die Behörden des Drittstaats nicht innerhalb der (verlängerten) Frist antworten, obwohl sie in einem Erinnerungsschreiben auf die Folgen einer Nichtbeantwortung hingewiesen wurden, so erhält das Gericht die Anordnung aufrecht. Lehnen die Behörden des Drittstaats die Offenlegung ab, so sollte das Gericht die Anordnung aufheben.

(52) In allen anderen Fällen einander widersprechender Verpflichtungen, die nicht mit den Grundrechten der betroffenen Person oder den grundlegenden Interessen des Drittstaats im Zusammenhang mit der nationalen Sicherheit oder Verteidigung verbunden sind, sollte das Gericht seine Entscheidung über die Aufrechterhaltung der Europäischen Herausgabeanordnung treffen, indem es eine Reihe von Faktoren abwägt, anhand deren die Stärke der Verbindung zu einem der beiden beteiligten Rechtssysteme, das jeweilige Interesse an der Einholung oder stattdessen der

Verhinderung der Offenlegung der Daten und die möglichen Konsequenzen für den Diensteanbieter, wenn er der Anordnung Folge leisten muss, festzustellen sind. Bei Cyberstraftaten ist zu beachten, dass der Tatort sowohl den Ort, an dem die Tat begangen wurde, als auch den Ort, an dem die Auswirkungen der Straftat eingetreten sind, umfasst.

(53) Die in Artikel 9 genannten Bedingungen gelten auch dann, wenn sich aus dem Recht eines Drittstaats Verpflichtungen ergeben, die einander widersprechen. Während dieses Verfahrens sollten die Daten gesichert werden. Wird die Anordnung aufgehoben, so kann eine neue Sicherungsanordnung erlassen werden, damit die Anordnungsbehörde die Herausgabe der Daten über andere Kanäle, beispielsweise im Wege der Rechtshilfe, erwirken kann.

(54) Es ist von wesentlicher Bedeutung, dass alle Personen, deren Daten in strafrechtlichen Ermittlungen oder in Strafverfahren angefordert werden, im Einklang mit Artikel 47 der Charta der Grundrechte der Europäischen Union einen wirksamen Rechtsbehelf einlegen können. Verdächtige und Beschuldigte sollten ihr Recht auf einen wirksamen Rechtsbehelf während des Strafverfahrens ausüben. Dies kann sich auf die Zulässigkeit oder gegebenenfalls die Gewichtung der auf eine solche Weise eingeholten Beweismittel auswirken. Darüber hinaus profitieren Verdächtige und Beschuldigte von allen für sie geltenden Verfahrensgarantien wie dem Recht auf Belehrung und Unterrichtung. Andere Personen, die weder Verdächtige noch Beschuldigte sind, sollten ebenfalls ein Recht auf einen wirksamen Rechtsbehelf haben. Daher sollte zumindest die Möglichkeit vorgesehen werden, die Rechtmäßigkeit einer Europäischen Herausgabeanordnung, einschließlich der Notwendigkeit und Verhältnismäßigkeit der Anordnung, anzufechten. Die vorliegende Verordnung sollte die möglichen Gründe für die Anfechtung der Rechtmäßigkeit der Anordnung nicht beschränken. Diese Rechtsbehelfe sollten im Anordnungsstaat im Einklang mit dem nationalen Recht ausgeübt werden. Vorschriften über den vorläufigen Rechtsschutz sollten durch nationales Recht geregelt werden.

(55) Darüber hinaus kann sich der Adressat während des Vollstreckungsverfahrens und der anschließenden Einlegung eines Rechtsbehelfs der Vollstreckung einer Europäischen Herausgabe- oder Sicherungsanordnung aus einer Reihe von bestimmten Gründen widersetzen, unter anderem wenn die Anordnung nicht von einer zuständigen Behörde erlassen oder validiert wurde oder wenn sie offenkundig gegen die Charta der Grundrechte der Europäischen Union verstößt oder offensichtlich missbräuchlich ist. So stünde beispielsweise eine Anordnung, mit der die Herausgabe von Inhaltsdaten 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.

(56) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union und Artikel 16 Absatz 1 AEUV hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Bei der Durchführung dieser Verordnung sollten die Mitgliedstaaten sicherstellen, dass personenbezogene Daten geschützt und nur gemäß der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 verarbeitet werden.

(57) Nach dieser Verordnung eingeholte personenbezogene Daten sollten nur dann verarbeitet werden, wenn dies für Zwecke der Prävention, Ermittlung, Aufdeckung

oder Verfolgung von Straftaten oder mit 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 Gewährleistung der Datensicherheit. Die Diensteanbieter sollten für die Übermittlung personenbezogener Daten an die zuständigen Behörden dasselbe sicherstellen. Der Zugang zu Informationen mit personenbezogenen Daten sollte befugten Personen vorbehalten sein, wofür durch Authentifizierungsverfahren gesorgt werden kann. Zur Gewährleistung der Authentifizierung sollte die Verwendung von Mechanismen erwogen werden, beispielsweise der notifizierten nationalen elektronischen Identifizierungssysteme oder Vertrauensdienste gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

(58) Die Kommission sollte eine Bewertung dieser Verordnung vornehmen, die sich auf die fünf Kriterien Effizienz, Wirksamkeit, Relevanz, Kohärenz und EU-Mehrwert stützen und die Grundlage für Folgenabschätzungen für mögliche weitere Maßnahmen bilden 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 Justizbehörden und Diensteanbietern, sodass sie elektronische Beweismittel schneller und wirksamer sicherstellen und übermitteln und gleichzeitig die notwendigen Sicherheitsanforderungen in benutzerfreundlicher Weise erfüllen können. Solche Formulare senken die Übersetzungskosten und tragen zu einem hohen Qualitätsstandard bei. Antwortformulare sollten einen standardisierten Informationsaustausch ermöglichen, insbesondere wenn Diensteanbieter die Anordnung nicht befolgen können, weil das Konto nicht existiert oder weil keine Daten verfügbar sind. Zudem dürften die Formulare auch die Erhebung von Statistiken erleichtern.

(60) Damit einem etwaigen Verbesserungsbedarf hinsichtlich des Inhalts der EPOC und der EPOC-PR sowie des Formulars für die Übermittlung von Informationen über die Unmöglichkeit der Vollstreckung eines EPOC oder eines EPOC-PR wirksam entsprochen werden kann, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union Rechtsakte zur Änderung der Anhänge I, II und III dieser Verordnung zu erlassen. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, und dass diese Konsultationen mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[40] niedergelegt wurden. Um insbesondere eine gleichberechtigte Beteiligung an der Ausarbeitung delegierter Rechtsakte zu gewährleisten, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch

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

Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Ausarbeitung der delegierten Rechtsakte befasst sind.

(61) Für die Einholung von elektronischen Beweismitteln sollten die auf dieser Verordnung basierenden Maßnahmen Europäische Ermittlungsanordnungen gemäß der Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates[41] 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 Beweismittel aus einem anderen Mitgliedstaat umfassen.

(62) Aufgrund technologischer Entwicklungen ist es möglich, dass in einigen Jahren neue Formen von Kommunikationsinstrumenten überwiegend verwendet werden oder Lücken bei der Anwendung dieser Verordnung entstehen. Daher ist es wichtig, eine Überprüfung ihrer Anwendung vorzusehen.

(63) Da das Ziel dieser Verordnung, nämlich die Verbesserung der grenzüberschreitenden Sicherstellung und Einholung elektronischer Beweismittel, 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 *[haben das Vereinigte Königreich und Irland schriftlich mitgeteilt, dass sie sich an der Annahme und der Anwendung dieser Verordnung beteiligen möchten]/[beteiligen sich das Vereinigte Königreich und Irland unbeschadet des Artikels 4 des Protokolls nicht an der Annahme dieser Verordnung, die daher für sie weder bindend noch ihnen 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 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates[42] angehört und gab am (...) eine Stellungnahme[43] ab —

---

41 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).

42 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

43 ABl. C vom , S. .

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 von einem Diensteanbieter, der in der Union Dienstleistungen anbietet, verlangen kann, elektronische Beweismittel herauszugeben oder zu sichern, unabhängig davon, wo sich die Daten befinden. Diese Verordnung berührt nicht die Befugnisse der nationalen Behörden, Diensteanbieter, die in dem betreffenden Hoheitsgebiet niedergelassen oder vertreten sind, zur Einhaltung ähnlicher nationaler Maßnahmen zu verpflichten.

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

Artikel 2
Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Europäische Herausgabeanordnung“ eine verbindliche Entscheidung einer Anordnungsbehörde eines Mitgliedstaats, mit der ein Diensteanbieter, der in der Union Dienstleistungen anbietet und in einem anderen Mitgliedstaat niedergelassen oder vertreten ist, zur Herausgabe elektronischer Beweismittel verpflichtet wird;

2. „Europäische Sicherungsanordnung“ eine verbindliche Entscheidung einer Anordnungsbehörde eines Mitgliedstaats, mit der ein Diensteanbieter, der in der Union Dienstleistungen anbietet und in einem anderen Mitgliedstaat niedergelassen oder vertreten ist, im Hinblick auf ein späteres Ersuchen um Herausgabe zur Sicherung elektronischer Beweismittel verpflichtet wird;

3. „Diensteanbieter“ jede natürliche oder juristische Person, die eine oder mehrere der folgenden Kategorien von Dienstleistungen anbietet:

   a) elektronische Kommunikationsdienste im Sinne des Artikels 2 Absatz 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[44], bei denen die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung ist, einschließlich sozialer Netzwerke, Online-Marktplätze, die Transaktionen zwischen ihren Nutzern erleichtern, und anderen Anbietern von Hosting-Diensten;

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

5. „Niederlassung“ entweder die tatsächliche Ausübung einer wirtschaftlichen Tätigkeit auf unbestimmte Zeit durch eine stabile Infrastruktur, von der aus die Geschäftstätigkeit der Dienstleistungserbringung ausgeübt wird, oder eine stabile Infrastruktur, von der aus die Geschäftstätigkeit verwaltet wird;

6. „elektronische Beweismittel“ Beweismittel, die zum Zeitpunkt des Erhalts eines Zertifikats über eine Herausgabe- oder Sicherungsanordnung in elektronischer Form von einem Diensteanbieter oder in seinem Auftrag gespeichert werden und aus gespeicherten Teilnehmerdaten, Zugangsdaten, Transaktionsdaten und Inhaltsdaten bestehen;

7. „Teilnehmerdaten“ alle Daten, die Folgendes betreffen:

a) die Identität eines Teilnehmers oder Kunden, wie der Name, das Geburtsdatum, die Postanschrift oder geografische Anschrift, Rechnungs- und Zahlungsdaten, die Telefonnummer oder die E-Mail-Adresse, die angegeben wurden;

b) die Art der Dienstleistung und ihre Dauer, einschließlich technischer Daten und 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 Passwörtern oder anderen Authentifizierungsmitteln, die anstelle eines Passworts verwendet werden –, die von einem Nutzer bereitgestellt oder auf Anfrage eines Nutzers erstellt werden;

8. „Zugangsdaten“ Daten über den Beginn und die Beendigung der Zugangssitzung eines Nutzers in Bezug auf einen Dienst, die ausschließlich zum Zweck der Identifizierung des Nutzers des Dienstes unbedingt erforderlich sind, wie das Datum und die Uhrzeit der Nutzung oder die Anmeldung bei und Abmeldung von dem Dienst, zusammen mit der IP-Adresse, die der Interzugangsanbieter dem Nutzer eines Dienstes zuweist, Daten zur Identifizierung der verwendeten Schnittstelle und der Nutzerkennung. Hierzu gehören auch elektronische Kommunikationsmetadaten

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

im Sinne des Artikels 4 Absatz 3 Buchstabe g der [Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation];

9. „Transaktionsdaten“ Daten über die Erbringung einer von einem Diensteanbieter angebotenen Dienstleistung, die Kontext- oder Zusatzinformationen über eine solche Dienstleistung liefern und von einem Informationssystem des Diensteanbieters generiert oder verarbeitet werden, beispielsweise Sende- und Empfangsdaten einer Nachricht oder einer anderen Art von Interaktion, Daten über den Standort des Geräts, Datum, Uhrzeit, Dauer, Größe, Route, Format, verwendetes Protokoll und Art der Kompression, sofern es sich bei diesen Daten nicht um Zugangsdaten handelt. Hierzu gehören auch elektronische Kommunikationsmetadaten im Sinne des Artikels 4 Absatz 3 Buchstabe g der [Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation];

10. „Inhaltsdaten“ alle in einem digitalen Format gespeicherten Daten wie Text, Sprache, Videos, Bilder und Tonaufzeichnungen, mit Ausnahme von Teilnehmer-, Zugangs- oder Transaktionsdaten;

11. „Informationssystem“ ein Informationssystem im Sinne des Artikels 2 Buchstabe a der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates[45];

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

13. „Vollstreckungsstaat“ den Mitgliedstaat, in dem der Adressat der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung ansässig oder niedergelassen 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 Vollstreckung 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 Vollstreckung übermittelt;

15. „Notfälle“ Situationen, in denen eine unmittelbare Gefahr für das Leben oder die körperliche Unversehrtheit einer Person oder für eine kritische Infrastruktur im Sinne des Artikels 2 Buchstabe a der Richtlinie 2008/114/EG des Rates[46] besteht.

Artikel 3
Anwendungsbereich

(1) Diese Verordnung gilt für Diensteanbieter, die Dienstleistungen in der Union anbieten.

---

45 Richtlinie 2013/40/EU 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).

46 Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (ABl. L 345 vom 23.12.2008, S. 75).

(2) Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen dürfen nur für 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 zur Herausgabe von Teilnehmerdaten und Zugangsdaten 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 Transaktionsdaten 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 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 und darf nur erlassen werden, wenn in einer vergleichbaren innerstaatlichen Situation im Anordnungsstaat für dieselbe Straftat eine ähnliche Maßnahme zur Verfügung stünde.

(3) Europäische Herausgabeanordnungen zur Herausgabe von Teilnehmer- oder Zugangsdaten können für alle Straftaten erlassen werden.

(4) Europäische Herausgabeanordnungen zur Herausgabe von Transaktions- oder Inhaltsdaten können nur erlassen werden

a) bei Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden, oder

b) bei den 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[47];

– Straftaten im Sinne der Artikel 3 bis 7 der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates[48];

– Straftaten im Sinne der Artikel 3 bis 8 der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates;

c) bei Straftaten im Sinne der Artikel 3 bis 12 und 14 der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates[49].

(5) Die Europäische Herausgabeanordnung enthält folgende Angaben:

---

47 Rahmenbeschluss 2001/413/JI des Rates vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (ABl. L 149 vom 2.6.2001, S. 1).

48 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).

49 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).

a) die Anordnungsbehörde und gegebenenfalls die validierende Behörde;

b) den Adressaten der Europäischen Herausgabeanordnung gemäß Artikel 7;

c) die Personen, deren Daten angefordert werden, es sei denn, der einzige Zweck der Anordnung besteht darin, eine Person zu identifizieren;

d) die Kategorie der angeforderten Daten (Teilnehmerdaten, Zugangsdaten, Transaktionsdaten oder Inhaltsdaten);

e) gegebenenfalls die Zeitspanne, für die die Herausgabe angefordert wird;

f) die anwendbaren Bestimmungen des Strafrechts des Anordnungsstaats;

g) in Notfällen oder bei Ersuchen um eine frühere Offenlegung die Gründe hierfür;

h) wenn die angeforderten Daten als Teil einer Infrastruktur gespeichert oder verarbeitet werden, die ein Diensteanbieter für ein Unternehmen oder eine Einrichtung, die keine natürlichen Personen sind, bereitstellt, eine Bestätigung, dass die Anordnung gemäß Absatz 6 erfolgt;

i) die Gründe für die Notwendigkeit und Verhältnismäßigkeit der Maßnahme.

(6) Wenn die angeforderten Daten als Teil einer Infrastruktur gespeichert oder verarbeitet werden, die ein Diensteanbieter für ein Unternehmen oder eine Einrichtung, die keine natürlichen Personen sind, bereitstellt, darf die Europäische Herausgabeanordnung nur dann an den Diensteanbieter gerichtet werden, wenn auf das Unternehmen oder die Einrichtung abzielende Ermittlungsmaßnahmen nicht geeignet sind, insbesondere weil sie die Ermittlung beeinträchtigen könnten.

(7) Wenn die Anordnungsbehörde Grund zu der Annahme hat, dass angeforderte Transaktions- oder Inhaltsdaten 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 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 konsultiert. Stellt die Anordnungsbehörde fest, dass die angeforderten Zugangs-, Transaktions- oder Inhaltsdaten 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. Europäische Sicherungsanordnungen zur Sicherung von Daten können für alle Straftaten erlassen werden.

(3) Die Europäische Sicherungsanordnung enthält folgende Angaben:

a) die Anordnungsbehörde und gegebenenfalls die validierende Behörde;

b) den Adressaten der Europäischen Sicherungsanordnung gemäß Artikel 7;

c) die Personen, deren Daten gesichert werden sollen, es sei denn, der einzige Zweck der Anordnung besteht darin, eine Person zu identifizieren;

d) die Kategorie der zu sichernden Daten (Teilnehmerdaten, Zugangsdaten, Transaktionsdaten oder Inhaltsdaten);

e) gegebenenfalls die Zeitspanne, für die die Sicherung angefordert wird;

f) die anwendbaren Bestimmungen des Strafrechts des Anordnungsstaats;

g) die Gründe für die Notwendigkeit und Verhältnismäßigkeit der Maßnahme.

Artikel 7

Adressat einer Europäischen Herausgabeanordnung und einer Europäischen Sicherungsanordnung

(1) Die Europäische Herausgabeanordnung und die Europäische Sicherungsanordnung werden direkt an einen Vertreter gerichtet, den der Diensteanbieter zum Zweck der Beweismittelerhebung in Strafverfahren benannt hat.

(2) Wenn kein Vertreter zu diesem Zweck benannt wurde, können die Europäische Herausgabeanordnung und die Europäische Sicherungsanordnung an eine beliebige Niederlassung des Diensteanbieters in der Union gerichtet werden.

(3) Wenn der Vertreter einem EPOC in einem Notfall gemäß Artikel 9 Absatz 2 nicht Folge leistet, kann das EPOC an eine beliebige Niederlassung des Diensteanbieters in der Union gerichtet werden.

(4) Wenn der Vertreter seinen Verpflichtungen aus Artikel 9 oder 10 nicht nachkommt und die Anordnungsbehörde der Auffassung ist, dass ein erhebliches Risiko eines Datenverlusts besteht, können die Europäische Herausgabeanordnung oder die Europäische Sicherungsanordnung an eine beliebige Niederlassung des Diensteanbieters in der Union gerichtet werden.

Artikel 8

Zertifikate über eine Europäische Herausgabe- oder Sicherungsanordnung

(1) Eine Europäische Herausgabe- oder Sicherungsanordnung wird dem Adressaten nach Artikel 7 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 und in einer Form, die einen schriftlichen Nachweis unter Bedingungen ermöglicht, die dem Adressaten die Feststellung der Echtheit gestatten.

Wenn Diensteanbieter, Mitgliedstaaten oder Einrichtungen der Union spezielle Plattformen oder andere sichere Kanäle für die Bearbeitung von Datenersuchen von Strafverfolgungs- und Justizbehörden eingerichtet haben, kann die Anordnungsbehörde das Zertifikat auch über diese Kanäle übermitteln.

(3) Das EPOC enthält die in Artikel 5 Absatz 5 Buchstaben a bis h aufgeführten Angaben, einschließlich ausreichender Informationen, um dem Adressaten die Feststellung der Anordnungsbehörde und die Kontaktaufnahme mit dieser zu ermöglichen. Die Gründe für die Notwendigkeit und Verhältnismäßigkeit der Maßnahme oder nähere Angaben zu den Ermittlungen dürfen nicht enthalten sein.

(4) Das EPOC-PR enthält die in Artikel 6 Absatz 3 Buchstaben a bis f aufgeführten Angaben, einschließlich ausreichender Informationen, um dem Adressaten die Feststellung der Anordnungsbehörde und die Kontaktaufnahme mit dieser zu ermöglichen. Die Gründe für die Notwendigkeit und Verhältnismäßigkeit der Maßnahme oder nähere Angaben zu den Ermittlungen dürfen nicht enthalten sein.

(5) Im Bedarfsfall sind das EPOC oder das EPOC-PR in eine vom Adressaten akzeptierte Amtssprache der Union zu übersetzen. Wurde keine Sprache angegeben, so werden das EPOC oder das EPOC-PR in eine der Amtssprachen des Mitgliedstaats übersetzt, in dem der Vertreter ansässig oder niedergelassen ist.

Artikel 9
Ausführung eines EPOC

(1) Nach Erhalt des EPOC sorgt der Adressat dafür, dass die angeforderten Daten spätestens innerhalb von zehn Tagen nach Erhalt des EPOC direkt an die Anordnungsbehörde oder die Strafverfolgungsbehörden gemäß den Angaben im EPOC übermittelt werden, es sei denn, die Anordnungsbehörde gibt Gründe für eine frühere Offenlegung an.

(2) In Notfällen übermittelt der Adressat die angeforderten Daten unverzüglich, spätestens jedoch innerhalb von sechs Stunden nach Erhalt des EPOC.

(3) Wenn der Adressat seiner Verpflichtung nicht nachkommen kann, weil das EPOC unvollständig ist, offensichtliche Fehler enthält oder keine ausreichenden Informationen zur Ausführung des EPOC enthält, setzt er die im EPOC angegebene Anordnungsbehörde unverzüglich hiervon in Kenntnis und bittet unter Verwendung des Formulars in Anhang III um Klarstellung. Er teilt der Anordnungsbehörde mit, ob eine Identifizierung und Sicherung gemäß Absatz 6 möglich war. 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.

(4) Wenn der Adressat seiner Verpflichtung aufgrund höherer Gewalt oder einer faktischen Unmöglichkeit, die nicht dem Adressaten oder, falls abweichend, dem Diensteanbieter angelastet werden kann, nicht nachkommen kann, unter anderem weil die Person, deren Daten angefordert werden, kein Kunde des Adressaten beziehungsweise des Diensteanbieters ist oder weil die Daten vor Erhalt des EPOC gelöscht wurden, setzt der Adressat die im EPOC angegebene Anordnungsbehörde 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.

(5) In allen Fällen, in denen der Adressat die angeforderten Informationen aus anderen Gründen überhaupt nicht, nicht vollständig oder nicht fristgerecht bereitstellt, informiert er die Anordnungsbehörde 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 setzt gegebenenfalls eine neue Frist für die Herausgabe der Daten durch den Diensteanbieter fest.

Ist der Adressat der Ansicht, dass das EPOC nicht ausgeführt werden kann, weil ausschließlich aus den in dem EPOC enthaltenen Informationen hervorgeht, dass es offenkundig gegen die Charta der Grundrechte der Europäischen Union verstößt oder offensichtlich missbräuchlich ist, so übermittelt er das Formular in Anhang III auch der zuständigen Vollstreckungsbehörde im Mitgliedstaat des Adressaten. In diesen Fällen kann die zuständige Vollstreckungsbehörde die Anordnungsbehörde entweder direkt oder über Eurojust oder das Europäische Justizielle Netz um Klarstellungen zu der Europäischen Herausgabeanordnung ersuchen.

(6) Der Adressat sichert die angeforderten Daten, wenn er sie nicht unverzüglich herausgibt, es sei denn, er kann die angeforderten Daten nicht anhand der Angaben im EPOC identifizieren; in diesem Fall ersucht er um Klarstellung gemäß Absatz 3. Die Daten werden so lange gesichert, bis sie herausgegeben werden, unabhängig davon, ob dies auf der Grundlage der klargestellten Europäischen Herausgabeanordnung und dem dazugehörigen Zertifikat oder über andere Kanäle wie die Rechtshilfe erfolgt. Wenn die Herausgabe und Sicherung von Daten nicht mehr erforderlich ist, setzen die Anordnungsbehörde und gegebenenfalls gemäß Artikel 14 Absatz 8 die Vollstreckungsbehörde den Adressaten unverzüglich hiervon in Kenntnis.

Artikel 10
Ausführung eines EPOC-PR

(1) Nach Erhalt des EPOC-PR sichert der Adressat unverzüglich die angeforderten Daten. Die Sicherung endet nach 60 Tagen, es sei denn, die Anordnungsbehörde bestätigt, dass das entsprechende Ersuchen um Herausgabe in die Wege geleitet wurde.

(2) Wenn die Anordnungsbehörde innerhalb der in Absatz 1 genannten Frist bestätigt, dass das entsprechende 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.

(3) Wenn die Sicherung nicht mehr erforderlich ist, setzt die Anordnungsbehörde den Adressaten unverzüglich hiervon in Kenntnis.

(4) Wenn der Adressat seiner Verpflichtung nicht nachkommen kann, weil das Zertifikat unvollständig ist, offensichtliche Fehler enthält oder keine ausreichenden Informationen zur Ausführung des EPOC-PR enthält, setzt er die im EPOC-PR angegebene Anordnungsbehörde unverzüglich hiervon in Kenntnis und bittet unter Verwendung des Formulars in Anhang III um Klarstellung. Die Anordnungsbehörde reagiert umgehend, spätestens jedoch innerhalb von fünf Tagen. Der Adressat stellt sicher, dass die erforderliche Klarstellung auf seiner Seite entgegengenommen werden kann, damit er seiner Verpflichtung gemäß Absatz 1 nachkommen kann.

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

(6) In allen Fällen, in denen der Adressat die angeforderten Informationen aus anderen im Formular in Anhang III aufgeführten Gründen nicht sichert, setzt er die Anordnungsbehörde 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.

Artikel 11
Vertraulichkeit und Nutzerinformationen

(1) Adressaten und, falls abweichend, Diensteanbieter treffen die erforderlichen Maßnahmen, um die Vertraulichkeit des EPOC oder des EPOC-PR sowie der herausgegebenen und gesicherten Daten zu gewährleisten, und sehen auf Aufforderung der Anordnungsbehörde davon ab, die Person, deren Daten angefordert werden, hiervon in Kenntnis zu setzen, um das betreffende Strafverfahren nicht zu behindern.

(2) Wenn die Anordnungsbehörde den Adressaten aufgefordert hat, die Person, deren Daten angefordert werden, nicht hiervon in Kenntnis zu setzen, unterrichtet die Anordnungsbehörde die Person, deren Daten mit dem EPOC angefordert wurden, ohne unnötige Verzögerung über die Herausgabe der Daten. Diese Unterrichtung kann 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 12
Kostenerstattung

Der Diensteanbieter kann eine Erstattung seiner Kosten durch den Anordnungsstaat geltend machen, wenn dies nach den nationalen Rechtsvorschriften des Anordnungsstaats für innerstaatliche Anordnungen in ähnlichen Situationen vorgesehen ist; die Erstattung erfolgt nach Maßgabe dieser nationalen Bestimmungen.

Kapitel 3: Sanktionen und Vollstreckung

Artikel 13
Sanktionen

Unbeschadet nationaler Rechtsvorschriften, die die Verhängung strafrechtlicher Sanktionen vorsehen, erlassen die Mitgliedstaaten Vorschriften über finanzielle Sanktionen, die bei

Verstößen gegen die Verpflichtungen aus den Artikeln 9, 10 und 11 zu verhängen sind, und treffen alle für die Anwendung finanzieller Sanktionen erforderlichen Maßnahmen. Die vorgesehenen finanziellen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen sowie diesbezügliche spätere Änderungen unverzüglich mit.

Artikel 14
Vollstreckungsverfahren

(1) Leistet der Adressat ohne Angabe von Gründen, die von der Anordnungsbehörde akzeptiert werden, einem EPOC nicht fristgerecht oder einem EPOC-PR nicht Folge, so kann die Anordnungsbehörde der zuständigen Behörde im Vollstreckungsstaat Folgendes übermitteln: die Europäische Herausgabeanordnung mit dem EPOC oder die Europäische Sicherungsanordnung mit dem EPOC-PR sowie das vom Adressaten ausgefüllte Formular in Anhang III und alle sonstigen einschlägigen Dokumente im Hinblick auf ihre Vollstreckung in einer Form, die einen schriftlichen Nachweis unter Bedingungen ermöglicht, die der Vollstreckungsbehörde die Feststellung der Echtheit gestatten. Zu diesem Zweck übersetzt die Anordnungsbehörde die Anordnung, das Formular und alle sonstigen zugehörigen Dokumente in eine der Amtssprachen des betreffenden Mitgliedstaats und setzt den Adressaten von der Übermittlung in Kenntnis.

(2) Nach dem Erhalt erkennt die Vollstreckungsbehörde eine gemäß Absatz 1 übermittelte Europäische Herausgabeanordnung oder Europäische Sicherungsanordnung ohne weitere Formalitäten an und ergreift die zu ihrer Vollstreckung erforderlichen Maßnahmen, es sei denn, die Vollstreckungsbehörde ist der Auffassung, dass einer der in den Absätzen 4 oder 5 genannten Gründe zutrifft oder dass die betreffenden Daten durch Immunitäten oder Vorrechte nach nationalem Recht geschützt sind oder dass ihre Offenlegung Auswirkungen auf grundlegende Interessen wie die nationale Sicherheit und Verteidigung haben könnte. Die Vollstreckungsbehörde beschließt die Anerkennung der Anordnung unverzüglich, spätestens jedoch fünf Arbeitstage nach Erhalt der Anordnung.

(3) Wenn die Vollstreckungsbehörde die Anordnung anerkennt, fordert sie den Adressaten förmlich auf, der entsprechenden Verpflichtung nachzukommen, und setzt ihn davon, dass er unter Geltendmachung der in den Absätzen 4 oder 5 aufgeführten Gründe die Vollstreckung ablehnen kann, sowie von den bei Nichtbefolgung anwendbaren Sanktionen in Kenntnis und legt eine Frist für die Befolgung oder Ablehnung fest.

(4) Der Adressat kann die Vollstreckung der Europäischen Herausgabeanordnung nur aus folgenden Gründen ablehnen:

a) Die Europäische Herausgabeanordnung wurde nicht von einer Anordnungsbehörde nach Artikel 4 erlassen oder validiert;

b) die Europäische Herausgabeanordnung wurde nicht wegen einer Straftat nach Artikel 5 Absatz 4 erlassen;

c) der Adressat konnte dem EPOC nicht Folge leisten, weil dies faktisch oder aufgrund höherer Gewalt nicht möglich war oder weil das EPOC offensichtliche Fehler enthält;

d) die Europäische Herausgabeanordnung betrifft keine Daten, die zum Zeitpunkt des Erhalts des EPOC von einem Diensteanbieter oder in dessen Auftrag gespeichert wurden;

e) die Dienstleistung fällt nicht unter diese Verordnung;

f) ausschließlich aus den in dem EPOC enthaltenen Informationen geht hervor, dass das EPOC offenkundig gegen die Charta verstößt oder offensichtlich missbräuchlich ist.

(5) Der Adressat kann die Vollstreckung der Europäischen Sicherungsanordnung nur aus folgenden Gründen ablehnen:

a) Die Europäische Sicherungsanordnung wurde nicht von einer Anordnungsbehörde nach Artikel 4 erlassen oder validiert;

b) der Diensteanbieter konnte dem EPOC-PR nicht Folge leisten, weil dies faktisch oder aufgrund höherer Gewalt nicht möglich war oder weil das EPOC-PR offensichtliche Fehler enthält;

c) die Europäische Sicherungsanordnung betrifft keine Daten, die zum Zeitpunkt des Erhalts des EPOC-PR von einem Diensteanbieter oder in dessen Auftrag gespeichert wurden;

d) die Dienstleistung fällt nicht unter diese Verordnung;

e) ausschließlich aus den in dem EPOC-PR enthaltenen Informationen geht hervor, dass das EPOC-PR offenkundig gegen die Charta verstößt oder offensichtlich missbräuchlich ist.

(6) Erhebt der Adressat Einwände, entscheidet die Vollstreckungsbehörde auf der Grundlage der von dem Adressaten bereitgestellten Informationen und erforderlichenfalls der von der Anordnungsbehörde gemäß Absatz 7 erhaltenen zusätzlichen Informationen, ob sie die Anordnung vollstreckt.

(7) Bevor die Vollstreckungsbehörde beschließt, die Anordnung gemäß den Absätzen 2 und 6 nicht anzuerkennen oder nicht zu vollstrecken, konsultiert sie in geeigneter Weise die Anordnungsbehörde. Gegebenenfalls ersucht sie die Anordnungsbehörde um weitere Auskünfte. Die Anordnungsbehörde beantwortet ein solches Ersuchen innerhalb von fünf Arbeitstagen.

(8) Alle Beschlüsse sind der Anordnungsbehörde und dem Adressaten unverzüglich in einer Form, die einen schriftlichen Nachweis ermöglicht, mitzuteilen.

(9) Erhält die Vollstreckungsbehörde die Daten von dem Adressaten, so übermittelt sie diese innerhalb von zwei Arbeitstagen der Anordnungsbehörde, es sei denn, die betreffenden Daten sind durch Immunitäten oder Vorrechte nach innerstaatlichem Recht geschützt oder haben Auswirkungen auf grundlegende Interessen wie die nationale Sicherheit und Verteidigung. In diesem Fall teilt sie der Anordnungsbehörde die Gründe für die Nichtübermittlung der Daten mit.

(10) Kommt der Adressat seinen Verpflichtungen aus einer anerkannten Anordnung, deren Vollstreckbarkeit von der Vollstreckungsbehörde bestätigt wurde, nicht nach, so verhängt diese Behörde eine finanzielle Sanktion nach Maßgabe des nationalen Rechts. Gegen den Beschluss zur Verhängung einer finanziellen Sanktion kann ein wirksamer Rechtsbehelf eingelegt werden.

Kapitel 4: Rechtsbehelfe

Artikel 15
Überprüfungsverfahren bei einander widersprechenden Verpflichtungen aufgrund der Grundrechte oder der grundlegenden Interessen eines Drittstaats

(1) Ist der Adressat der Ansicht, dass die Befolgung einer Europäischen Herausgabeanordnung im Widerspruch zu den geltenden Rechtsvorschriften eines Drittstaats stehen würde, welche die Offenlegung der betreffenden Daten mit der Begründung verbieten, dass dies zum Schutz der Grundrechte der betroffenen Personen oder der grundlegenden Interessen des Drittstaats im Zusammenhang mit der nationalen Sicherheit oder Verteidigung notwendig ist, so teilt er der Anordnungsbehörde gemäß dem Verfahren des Artikels 9 Absatz 5 seine Gründe für die Nichtausführung der Europäischen Herausgabeanordnung mit.

(2) Der begründete Einwand muss alle sachdienlichen Angaben zu den betreffenden Rechtsvorschriften des Drittstaats, zu ihrer Anwendbarkeit auf den vorliegenden Fall und zur Art der einander widersprechenden Verpflichtungen enthalten. Er darf sich nicht darauf stützen, dass in den geltenden Rechtsvorschriften des Drittstaats keine vergleichbaren Bestimmungen über die Bedingungen, Formvorschriften und Verfahren für den Erlass einer Herausgabeanordnung existieren, und auch nicht allein darauf, dass die Daten in einem Drittstaat gespeichert sind.

(3) Die Anordnungsbehörde überprüft die Europäische Herausgabeanordnung auf der Grundlage des begründeten Einwands. Beabsichtigt die Anordnungsbehörde, die Europäische Herausgabeanordnung aufrechtzuerhalten, so beantragt sie eine Überprüfung durch das zuständige Gericht des betreffenden Mitgliedstaats. Die Ausführung der Anordnung wird bis zum Abschluss des Überprüfungsverfahrens ausgesetzt.

Das zuständige Gericht beurteilt zunächst, ob ein Widerspruch vorliegt, und prüft dazu, ob

a) die Rechtsvorschriften des Drittstaats angesichts der besonderen Umstände des betreffenden Falls Anwendung finden, und wenn ja,

b) die Rechtsvorschriften des Drittstaats, wenn sie auf die besonderen Umstände des betreffenden Falls angewandt werden, die Offenlegung der betreffenden Daten verbieten.

(4) Bei dieser Beurteilung sollte das Gericht berücksichtigen, ob die betreffenden Rechtsvorschriften des Drittstaats nicht weniger dem Schutz der Grundrechte oder der grundlegenden Interessen des Drittstaats im Zusammenhang mit der nationalen Sicherheit oder Verteidigung dienen, sondern vielmehr offensichtlich darauf abzielen, andere Interessen zu schützen, oder dazu genutzt werden, rechtswidrige Handlungen vor Ersuchen von Strafverfolgungsbehörden im Rahmen strafrechtlicher Ermittlungen abzuschirmen.

(5) Stellt das zuständige Gericht fest, dass kein relevanter Widerspruch im Sinne der Absätze 1 und 4 vorliegt, so erhält es die Anordnung aufrecht. Stellt das zuständige Gericht fest, dass ein relevanter Widerspruch im Sinne der Absätze 1 und 4 vorliegt, so übermittelt das zuständige Gericht den zentralen Behörden des betreffenden Drittstaats über seine nationale zentrale Behörde alle sachdienlichen faktischen und rechtlichen Informationen zu dem Fall, einschließlich seiner Beurteilung, wobei es

eine Antwortfrist von 15 Tagen festsetzt. Auf begründeten Antrag der zentralen Behörde des Drittstaats kann die Frist um 30 Tage verlängert werden.

(6) Setzt die zentrale Behörde des Drittstaats innerhalb der Frist das zuständige Gericht davon in Kenntnis, dass sie Einwände gegen die Ausführung der Europäischen Herausgabeanordnung in dem betreffenden Fall hat, so hebt das zuständige Gericht die Anordnung auf und teilt dies der Anordnungsbehörde und dem Adressaten mit. Gehen innerhalb der (verlängerten) Frist keine Einwände ein, so übermittelt das zuständige Gericht ein Erinnerungsschreiben, in dem der zentralen Behörde des Drittstaats fünf weitere Tage für die Antwort eingeräumt werden und sie auf die Folgen einer Nichtbeantwortung hingewiesen wird. Gehen innerhalb dieser zusätzlichen Frist keine Einwände ein, so erhält das zuständige Gericht die Anordnung aufrecht.

(7) Stellt das zuständige Gericht fest, dass die Anordnung aufrechtzuerhalten ist, so teilt es dies der Anordnungsbehörde und dem Adressaten mit, der sodann die Anordnung ausführen muss.

Artikel 16
Überprüfungsverfahren bei einander widersprechenden Verpflichtungen aus anderen Gründen

(1) Ist der Adressat der Ansicht, dass die Befolgung einer Europäischen Herausgabeanordnung im Widerspruch zu den geltenden Rechtsvorschriften eines Drittstaats stehen würde, welche die Offenlegung der betreffenden Daten aus anderen als den in Artikel 15 genannten Gründen verbieten, so teilt er der Anordnungsbehörde gemäß dem Verfahren des Artikels 9 Absatz 5 seine Gründe für die Nichtausführung der Europäischen Herausgabeanordnung mit.

(2) Der begründete Einwand muss alle sachdienlichen Angaben zu den betreffenden Rechtsvorschriften des Drittstaats, zu ihrer Anwendbarkeit auf den vorliegenden Fall und zur Art der einander widersprechenden Verpflichtungen enthalten. Er darf sich nicht darauf stützen, dass in den geltenden Rechtsvorschriften des Drittstaats keine vergleichbaren Bestimmungen über die Bedingungen, Formvorschriften und Verfahren für den Erlass einer Herausgabeanordnung existieren, und auch nicht allein darauf, dass die Daten in einem Drittstaat gespeichert sind.

(3) Die Anordnungsbehörde überprüft die Europäische Herausgabeanordnung auf der Grundlage des begründeten Einwands. Beabsichtigt die Anordnungsbehörde, die Europäische Herausgabeanordnung aufrechtzuerhalten, so beantragt sie eine Überprüfung durch das zuständige Gericht des betreffenden Mitgliedstaats. Die Ausführung der Anordnung wird bis zum Abschluss des Überprüfungsverfahrens ausgesetzt.

(4) Das zuständige Gericht beurteilt zunächst, ob ein Widerspruch vorliegt, und prüft dazu, ob

a) die Rechtsvorschriften des Drittstaats angesichts der besonderen Umstände des betreffenden Falls Anwendung finden, und wenn ja,

b) die Rechtsvorschriften des Drittstaats, wenn sie auf die besonderen Umstände des betreffenden Falls angewandt werden, die Offenlegung der betreffenden Daten verbieten.

(5) Stellt das zuständige Gericht fest, dass kein relevanter Widerspruch im Sinne der Absätze 1 und 4 vorliegt, so erhält es die Anordnung aufrecht. Stellt das zuständige Gericht fest, dass die Rechtsvorschriften des Drittstaats, wenn sie auf die besonderen Umstände des betreffenden Falls angewandt werden, die Offenlegung der betreffenden Daten verbieten, so entscheidet es, ob die Anordnung aufrechtzuerhalten oder zurückzuziehen ist, und stützt sich dabei insbesondere auf folgende Faktoren:

a) das nach den einschlägigen Rechtsvorschriften des Drittstaats geschützte Interesse, einschließlich des Interesses des Drittstaats an der Verhinderung der Offenlegung der Daten;

b) den Grad der Verbindung der Strafsache, wegen der die Anordnung erlassen wurde, zu einem der beiden Rechtssysteme; hierfür maßgeblich sind unter anderem:

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

der Ort, an dem die betreffende Straftat begangen wurde;

c) den Grad der Verbindung zwischen dem Diensteanbieter und dem betreffenden Drittstaat; in diesem Zusammenhang wird durch den Datenspeicherort allein kein wesentlicher Verbindungsgrad bewirkt;

d) das Interesse des ermittelnden Staates an der Einholung der betreffenden Beweismittel aufgrund der Schwere der Straftat und der Bedeutung einer zügigen Beweiserhebung;

e) die möglichen Konsequenzen der Befolgung der Europäischen Herausgabeanordnung für den Adressaten oder den Diensteanbieter, einschließlich der möglicherweise zu verhängenden Sanktionen.

(6) Beschließt das zuständige Gericht, die Anordnung aufzuheben, so teilt es dies der Anordnungsbehörde und dem Adressaten mit. Stellt das zuständige Gericht fest, dass die Anordnung aufrechtzuerhalten ist, so teilt es dies der Anordnungsbehörde und dem Adressaten mit, der sodann die Anordnung ausführen muss.

Artikel 17
Wirksame Rechtsbehelfe

(1) Verdächtige und Beschuldigte, deren Daten im Wege einer Europäischen Herausgabeanordnung eingeholt wurden, haben unbeschadet der nach der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 verfügbaren Rechtsbehelfe das Recht, während des Strafverfahrens, für das die Anordnung erlassen wurde, wirksame Rechtsbehelfe gegen die Europäische Herausgabeanordnung einzulegen.

(2) Handelt es sich bei der Person, deren Daten eingeholt wurden, nicht um einen Verdächtigen oder Beschuldigten in einem Strafverfahren, für das die Anordnung erlassen wurde, so hat der Betreffende unbeschadet der nach der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 verfügbaren Rechtsbehelfe das Recht, im Anordnungsstaat wirksame Rechtsbehelfe gegen die Europäische Herausgabeanordnung einzulegen.

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

(4) Unbeschadet des Artikels 11 ergreift die Anordnungsbehörde die geeigneten Maßnahmen, um zu gewährleisten, dass Informationen über die nach nationalem Recht bestehenden Möglichkeiten zur Einlegung von Rechtsbehelfen 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) Unbeschadet der nationalen Verfahrensvorschriften stellen die Mitgliedstaaten sicher, dass in einem Strafverfahren im Anordnungsstaat bei der Bewertung der mittels einer Europäischen Herausgabeanordnung eingeholten Beweismittel die Verteidigungsrechte gewahrt werden und ein faires Verfahren gewährleistet wird.

Artikel 18

Gewährleistung von Immunitäten und Vorrechten nach dem Recht des Vollstreckungsstaats

Wenn die durch die Europäische Herausgabeanordnung eingeholten Transaktions- oder Inhaltsdaten durch Immunitäten oder Vorrechte nach dem Recht des Mitgliedstaats des Adressaten geschützt sind oder sich auf grundlegende Interessen dieses Mitgliedstaats wie die nationale Sicherheit und Verteidigung auswirken, stellt das Gericht des Anordnungsstaats bei der Prüfung der Relevanz und der Zulässigkeit der betreffenden Beweismittel während des Strafverfahrens, für das die Anordnung erlassen wurde, sicher, dass diese Gründe genauso berücksichtigt werden als wären sie im nationalem Recht vorgesehen. Das Gericht kann die Behörden des betreffenden Mitgliedstaats, das Europäische Justizielle Netz für Strafsachen oder Eurojust konsultieren.

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 Nachweise 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 Nachweise 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, der Diensteanbieter, an die sie gerichtet wurden, und der jeweiligen Situation (Notfall oder nicht);

b) die Zahl der EPOC, denen Folge geleistet und denen nicht Folge geleistet wurde, aufgeschlüsselt nach der Art der angeforderten Daten, der Diensteanbieter, an die sie gerichtet wurden, und der jeweiligen Situation (Notfall oder nicht);

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, der Diensteanbieter, an die die EPOC gerichtet wurden, und der jeweiligen Situation (Notfall oder nicht);

d) die Zahl der zwecks Vollstreckung einem Vollstreckungsstaat übermittelten und von diesem entgegengenommenen Europäischen Herausgabeanordnungen, aufgeschlüsselt nach der Art der angeforderten Daten, der Diensteanbieter, an die sie gerichtet wurden, und der jeweiligen Situation (Notfall oder nicht), sowie die Zahl solcher Anordnungen, denen Folge geleistet wurde;

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

Artikel 20
Änderungen der Zertifikate und Formulare

Die Kommission erlässt gemäß Artikel 21 delegierte Rechtsakte zur Änderung der Anhänge I, II und III, um einem etwaigen Verbesserungsbedarf hinsichtlich des Inhalts der EPOC- und der EPOC-PR-Formulare sowie der Formulare für die Übermittlung von Informationen über die Unmöglichkeit der Ausführung eines EPOC oder eines EPOC-PR wirksam zu entsprechen.

Artikel 21
Ausübung der Befugnisübertragung

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

(2) Die Befugnisübertragung gemäß Artikel 20 ist unbefristet und gilt ab dem *[Tag des Geltungsbeginns dieser Verordnung]*.

(3) Die Befugnisübertragung gemäß Artikel 20 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der

Interinstitutionellen Vereinbarung über bessere Rechtsetzung vom 13. April 2016[50] festgelegten Grundsätzen.

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

(6) Ein delegierter Rechtsakt, der gemäß Artikel 20 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 22
Mitteilungen

(1) Jeder Mitgliedstaat teilt der Kommission bis zum *[Tag des Geltungsbeginns 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(n), die befugt ist (sind), im Namen eines anderen Mitgliedstaats Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen zu vollstrecken;

c) die Gerichte, die befugt sind, sich mit begründeten Einwänden von Adressaten gemäß den Artikeln 15 und 16 zu befassen.

(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, auf die Artikel 9 des Beschlusses 2008/976/JI des Rates[51] Bezug nimmt, öffentlich zugänglich.

Artikel 23
Bezug zu Europäischen Ermittlungsanordnungen

Die Behörden der Mitgliedstaaten können weiterhin Europäische Ermittlungsanordnungen im Einklang mit der Richtlinie 2014/41/EU für die Erhebung von Beweismitteln erlassen, die auch unter diese Verordnung fallen würden.

Artikel 24
Bewertung

Spätestens am *[fünf 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 auch geprüft wird, ob ihr Anwendungsbereich erweitert werden muss. Erforderlichenfalls

[50] ABl. L 123 vom 12.5.2016, S. 13.

[51] Beschluss 2008/976/JI des Rates vom 16. Dezember 2008 über das Europäische Justizielle Netz (ABl. L 348 vom 24.12.2008, S. 130).

werden dem Bericht Legislativvorschläge 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 … *[sechs Monate nach ihrem Inkrafttreten]*.

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

Geschehen zu Brüssel am […]

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

EUROPÄISCHE
KOMMISSION

Straßburg, den 17.4.2018
COM(2018) 225 final

ANNEXES 1 to 3

ANHÄNGE

zum

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates

über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen

{SWD(2018) 118 final} - {SWD(2018) 119 final}

ANHANG I

ZERTIFIKAT ÜBER EINE EUROPÄISCHE HERAUSGABEANORDNUNG (EPOC) ZUR

HERAUSGABE ELEKTRONISCHER BEWEISMITTEL

Gemäß der Verordnung (EU)...[1] muss der Adressat des Zertifikats über eine Europäische Herausgabeanordnung (EPOC) das EPOC ausführen und der unter Abschnitt G Ziffer i des EPOC genannten Behörde die angeforderten Daten übermitteln. 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.

Der Adressat trifft 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).

Adressat:…….……..…

ABSCHNITT B: Fristen

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

□ spätestens binnen 10 Tagen

□ spätestens binnen 6 Stunden in einem Notfall aufgrund:

□ einer unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit einer Person. Begründung, falls erforderlich:

…….

□ einer unmittelbaren Gefahr für eine kritische Infrastruktur im Sinne des Artikels 2 Buchstabe a der Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

□ binnen einer anderen Frist (bitte angeben): ……..….. aus folgendem Grund:

□ unmittelbare Gefahr, dass die angeforderten Daten gelöscht werden
□ andere dringende Ermittlungsmaßnahmen
□ unmittelbar anstehendes Gerichtsverfahren
□ Verdächtiger oder Beschuldigter in Untersuchungshaft
□ sonstige Gründe: …….....

[1] Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (*ABl. L...*).

ABSCHNITT C: Nutzerinformationen

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

□ der Adressat **die Person,** deren Daten mit dem EPOC angefordert werden, **hiervon nicht in Kenntnis setzen darf**.

ABSCHNITT D: Herauszugebende elektronische Beweismittel

i) Dieses EPOC betrifft (Zutreffendes bitte ankreuzen):

□ Teilnehmerdaten, die zumindest Folgendes umfassen:

□ 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, IP-Adresse, 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

□ Debit- oder Kreditkarteninformationen (die vom Nutzer zu Abrechnungszwecken bereitgestellt wurden), einschließlich anderer Zahlungsmittel

□ PUK-Codes

□ Zugangsdaten, die zumindest Folgendes umfassen:

□ IP-Verbindungsdaten/-protokolle zu Identifizierungszwecken

□ Transaktionsdaten

□ Verkehrsdaten, die zumindest Folgendes umfassen:

a) für (Mobil-)Telefonie

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

□ Verbindungszeit und -dauer

□ 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, E-Mail-Header-Informationen, 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 Transaktionsdaten, die zumindest Folgendes umfassen:

□ Historie über Prepaid-Aufladevorgänge
□ Kontaktliste

□ Inhaltsdaten, die zumindest Folgendes umfassen:

□ (Web-)Mailbox-Dump
□ Online-Storage-Dump (vom Nutzer generierte Daten)
□ Pagedump
□ Message log/Backup
□ Voicemail-Dump
□ Server-Inhalte
□ Geräte-Backup

ii) Die nachstehenden Informationen werden Ihnen zur Ausführung des EPOC zur Verfügung gestellt:

□ IP-Adresse:…….
□ Telefonnummer:…….
□ E-Mail-Adresse:…….....
□ IMEI-Nummer:……..
□ MAC-Adresse:……...
□ Person(en), deren Daten angefordert werden:…….……..
□ Name des Dienstes: ……...
□ Sonstiges: …….

iii) gegebenenfalls 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 Diensteanbieter/Vertreter/Behörde angeben, an den/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 Transaktions- 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 werden;

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

□ 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- und Zugangsdaten)

□ Staatsanwalt (für Transaktions- 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 hat

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

□ Richter, Gericht oder Ermittlungsrichter
□ Staatsanwalt (für Teilnehmer- und Zugangsdaten)

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 SICHERUNGSEANORDNUNG (EPOC-PR) ZUR SICHERUNG ELEKTRONISCHER BEWEISMITTEL

Gemäß der Verordnung (EU)...[2] muss der Empfänger des Zertifikats über eine Europäische Sicherungsanordnung (EPOC-PR) unverzüglich nach Erhalt des EPOC-PR die angeforderten Daten sichern. 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.

Der Empfänger trifft 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).

Adressat:…….……..…..…

ABSCHNITT B: Nutzerinformationen

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

□ der Adressat **die Person,** deren Daten mit dem EPOC-PR angefordert werden, **nicht hiervon in Kenntnis setzen darf**.

ABSCHNITT C: Zu sichernde elektronische Beweismittel

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

□ Teilnehmerdaten, die zumindest Folgendes umfassen:

□ 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, IP-Adresse, SIM-Kartennummer, MAC-Adresse) und zugehörige(s) Gerät/Geräte

□ Angaben zum Profil (Nutzername, Profilbild)

[2] Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (*ABl. L...).*

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

□ Debit- oder Kreditkarteninformationen (die vom Nutzer zu Abrechnungszwecken bereitgestellt wurden), einschließlich anderer Zahlungsmittel

□ PUK-Codes

□ Zugangsdaten, die zumindest Folgendes umfassen:

□ IP-Verbindungsdaten/-protokolle zu Identifizierungszwecken

□ Transaktionsdaten:

□ Verkehrsdaten, die zumindest Folgendes umfassen:

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, E-Mail-Header-Informationen, 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 Transaktionsdaten, die zumindest Folgendes umfassen:

□ Historie über Prepaid-Aufladevorgänge

□ Kontaktliste

□ Inhaltsdaten, die zumindest Folgendes umfassen:

□ (Web-)Mailbox-Dump

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

□ Page-Dump

□ Message log/Backup

□ Voicemail-Dump

□ Server-Inhalte

□ Geräte-Backup

ii) Die nachstehenden Informationen werden Ihnen zur Ausführung des EPOC-PR Verfügung gestellt:

□ IP-Adresse:……..

- □ Telefonnummer:……..…..….
- □ E-Mail-Adresse:……...…...
- □ IMEI-Nummer:…….…...
- □ MAC-Adresse:…….
- □ Person(en), deren Daten angefordert werden:……..……..
- □ Name des Dienstes:……..
- □ Sonstiges:…….……

iii) gegebenenfalls 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: Kontaktangaben

Behörde/Ansprechpartner für Rückfragen im Zusammenhang mit der Ausführung des EPOC-PR: ……

ANHANG III

INFORMATIONEN ÜBER DIE UNMÖGLICHKEIT, DAS EPOC / EPOC-PR AUSZUFÜHREN

ABSCHNITT A:

Die nachfolgenden Informationen betreffen:

□ die Europäische Herausgabeanordnung (EPOC)

□ die Europäische Sicherungsanordnung (EPOC-PR)

ABSCHNITT B:

Adressat des EPOC/EPOC-PR: ……..……..……..

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: ……..

Datum der Übermittlung des EPOC/EPOC-PR (sofern bekannt): ...……

ABSCHNITT D: Gründe für die Unmöglichkeit der Ausführung

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 Fehler.

□ EPOC/EPOC-PR enthält keine ausreichenden Angaben.

□ Aufgrund *höherer Gewalt* oder einer faktischen Unmöglichkeit, die dem Adressaten oder dem Diensteanbieter nicht angelastet werden kann.

□ 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 Dienst fällt nicht unter die Verordnung (EU) .... .

□ Die Europäische Herausgabeanordnung / Europäische Sicherungsanordnung betrifft keine Daten, die zum Zeitpunkt des Erhalts 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 offenkundig gegen die Grundrechtecharta verstößt oder offensichtlich missbräuchlich ist.

□ Die Befolgung der Europäischen Herausgabeanordnung 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 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 bis zur Herausgabe gesichert, oder bis die Anordnungsbehörde oder gegebenenfalls die Vollstreckungsbehörde mitteilt, dass die Sicherung und Herausgabe von Daten nicht mehr erforderlich ist.

□ werden nicht gesichert, da sie nicht anhand der Angaben im EPOC / EPOC-PR identifiziert werden können.

ABSCHNITT H: Angaben zum Diensteanbieter bzw. seinem Vertreter

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

Name der bevollmächtigten Person:.....

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