Rat der
Europäischen Union

Brüssel, den 30. November 2018
(OR. en)

15020/18

Interinstitutionelles Dossier:
2018/0108(COD)

JAI 1236
COPEN 428
CYBER 304
DROIPEN 192
JAIEX 160
ENFOPOL 596
DAPIX 366
EJUSTICE 163
MI 917
TELECOM 442
DATAPROTECT 263
CODEC 2180

VERMERK

Absender:	Vorsitz
Empfänger:	Rat
Nr. Vordok.:	14351/1/18 REV1
Nr. Komm.dok.:	8110/18
Betr.:	Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen – Allgemeine Ausrichtung

EINLEITUNG

1. Am 17. April 2018 hat die Kommission den oben genannten Vorschlag, dessen Rechtsgrundlage Artikel 82 Absatz 1 AEUV ist, angenommen und dem Rat und dem Europäischen Parlament zugeleitet. Ziel des Vorschlags ist die Einführung Europäischer Herausgabeanordnungen und Sicherungsanordnungen, mit denen elektronische Beweismittel in einem anderen Hoheitsgebiet ohne Einschaltung der dort zuständigen Behörden eingeholt und gesichert werden können. Die Anordnungen sind insbesondere auf den grenzüberschreitenden Zugang zu elektronischen Beweismitteln ausgerichtet, wobei es darum geht, die Mechanismen der justiziellen Zusammenarbeit den Erfordernissen der Kriminalitätsbekämpfung im digitalen Zeitalter anzupassen.

2. Mit der vorgeschlagenen Verordnung wird die Möglichkeit geschaffen, jede Kategorie gespeicherter Daten anzufordern. Für Verkehrs- und Inhaltsdaten ist darin jedoch [anders als für Teilnehmer- und Zugangsdaten] eine besondere Einschränkung vorgesehen, da sie nur dann angefordert werden können, wenn sie Straftaten betreffen, die mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden, oder aber bestimmte mit dem Cyberspace zusammenhängende oder durch den Cyberspace ermöglichte Straftaten sowie Straftaten mit einem terroristischen Hintergrund.

3. Im Vorschlag ist für die Vollstreckung der Europäischen Herausgabeanordnung eine verbindliche Frist von 10 Tagen vorgesehen, aber in Notfällen (Situationen, in denen Leib und Leben oder die körperliche Unversehrtheit einer Person oder eine kritische Infrastruktur unmittelbar bedroht sind) beträgt diese Frist sechs Stunden. Im Fall der Europäischen Sicherungsanordnung hat die zuständige Behörde 60 Tage Zeit, um zu bestätigen, dass sie das entsprechende Ersuchen um Herausgabe der Daten (auch im Rahmen des Rechtshilfeverfahrens) in die Wege geleitet hat. Wenn einer Anordnung nicht Folge geleistet wird, können Sanktionen gegen den Diensteanbieter verhängt werden.

4. Die Anordnungen sind zur Einholung elektronischer Beweismittel gemäß der vorgeschlagenen Richtlinie an den Diensteanbieter, der in der Union Dienste anbietet, oder an einen vom Diensteanbieter benannten Vertreter in einem anderen Mitgliedstaat zu richten. Im Verordnungsentwurf sind Kriterien für die Art der angebotenen Dienste (elektronische Kommunikationsdienste, Dienste der Informationsgesellschaft, Hosting-Dienste, IP-Adressendienste, Datenschutz- und Proxy-Dienste) vorgesehen, aber es werden auch bestimmte Arten von Diensteanbietern genannt (Domänennamen-Register oder -Registrierstellen).

5. Am 18. Oktober 2018 hat der Europäische Rat[1] nach Lösungen verlangt, um einen raschen und effizienten grenzüberschreitenden Zugang zu elektronischen Beweismitteln zu gewährleisten, damit Terrorismus und andere Formen der schweren und organisierten Kriminalität sowohl innerhalb der Union als auch auf internationaler Ebene wirksam bekämpft werden können. Er hob hervor, dass über die Kommissionsvorschläge über elektronische Beweismittel spätestens zum Ende dieser Legislaturperiode eine Einigung erzielt werden sollte.

6. Im Europäischen Parlament wurde Frau Birgit Sippel (LIBE, S&D) am 24. Mai 2018 als Berichterstatterin benannt. Der LIBE-Ausschuss hat am 11. Juni 2018 über den Vorschlag beraten und dazu mehrere Sitzungen und Anhörungen abgehalten, einschließlich einer öffentlichen Anhörung am 27. November 2018. Eine Frist für die Annahme des Bericht wurde bisher nicht festgelegt.

7. Der Europäische Wirtschafts- und Sozialausschuss hat seine Stellungnahme am 12. Juli 2018[2] angenommen.

---

1 Dok. EUCO 13/18, Ziffer 9.
2 Dok. 11533/18.

II. BERATUNGEN IM RAT

8. Die Kommission hat diesen Vorschlag der Gruppe "Zusammenarbeit in Strafsachen" am 27. April 2018 vorgelegt; daraufhin wurde in der Gruppe am 5./6. Mai 2018 der Verordnungsentwurf Artikel für Artikel geprüft und die Folgenabschätzung erörtert. Die Folgenabschätzung und der Vorschlag wurden von den Delegationen grundsätzlich positiv aufgenommen.

9. Schwerpunkte der Aussprachen waren vor allem der Vorschlag der Kommission, Europäische Herausgabeanordnungen direkt an den Diensteanbieter oder dessen Vertreter zu richten, ohne den Mitgliedstaat, in dem dieser ansässig ist (d. h. den Vollstreckungsstaat), einzuschalten, die Definition des Begriffs "Diensteanbieter", Immunitäten und Vorrechte, die Überprüfung des Verfahrens bei einander widersprechenden Verpflichtungen und die Sanktionen bei Nichteinhaltung der Verpflichtungen aus der Verordnung.

10. Die Prüfung des Vorschlags durch die Gruppe fand unter bulgarischem und österreichischem Vorsitz statt. Es wurden zwölf Sitzungen abgehalten, die zu fünf aufeinanderfolgenden überarbeiteten Fassungen führten. Die Beratungen im Hinblick auf die Vorlage des in der Anlage zu diesem Vermerk wiedergegebenen Kompromisstexts zwecks Festlegung einer allgemeinen Ausrichtung auf der nächsten Tagung des JI-Rates am 6./7. Dezember 2018 wurden am 20. November 2018 abgeschlossen.

11. In den in der Anlage wiedergegebenen überarbeiteten Kompromisstext des Vorsitzes sind die Ergebnisse der Beratungen in den Sitzungen der Gruppe, die schriftlichen Beiträge der Delegationen sowie die Vorbehalte der Mitgliedstaaten zu dem Text eingeflossen. Die Erwägungsgründe wurden an die Änderungen im verfügenden Teil angepasst. Änderungen gegenüber dem Vorschlag der Kommission sind wie folgt kenntlich gemacht: neuer Text durch **Fettdruck**, Streichungen durch [...].

III. FAZIT

12. Der in der Anlage wiedergegebene Text zeugt von den Bemühungen des Vorsitzes und der Mitgliedstaaten, zu einem Kompromiss zu gelangen.

13. Am 28. November 2018 erzielte der Ausschuss der Ständigen Vertreter ein Einvernehmen über den in der Anlage wiedergegebenen Kompromisstext des Vorsitzes, wobei die einzige Änderung darin bestand, dass der Vorbehalt von Sl in der Fußnote 27 aufgehoben wurde.

14. Der Rat wird daher ersucht, eine allgemeine Ausrichtung zu diesem Text festzulegen, die als Grundlage für die Verhandlungen mit dem Europäischen Parlament im Rahmen des ordentlichen Gesetzgebungsverfahrens (Artikel 294 AEUV) dienen soll.

ANLAGE

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen[3]

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[4],

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] Die Niederlande, Finnland, die Tschechische Republik und Lettland haben Vorbehalte zum gesamten Kompromisstext. Im Fall der Niederlande betreffen diese Vorbehalte unter anderem die Artikel 5, 6, 7a, Artikel 11 Absatz 3 und die Artikel 12a, 12b, 14 und 17.

[4] ABl. C vom , S. .

(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 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[5] 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[6] 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.

---

[5] JOIN(2017) 450 final.

[6] 2017/2068(INI).

(9) Der fragmentierte Rechtsrahmen stellt die Diensteanbieter, die Ersuchen von Strafverfolgungsbehörden Folge leisten wollen, vor Probleme. Daher muss ein europäischer Rechtsrahmen für elektronische Beweismittel geschaffen werden, mit dem Diensteanbieter im Anwendungsbereich des Instruments verpflichtet werden, Behörden direkt zu antworten, ohne dass [...] **eine systematische** Einschaltung einer Justizbehörde im Mitgliedstaat des Diensteanbieters **in jedem Fall** 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.

(**12a**) **Hat der Anordnungsmitgliedstaat Hinweise darauf, dass in einem anderen Mitgliedstaat möglicherweise ein paralleles Strafverfahren geführt wird, so konsultiert er die Behörden dieses Mitgliedstaats gemäß dem Rahmenbeschluss 2009/948/JI des Rates[7]. In keinem Fall sollte eine Europäische Herausgabeanordnung erlassen werden, wenn der Anordnungsmitgliedstaat Hinweise darauf hat, dass dies dem Grundsatz "ne bis in idem" zuwiderlaufen würde.**

[7] 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).

(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[8], 2012/13/EU[9], 2013/48/EU[10], (EU) 2016/343[11], (EU) 2016/800[12] und (EU) 2016/1919[13] 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.

---

8 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).

9 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).

10 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).

11 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).

12 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).

13 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).

(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. **Diese Verordnung sollte auch für andere Anbieter von** [...] Diensten der Informationsgesellschaft [...] im Sinne der Richtlinie (EU) 2015/1535 **gelten, die zwar** nicht als Anbieter elektronischer Kommunikationsdienste gelten**, ihren Nutzern aber ermöglichen, miteinander zu kommunizieren, oder Dienstleistungen anbieten, die ihnen die Verarbeitung oder Speicherung von Daten ermöglichen. Dies sollte dem Budapester Übereinkommen über Computerkriminalität entsprechen. Der Begriff der Datenverarbeitung sollte im technischen Sinne ausgelegt werden und sich auf die Erstellung oder Bearbeitung von Daten beziehen, das heißt auf technische Vorgänge, bei denen Daten mithilfe der Rechenleistung von Computern erzeugt oder verändert werden. Unter derartige Kategorien von Diensteanbietern fallen beispielsweise** Online-Marktplätze, die [...] Verbrauchern **und** Unternehmen **ermöglichen, miteinander zu kommunizieren**, und andere Hosting-Dienste, einschließlich Cloud-Computing-Diensten**, sowie Plattformen für Online-Spiele und Online-Glücksspiele**. **Wenn ein Anbieter von Diensten der Informationsgesellschaft seinen Nutzern nicht ermöglicht, miteinander zu kommunizieren, sondern lediglich einen Diensteanbieter bereitstellt, oder ihnen nicht ermöglicht, Daten zu verarbeiten oder zu speichern, oder wenn die Datenspeicherung/-verarbeitung nicht wesentlicher Bestandteil der für den Nutzer erbrachten Dienstleistung ist, wie im Fall online erbrachter Rechts-, Architektur-, Ingenieur- und Buchführungsleistungen, fällt er nicht unter die Definition, selbst wenn er unter die Definition des Begriffs "Dienstleistung der Informationsgesellschaft" im Sinne der Richtlinie (EU) 2015/1535 fällt.** […]

(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.

(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.

(24a) Da Rechtshilfeverfahren nach dem in den Mitgliedstaaten geltenden einzelstaatlichen Recht als Strafverfahren gelten können, sollte klargestellt werden, dass eine Europäische Herausgabeanordnung oder eine Europäische Sicherungsanordnung nicht erlassen werden sollte, um einem anderen Mitgliedstaat oder Drittstaat Rechtshilfe zu leisten. In solchen Fällen sollte das Rechtshilfeersuchen an den Mitgliedstaat oder den Drittstaat gerichtet werden, der nach seinem innerstaatlichen Recht Rechtshilfe leisten kann. Wenn die Anordnungsbehörde jedoch bereits gemäß dieser Verordnung elektronische Beweismittel für eigene strafrechtliche Ermittlungen oder Strafverfahren eingeholt hat und diese Beweismittel anschließend übermittelt werden, sollten die nach dem Grundsatz der Spezialität geltenden Bedingungen zur Anwendung kommen.

(24b) Diese Verordnung sollte für Strafverfahren gelten, die von der Anordnungsbehörde eingeleitet wurden, um Verurteilte, die sich der Justiz entzogen haben, im Hinblick auf die Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung zu lokalisieren. Allerdings sollte, wenn die Entscheidung über die Strafe oder die freiheitsentziehende Maßregel der Sicherung in Abwesenheit ergangen ist, nicht die Möglichkeit bestehen, eine Europäische Herausgabeanordnung oder eine Europäische Sicherungsanordnung zu erlassen, da sich die innerstaatlichen Rechtsvorschriften der Mitgliedstaaten in Bezug auf Abwesenheitsurteile in der Europäischen Union stark unterscheiden.

(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 **besonderer faktischer Kriterien, beispielsweise** 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[14] auf einen oder mehrere Mitgliedstaaten ausrichtet. Andererseits kann die Erbringung der Dienstleistung zum Zwecke der bloßen Einhaltung des in der Verordnung (EU) 2018/302[15] 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 **, wobei die Auswirkungen der Maßnahme auf die Grundrechte der Person, deren Daten angefordert werden, gebührend zu berücksichtigen sind**.

---

14 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).

15 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).

(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 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.

(33a) Wenn eine Anordnung zur Einholung verschiedener Datenkategorien erlassen wird, muss die Anordnungsbehörde sicherstellen, dass die Bedingungen und Verfahren für alle betroffenen Datenkategorien, beispielsweise die Notifizierung des Vollstreckungsstaats, eingehalten werden.

(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.

(34a) Wenn Daten als Teil einer Infrastruktur gespeichert oder verarbeitet, die ein Diensteanbieter einer Behörde bereitstellt, sollten nur Behörden desselben Mitgliedstaats in der Lage sein, eine Europäische Herausgabeanordnung oder Sicherungsanordnung zu erlassen, da solche Daten als besonders sensibel betrachtet werden können. Als Behörde sollte jede öffentliche Stelle verstanden werden, die nach dem geltenden innerstaatlichen Recht mit der Führung und/oder Verwaltung eines Teils oder eines Aspekts des öffentlichen Lebens beauftragt ist, beispielsweise Zweige der Judikative, Legislative oder Exekutive eines Staates, einer Provinz oder einer Gemeinde.

(35) Auf Immunitäten und Vorrechte für Personengruppen (wie Diplomaten) oder besonders geschützte Beziehungen (wie das Recht auf Vertraulichkeit der Kommunikation zwischen Anwalt und Mandant **oder das Recht der Journalisten auf Quellenschutz**) 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. [...] **Ob ein zweiter Rechtsrahmen berücksichtigt werden muss, sollte von der Stärke der Verbindung der Person, deren Daten angefordert werden, zum Anordnungsstaat abhängig sein. Wenn diese Person ihren Wohnsitz im Hoheitsgebiet des Anordnungsstaats hat, besteht eine starke Verbindung zum Anordnungsstaat. Deshalb sollte zur Bewertung von** Immunitäten und Vorrechten **ausschließlich der Rechtsrahmen des Anordnungsstaats Anwendung finden**. **Derselbe Grundsatz gilt auch für die Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien, sowie für die grundlegenden Interessen des Vollstreckungsstaats. Bis zum Zeitpunkt der Anforderung von Inhalts- oder Transaktionsdaten haben die Behörden aufgrund der vorausgehenden Ermittlungsschritte in der Regel einen Hinweis darauf, wo die betreffenden Person ihren Wohnsitz hat. Außerdem belegen Statistiken, dass die Person ihren Wohnsitz in der überwiegenden Mehrzahl der Fälle im Anordnungsstaat hat. Wenn das nicht der Fall ist, beispielsweise weil die Person, deren Daten angefordert werden, Vorkehrungen getroffen hat, um ihren Aufenthaltsort zu verbergen, sollte nach demselben Grundsatz verfahren werden.**

(35a) **D**ie Immunitäten und Vorrechte **sowie Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien**, die [...] Transaktions- oder Inhaltsdaten im **Vollstreckungsstaat** [...] schützen, sollten **deshalb** [...] berücksichtigt werden, **wenn die Anordnungsbehörde berechtigten Grund zu der Annahme hat, dass die Person, deren Daten angefordert werden, ihren Wohnsitz in einem anderen Hoheitsgebiet hat**. Dies gilt insbesondere, wenn [...] **das Recht dieses Mitgliedstaats 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. [...] **D**iese Aspekte sollten nicht nur beim Erlass der Anordnung berücksichtigt werden, sondern auch zu einem späteren Zeitpunkt [...], und im Falle eines Vollstreckungsverfahrens durch die vollstreckende Behörde.

(35b) Wenn die Anordnungsbehörde Transaktionsdaten einholen möchte und berechtigten Grund zu der Annahme hat, dass die Person, deren Daten angefordert werden, ihren Wohnsitz in einem anderen Hoheitsgebiet hat, und dass die angeforderten Daten durch Immunitäten und Vorrechte, die nach dem Recht des Vollstreckungsstaats gewährt werden, oder durch Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien geschützt sind, oder dass sich die Offenlegung der betreffenden Daten auf die grundlegenden Interessen dieses Mitgliedstaats wie die nationale Sicherheit oder Verteidigung auswirken könnte, sollte sich die Anordnungsbehörde um Klärung des Sachverhalts, einschließlich durch entsprechende Konsultationen, bemühen.

(35c) Wenn die Europäische Herausgabeanordnung Inhaltsdaten betrifft und die Anordnungsbehörde berechtigten Grund zu der Annahme hat, dass die Person, deren Daten angefordert werden, ihren Wohnsitz in einem anderen Hoheitsgebiet hat, wird der Vollstreckungsstaat notifiziert und kann die Anordnungsbehörde sobald möglich, vorzugsweise innerhalb von 10 Tagen, über Umstände – wie Vorrechte oder Immunitäten der Person, deren Daten angefordert werden, oder Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien – informieren, die zum Widerruf oder zur Anpassung der Anordnung führen könnten. Bei Inhaltsdaten handelt es sich im Gegensatz zu Nichtinhaltsdaten um besonders sensible Daten, da damit unter Umständen persönliche Gedanken sowie sensible Einzelheiten aus dem Privatleben preisgegeben werden. Dadurch ist es gerechtfertigt, diese Daten anders zu behandeln und die Behörden des Vollstreckungsstaats frühzeitig in das Verfahren einzubeziehen. In solchen Fällen sollte der Anordnungsmitgliedstaat zu dem Zeitpunkt, zu dem das Zertifikat dem Diensteanbieter vorgelegt wird, dem Vollstreckungsstaat eine Kopie des Zertifikats übermitteln. Um eine zügige Überprüfung zu ermöglichen, sollte sich die Anordnungsbehörde, wenn das Zertifikat übersetzt werden muss, für eine der vom Vollstreckungsstaat akzeptierten Sprachen entscheiden, selbst wenn der Diensteanbieter angegeben hat, dass er auch Zertifikate in einer Sprache akzeptieren würde, die keine Amtssprache des Vollstreckungsstaats ist. Wenn sich die notifizierte Behörde auf Umstände beruft, sollte sie der Anordnungsbehörde zu den Immunitäten oder Vorrechten sowie zu den Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien, die der Person nach ihrem Recht gewährt werden, oder zu den Auswirkungen der Anordnung auf grundlegende Interessen dieses Mitgliedstaats wie die nationale Sicherheit oder Verteidigung alle einschlägigen Informationen vorlegen.

(35d) Wenn die Person zu dem Zeitpunkt, zu dem die Europäische Herausgabeanordnung erlassen wurde, mehr als einen Wohnsitz hat und sich einer der Wohnsitze im Hoheitsgebiet des Anordnungsstaats befindet, oder wenn sich der Wohnsitz der Person trotz angemessener und verhältnismäßiger Bemühungen nicht feststellen lässt, findet das obengenannte Verfahren keine Anwendung. Eine kurzer Besuch, ein Urlaub oder vergleichbarer Aufenthalt im Anordnungsmitgliedstaat ohne jegliche weitere wesentliche Verbindung sind für die Feststellung eines Wohnsitzes in diesem Mitgliedstaat jedoch nicht ausreichend.

(35e) Um eine zügige Abwicklung des Verfahrens zu ermöglichen, sollte bereits zum Zeitpunkt des Erlasses oder der Validierung der Anordnung festgestellt werden, ob eine Notifizierung der Behörden des Vollstreckungsstaats erforderlich ist. Eine anschließende Änderung des Wohnsitzes sollte keinen Einfluss auf das Verfahren haben. Wenn die Anordnungsbehörde keinen berechtigten Grund zu der Annahme hatte, dass die Person, deren Daten angefordert werden, ihren Wohnsitz zum Zeitpunkt des Erlasses oder der Validierung der Anordnung ihren Wohnsitz in einem anderen Hoheitsgebiet hat, und sich später herausstellt, dass diese Person ihren Wohnsitz in Wirklichkeit nicht im Hoheitsgebiet des Anordnungsmitgliedstaats hatte, sollte keine spätere Überprüfung oder Notifizierung erforderlich sein. Die betroffene Person kann jedoch während des gesamten Strafverfahrens ihre Rechte sowie die Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien geltend machen, und auch der andere Mitgliedstaat könnte sich während des Strafverfahrens jederzeit auf grundlegende Interessen wie nationale Sicherheit und Verteidigung berufen. Diese Gründe könnten zudem auch während des Vollstreckungsverfahrens geltend gemacht werden.

(35f) Wenn Daten durch nach dem Recht des Vollstreckungsstaats gewährte Vorrechte oder Immunitäten oder Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien geschützt sind oder sich die Offenlegung von Daten auf die grundlegenden Interessen dieses Mitgliedstaats auswirken könnte, sollte der Anordnungsstaat, um diesen Gründen Geltung zu verleihen, sicherstellen, dass sie genauso berücksichtigt werden, als wären sie in seinem nationalen Recht vorgesehen. Wenn beispielsweise solche Vorrechte oder Immunitäten nach dem Recht des Anordnungsmitgliedstaats nicht gewährt werden, sollte der Schutz – unter Berücksichtigung der mit dem besonderen Schutz verfolgten Ziele und Interessen und der damit verbundenen Auswirkungen – soweit möglich an die im Recht des Anordnungsstaats am ehesten vergleichbaren Vorrechte oder Immunitäten angepasst werden. Die im nationalen Recht für vergleichbaren Fälle vorgesehenen rechtlichen Konsequenzen sollten Anwendung finden. Um festzustellen, wie diese Gründe genauso berücksichtigt werden können, als wären sie im eigenen nationalen Recht vorgesehen, kann die Anordnungsbehörde die notifizierte Behörde entweder direkt oder über das Europäische Justizielle Netz für Strafsachen oder Eurojust um weitere Information zur Art und Wirkung des Schutzes ersuchen. Während der Vollstreckungsstaat sämtliche auf diese Gründe gestützte Einwände erheben kann, kann sich die Person, deren Daten angefordert werden, nur auf ihre Rechte, beispielsweise Vorrechte oder Immunitäten, berufen und keine Einwände aufgrund eines grundlegenden Interesses des Vollstreckungsstaats erheben.

(35g) Wenn es aufgrund eines Vorrechts oder einer Immunität untersagt ist, die Daten zu nutzen, diese Rechte aber aufgehoben werden könnten, und wenn die Anordnungsbehörde beabsichtigt, die eingeholten Daten als Beweismittel zu verwenden, oder die Anordnung, wenn die Daten bisher nicht eingeholt wurden, nicht zurückzieht, sollte der Anordnungsmitgliedstaat bei der zuständigen Behörde die Aufhebung des Vorrechts oder der Immunität beantragen können.

(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.

(36a) Damit die uneingeschränkte Wahrung der Grundrechte sichergestellt ist, sollte die Validierung von Europäischen Herausgabeanordnungen oder Sicherungsanordnungen durch die Justizbehörden grundsätzlich vor dem Erlass der Anordnung erwirkt werden. Von diesem Grundsatz kann bei der Anforderung von Teilnehmer- und Zugangsdaten nur in Ausnahmefällen abgesehen werden, wenn die Anordnungsbehörde hinreichend begründet, dass ein Notfall vorliegt und es nicht möglich ist, rechtzeitig eine vorherige Validierung durch die Justizbehörde einzuholen, insbesondere weil die Validierungsbehörde nicht erreicht werden kann, um eine Validierung einzuholen, und die Bedrohung so unmittelbar ist, dass sofort gehandelt werden muss. Dies gilt jedoch nur, wenn dieses Verfahren für einen gleich gelagerten innerstaatlichen Fall im nationalen Recht vorgesehen ist.

(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. **Wenn die Europäische Herausgabeanordnung oder Sicherungsanordnung infolge einer Nichteinhaltung durch den Vertreter an den Diensteanbieter gerichtet wird, kann sie auch gegen den Diensteanbieter vollstreckt werden.**

(38) Europäische Herausgabe- und Sicherungsanordnungen sollten dem **Adressaten** 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 **Vollstreckungsstaats** oder in eine andere Amtssprache, der der Diensteanbieter zugestimmt hat, übersetzt werden.

(39) Die zuständige Anordnungsbehörde **oder die für die Übermittlung zuständige Behörde** sollte das EPOC oder das EPOC-PR im Einklang mit den Vorschriften zum Schutz personenbezogener Daten **sicher und zuverlässig** 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 **auf eine sichere und zuverlässige Weise, die die Feststellung der Echtheit des Absenders und der Unversehrtheit der Daten gestattet,** 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 [...] Behörde 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 [...] **der Europäischen Herausgabe-anordnung** 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.

(41a) Der Adressat sollte nicht zur Befolgung der Anordnung verpflichtet sein, wenn dies aus Gründen, die zum Zeitpunkt des Eingangs der Anordnung nicht vom Adressaten oder, falls abweichend, vom Diensteanbieter herbeigeführt wurden, faktisch unmöglich ist. Von einer solchen faktischen Unmöglichkeit sollte ausgegangen werden, wenn die Person, deren Daten angefordert wurden, nicht Kunde des Diensteanbieters ist oder selbst nach Anforderung weiterer Informationen für die Anordnungsbehörde nicht als solcher identifiziert werden kann oder wenn die Daten vor Eingang der Anordnung rechtmäßig gelöscht wurden.

(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**. Außerdem sollten sie** [...] davon absehen, die Person, deren Daten angefordert werden, hierüber zu informieren, um gemäß Artikel 23 der Verordnung (EU) 2016/679[16] die Ermittlung von Straftaten sicherzustellen, [...] **es sei denn, sie werden von der Anordnungsbehörde ersucht, diese Person zu informieren**. **In diesen Fällen sollte die Anordnungsbehörde dem Diensteanbieter auch die notwendigen Informationen über anwendbare Rechtsbehelfe bereitstellen, damit sie in die der Person zur Verfügung gestellten Informationen aufgenommen werden können.** Nutzerinformationen tragen **in jedem Fall** 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 von der Behörde bereitgestellt werden, wenn der Diensteanbieter **nicht** aufgefordert wurde, den Nutzer [...] zu informieren, [...] **sobald** keine Gefahr besteht, dass laufende Ermittlungen gefährdet werden[17]. **Die Anordnungsbehörde kann davon absehen, die Person, deren Teilnehmer- oder Zugangsdaten angefordert wurden, zu informieren, wenn das zum Schutz der Grundrechte und der berechtigten Interessen einer anderen Person notwendig und verhältnismäßig ist und insbesondere, wenn diese Rechte und Interessen gegenüber dem Interesse der Person, deren Daten angefordert wurden, an einer entsprechenden Unterrichtung überwiegen. Das könnte der Fall sein, wenn eine Anordnung die Teilnehmer- oder Zugangsdaten eines Dritten betreffen, da für den Verdächtigen die Unschuldsvermutung gilt. Wenn der Anordnungsbehörde die Identität der betreffenden Person nicht bekannt ist, sollten Untersuchungen zur Feststellung der Identität dieser Person nur stattfinden, wenn dies angesichts der Invasivität der Maßnahme und des mit der Feststellung der Identität verbundenen Aufwands notwendig und verhältnismäßig erscheint.**

(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.

---

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 (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

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 (ABl. L 119 vom 4.5.2016, S. 89).

(45) Das Vollstreckungsverfahren ist ein Verfahren, bei dem der Adressat [...] aus bestimmten beschränkten Gründen **formelle Gründe gegen** die Vollstreckung **geltend machen** kann. Die Vollstreckungsbehörde kann die Anerkennung und Vollstreckung der Anordnung [...] aus denselben Gründen [...] **sowie dann ablehnen,** wenn **sie gemäß dieser Verordnung zu berücksichtigen sind, weil** gemäß den betreffenden nationalen Rechtsvorschriften Immunitäten und Vorrechte **sowie Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien** gelten, oder [...] 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.

(45a) Wenn im Einzelfall die angemessenen finanziellen Sanktionen festgelegt werden, sollten die zuständigen Behörden alle einschlägigen Umstände berücksichtigen, beispielsweise Art, Schwere und Dauer des Verstoßes, ob der Verstoß absichtlich oder fahrlässig begangen wurde, ob der Diensteanbieter bereits vergleichbare Verstöße zu verantworten hatte, und die Finanzkraft des haftenden Diensteanbieters. In Ausnahmefällen kann die Bewertung dazu führen, dass sich die Vollstreckungsbehörde gegen die Verhängung finanzieller Sanktionen entscheidet. Besondere Beachtung sollten diesbezüglich Kleinstunternehmen finden, die einer Anordnung in einem Notfall wegen Personalmangels außerhalb der üblichen Geschäftszeiten nicht Folge leisten, sofern die Daten unverzüglich übermittelt werden.

(46) [...] Diensteanbieter **sollten** in den Mitgliedstaaten nicht für Schäden haftbar gemacht werden, die ihren Nutzern oder Dritten [...] aufgrund der Befolgung eines EPOC oder eines EPOC-PR in guter Absicht entstehen. **Die Verantwortung für die Gewährleistung der Rechtmäßigkeit der Anordnung, insbesondere ihre Notwendigkeit und Verhältnismäßigkeit, sollte bei der Anordnungsbehörde liegen.**

(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 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, **kann** sich das zuständige Gericht gegebenenfalls auf angemessenes externes Fachwissen, beispielsweise [...] zur Auslegung des Rechts des betreffenden Drittstaats**,** stützen. 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 **Rechtsvorschriften** des Drittstaats **gelten und, wenn das der Fall ist, ob sie** die Offenlegung der betreffenden Daten [...] verbieten [...]. [...] Wenn das Gericht zu dem Schluss gelangt, dass die widersprüchlichen Bestimmungen des Drittstaats die Offenlegung der betreffenden Daten [...] verbieten, [...]

[…] 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. **Bei der Bewertung sollte dem Schutz der Grundrechte im Rahmen der Bestimmungen des Drittstaats und anderen grundlegenden Interessen des Drittstaats beispielsweise im Zusammenhang mit der nationalen Sicherheit, sowie dem Grad der Verbindung der Strafsache zu einem der beiden Rechtssysteme besondere Bedeutung und besonderes Gewicht beigemessen werden.**

(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 [...] ausüben**, wann immer eingeholte Daten in Strafverfahren gegen sie verwendet werden**. 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, **deren Daten zwar angefordert wurden,** die **aber** 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) [...] Während des Vollstreckungsverfahrens **kann die Vollstreckungsbehörde die Anerkennung und** Vollstreckung einer Europäischen Herausgabe- oder Sicherungsanordnung aus einer Reihe von bestimmten Gründen **ablehnen**. […]

(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.

(56a) Wenn elektronische Beweismittel durch eine Europäische Herausgabeanordnung in einem anderen Verfahren und zu einem anderen Zweck als dem Zweck eingeholt wurden, aus dem die Anordnung erteilt wurde, sollte die Übermittlung und die Nutzung dieser Beweismittel Beschränkungen unterliegen; dies gilt insbesondere bei Straftaten, in deren Fall die Anordnungsbehörde auch eine Europäische Herausgabeanordnung hätte erteilen können. Elektronische Beweismittel sollten zudem nur genutzt und übermittelt werden können, wenn die Daten benötigt werden, um eine unmittelbare und schwere Bedrohung der öffentlichen Sicherheit des betreffenden Mitgliedstaats oder Drittstaats sowie deren grundlegender Interessen abzuwenden. Für die internationale Übermittlung elektronischer Beweismittel gelten ferner die Bedingungen des Kapitels V der Richtlinie (EU) 2016/680. Wenn die eingeholten personenbezogenen Daten verwendet werden, um eine unmittelbare und schwere Bedrohung der öffentlichen Sicherheit des betreffenden Mitgliedstaats oder Drittstaats sowie deren grundlegender Interessen abzuwenden, und die Bedrohung möglicherweise keine strafrechtlichen Ermittlungen nach sich zieht, sollte die Verordnung (EU) 2016/679 zur Anwendung kommen.

(56b) Im Zusammenhang mit ihrer Erklärung zur Sprachenregelung werden die Mitgliedstaaten ersucht, mindestens eine zusätzliche Sprache aufzunehmen, die in ihrem Land keine Amtssprache ist.

(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[18] 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 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[19] nicht ersetzen. Die Behörden der Mitgliedstaaten sollten das für **den vorliegenden Fall** 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 Verwirklichung dieser Ziele erforderliche Maß hinaus.

---

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

19 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).

(64) Gemäß Artikel 3 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts hat [...] Irland schriftlich mitgeteilt, dass es sich an der Annahme und der Anwendung dieser Verordnung beteiligen möchte; das Vereinigte Königreich [...] beteiligt sich unbeschadet des Artikels 4 des Protokolls nicht an der Annahme dieser Verordnung, die daher für das Vereinigte Königreich weder bindend noch ihm 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[20] angehört und gab am (...) eine Stellungnahme[21] ab —

[20] 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).

[21] 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**, ausgenommen Finanzdienstleistungen im Sinne des Artikels 2 Absatz 2 Buchstabe b der Richtlinie 2006/123/EG**:

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

(b) Internetdomänennamen- und IP-Adressendienste wie IP-Adressenanbieter, Domänennamen-Register, Domänennamen-Registrierungsstellen und damit verbundene Datenschutz- und Proxy-Dienste;

(c) **andere** Dienste der Informationsgesellschaft im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates[22], **die**

– **ihren Nutzern ermöglichen, miteinander zu kommunizieren, oder**

– Nutzern, für die die Dienstleistung erbracht wird, die Verarbeitung oder Speicherung von Daten ermöglichen [...][23];

(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) **aufgrund konkreter faktischer Kriterien** eine wesentliche Verbindung zu dem/den unter Buchstabe a genannten Mitgliedstaat(en) hat/haben;

(5) "Niederlassung" **oder "niedergelassen sein"** [...] die tatsächliche Ausübung einer wirtschaftlichen Tätigkeit auf unbestimmte Zeit durch eine stabile Infrastruktur, von der aus die Geschäftstätigkeit der Dienstleistungserbringung ausgeübt [...] oder [...] 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;

---

22 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).

23 Finnland, Lettland und Luxemburg haben diesbezüglich Vorbehalte, weil die Behörden nicht verpflichtet sein sollten, einer Europäischen Herausgabe- oder Sicherungsanordnung nachzukommen (Finnland), weil die Begriffsbestimmung nach wie vor zu unklar ist und keine Rechtssicherheit bietet (Luxemburg), und weil eine weitere Auseinandersetzung mit der Begriffsbestimmung notwendig ist, vor allem im Zusammenhang mit dem Vorschlag für eine Richtlinie zur Festlegung einheitlicher Regeln für die Benennung rechtlicher Vertreter zwecks Erhebung von Beweismitteln in Strafverfahren (Lettland).

(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 im Sinne des Artikels 4 Absatz 3 Buchstabe [...] **c** 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 [...] **c** 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[24];

(12) "Anordnungsstaat" den Mitgliedstaat, in dem die Europäische Herausgabeanordnung oder die Europäische Sicherungsanordnung erlassen wird;

---

[24] 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).

(13) "Vollstreckungsstaat" den Mitgliedstaat, in dem der Adressat der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung ansässig oder niedergelassen ist und an den **erforderlichenfalls** 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[25] besteht.

Artikel 3
Anwendungsbereich

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

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

(2) Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen dürfen nur für Strafverfahren [...] **und zur Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung, sofern diese in dem Fall, dass sich der Verurteilte der Justiz entzogen hat, nicht in Abwesenheit ergangenen sind,** [...] 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[26].

(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.

---

25 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).

26 Die Tschechische Republik, Finnland, Lettland und Deutschland haben Vorbehalte hinsichtlich der Ausweitung des Geltungsbereichs auf Verurteilte, die sich der Justiz entzogen haben; dasselbe gilt für die parallelen Bestimmungen in Artikel 5 Absatz 3 und Artikel 6 Absatz 2.

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.

(5) In hinreichend begründeten Notfällen können die in Absatz 1 Buchstabe b und Absatz 3 Buchstabe b genannten Behörden die betreffende Anordnung für Teilnehmer- und Zugangsdaten ohne vorherige Validierung erlassen, wenn die Validierung nicht rechtzeitig eingeholt werden kann und diese Behörden die Anordnung in einem vergleichbaren innerstaatlichen Fall ohne Validierung erlassen könnten. Die Anordnungsbehörde fordert unverzüglich, spätestens binnen 48 Stunden, eine Ex-post-Validierung an. Wird eine solche Ex-post-Validierung nicht gewährt, so widerruft die Anordnungsbehörde die Anordnung umgehend und gewährleistet im Einklang mit dem innerstaatlichen Recht, dass eingeholte Daten entweder gelöscht oder nicht als Beweismittel verwendet werden.[27]

(6) Jeder Mitgliedstaat kann für die administrative Übermittlung von Zertifikaten, Anordnungen und Notifizierungen, den Empfang von Daten und Notifizierungen und die Übermittlung anderer offizieller Korrespondenz in Bezug auf Zertifikate oder Anordnungen eine oder mehrere zentrale Behörden benennen.

---

27 Griechenland und Luxemburg haben in Bezug auf die Möglichkeit einer Ex-post-Validierung Vorbehalte.

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 **und zur Vollstreckung von mindestens viermonatigen Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung** erlassen werden.

(4) Europäische Herausgabeanordnungen zur Herausgabe von Transaktions- oder Inhaltsdaten können nur erlassen werden[28]

(a) bei Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden[29], 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[30];

– Straftaten im Sinne der Artikel 3 bis 7 der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates[31];

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

---

28 Finnland und Slowenien würden hier eine Liste bevorzugen.

29 Zypern hat einen Vorbehalt zu der Bedingung, bei Straftaten mit einem Strafmaß unter fünf Jahren eine Europäische Herausgabeanordnung zu erlassen.

30 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).

31 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).

(c) bei Straftaten im Sinne der Artikel 3 bis 12 und 14 der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates[32].

d) zur Vollstreckung von mindestens viermonatigen Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung, die wegen Straftaten gemäß Buchstabe a, b und c verhängt wurden.

(5) Die Europäische Herausgabeanordnung enthält folgende Angaben:

(a) die Anordnungsbehörde und gegebenenfalls die validierende Behörde;

(b) den Adressaten der Europäischen Herausgabeanordnung gemäß Artikel 7;

(c) **den Nutzer**, es sei denn, der einzige Zweck der Anordnung besteht **in der Identifizierung des Nutzers, oder jegliche andere eindeutige Kennung wie Nutzername, ID oder Kontobezeichnung** […] zur Bestimmung der angeforderten Daten;

(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.

---

[32] 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).

(6a) **Eine Europäische Herausgabeanordnung zur Herausgabe von Daten, die im Rahmen einer Infrastruktur gespeichert oder verarbeitet werden, die ein Diensteanbieter einer Behörde bereitstellt, kann nur erlassen werden, wenn sich die Behörde, für die Daten gespeichert oder verarbeitet werden, im Anordnungsstaat befindet.**

(7) […] **Wenn die Anordnung Transaktionsdaten betrifft und die** Anordnungsbehörde **berechtigten** Grund zu der Annahme hat, dass **die Person, deren Daten angefordert werden, ihren Wohnsitz nicht im Hoheitsgebiet des Anordnungsstaats hat und**

a. die angeforderten Daten durch Immunitäten und Vorrechte geschützt sind, die nach dem Recht des **Vollstreckungsstaats** [...] gewährt werden, oder in diesem Mitgliedstaat **Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien unterliegen**, oder die Offenlegung der betreffenden Daten sich auf die grundlegenden Interessen des [...] **Vollstreckungsstaats** wie die nationale Sicherheit oder Verteidigung auswirken könnte, **klärt** die Anordnungsbehörde vor Erlass der Europäischen Herausgabeanordnung **die Umstände im Sinne von Buchstabe b**, unter anderem indem sie die zuständigen Behörden des **Vollstreckungsstaats** entweder direkt oder über Eurojust oder das Europäische Justizielle Netz konsultiert. Stellt die Anordnungsbehörde fest, dass die angeforderten [...] Transaktionsdaten [...] durch solche Immunitäten und Vorrechte **oder durch Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien** geschützt sind oder dass ihre Offenlegung Auswirkungen auf die grundlegenden Interessen des anderen Mitgliedstaats **wie die nationale Sicherheit oder Verteidigung** hätte, so **berücksichtigt sie diese Umstände genauso, als wären sie im eigenen nationalen Recht vorgesehen, und** erlässt die Europäische Herausgabeanordnung nicht **oder passt diese entsprechend an, soweit das notwendig ist, um diesen Gründen Geltung zu verleihen**[33].

(8) **Wenn eine Behörde des Vollstreckungsstaats für die Aufhebung des Vorrechts oder der Immunität zuständig ist, kann die Anordnungsbehörde die Vollstreckungsbehörde ersuchen, diese zuständige Behörde zu kontaktieren, um sie unverzüglich um die Ausübung ihrer Zuständigkeit zu ersuchen. Ist eine Behörde eines anderen Mitgliedstaats oder eines Drittstaats oder eine internationale Organisation für die Aufhebung des Vorrechts oder der Immunität zuständig, so kann die Anordnungsbehörde die betreffende Behörde um Ausübung dieser Zuständigkeit ersuchen.**

---

33 Deutschland und die Tschechische Republik sind für die Aufnahme von Inhaltsdaten. Deutschland hat zudem darum ersucht, dass in diese Bestimmung und in Artikel 12a eine Grundrechteklausel aufgenommen wird. Ungarn hat wegen der Logik dieser Bestimmung einen Sachvorbehalt eingelegt: Aus seiner Sicht sollte grundsätzlich, auch im Fall der parallelen Bestimmungen in Artikel 5 Absatz 7, Artikel 7a, Artikel 9 Absatz 5, Artikel 12a und Artikel 14, eine vorherige Konsultation vorgesehen sein, wenn berechtigterweise von einer Ablehnung auszugehen ist.

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. **Artikel 5 Absatz 6a gilt entsprechend.**

(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 **und zur Vollstreckung von mindestens viermonatigen Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung** 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) den [...] **Nutzer**, es sei denn, der einzige Zweck der Anordnung besteht **in der Identifizierung des Nutzers, oder jegliche andere eindeutige Kennung wie Nutzername, ID oder Kontobezeichnung** […] zur Bestimmung der angeforderten Daten;;

(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 **die Europäische Herausgabeanordnung** 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 7a
Notifizierung[34]

(1) Wenn die Europäische Herausgabeanordnung Inhaltsdaten betrifft und die Anordnungsbehörde berechtigten Grund zu der Annahme hat, dass die Person, deren Daten angefordert werden, ihren Wohnsitz in einem anderen Hoheitsgebiet hat, wird der zuständigen Behörde des Vollstreckungsstaats zum selben Zeitpunkt ein Exemplar des EPOC vorgelegt, zu dem das EPOC dem Adressaten gemäß Artikel 7 vorgelegt wird.

(2) **Die notifizierte Behörde kann die Anordnungsbehörde über Umstände im Sinne von Artikel 5 Absatz 7 Buchstabe b möglichst bald informieren und bemüht sich darum, dies binnen 10 Tagen zu tun. Die Anordnungsbehörde berücksichtigt diese Umstände genauso, als wären sie im eigenen nationalen Recht vorgesehen, und widerruft die Anordnung oder passt sie gegebenenfalls dahingehend an, dass diesen Gründen, wenn die Daten noch nicht bereitgestellt wurden, Geltung verliehen wird. Wenn die Anordnung widerrufen wird, setzt die Anordnungsbehörde den Adressaten davon umgehend in Kenntnis.**

(3) Wenn eine Behörde des Vollstreckungsstaats für die Aufhebung des Vorrechts oder der Immunität zuständig ist, kann die Anordnungsbehörde die notifizierte Behörde ersuchen, die zuständige Behörde zu kontaktieren, um sie unverzüglich um die Ausübung ihrer Zuständigkeit zu ersuchen. Ist eine Behörde eines anderen Mitgliedstaates oder eines Drittstaats oder eine internationale Organisation für die Aufhebung des Vorrechts oder der Immunität zuständig, so ist es an der Anordnungsbehörde, die betreffende Behörde um Ausübung dieser Zuständigkeit zu ersuchen.

(4) Die Notifizierung bewirkt keine Aussetzung der Verpflichtungen des Adressaten aus dieser Verordnung.

---

34 Die Tschechische Republik, Finnland, Deutschland, Griechenland, Ungarn und Lettland haben Vorbehalte zum Notifizierungsverfahren und plädieren für ein Verfahren von größerer Tragweite, das auch Transaktionsdaten einschließt, sowie für eine Grundrechteklausel, d. h. für die Nennung von Gründen, wenn eine notifizierte Behörde abgewiesen wird; außerdem sollte die Bestimmung, in der dargelegt wird, was als "nationaler Fall" gilt, rückgängig gemacht werden; und schließlich sollte aus Sicht Deutschlands nicht das Zertifikat, sondern die Anordnung selbst übermittelt werden, während die Tschechische Republik die Ansicht vertritt, dass beide – Anordnung und Zertifikat – übermittelt werden sollten.
Belgien, Bulgarien, Estland, Frankreich, Irland, Italien, Polen, Portugal und Spanien haben Vorbehalte zum Notifizierungsverfahren und zu den Bestimmungen bezüglich der Einführung eines Notifizierungsverfahrens, insbesondere Artikel 5 Absatz 7, Artikel 9, Artikel 12a und Artikel 14, sowie zu den dazugehörigen Erwägungsgründen und ziehen den Vorschlag der Kommission vor, in dem keine Notifizierung vorgesehen ist; Belgien, Luxemburg, Irland, Slowenien und Polen wären – wenn überhaupt – für eine Notifizierung desjenigen Mitgliedstaats, in dem die Person, deren Daten angefordert werden, ihren Wohnsitz hat.

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) **Das** EPOC oder das EPOC-PR **wird durch die oder im Auftrag der Anordnungsbehörde auf sichere und zuverlässige Weise übermittelt**, die dem Adressaten **ermöglicht,** einen schriftlichen Nachweis **zu erbringen, und** die Feststellung der Echtheit **des Zertifikats** gestattet.

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 **in einer sicheren und zuverlässigen Weise, die die Feststellung der Echtheit und der Unversehrheit gestattet,** 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[35].

(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 [...] einer faktischen Unmöglichkeit **aus Gründen, die nicht vom Adressaten oder vom Diensteanbieter zum Zeitpunkt des Eingangs der Anordnung herbeigeführt wurden,** nicht nachkommen kann, [...] 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. […]

---

35 Deutschland schlägt vor, dass zumindest ein neuer Erwägungsgrund des Inhalts aufgenommen wird, dass die Kommission und die Mitgliedstaaten zusammenarbeiten und möglichst bald sichere elektronische Kommunikationskanäle schaffen, die es gestatten, Echtheit und Unversehrtheit festzustellen.

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.

[…][36]

(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.

---

36 Ungarn hat einen Vorbehalt zu der Streichung eingelegt.

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 [...] einer faktischen Unmöglichkeit **aus Gründen, die nicht vom Adressaten oder vom Diensteanbieter zum Zeitpunkt des Eingangs der Anordnung herbeigeführt wurden,** nicht nachkommen kann, [...] 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. […]

6. In allen Fällen, in denen der Adressat die angeforderten Informationen aus anderen [...] 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[37]

1. Adressaten und, falls abweichend, Diensteanbieter treffen die erforderlichen Maßnahmen, um die Vertraulichkeit des EPOC oder des EPOC-PR sowie der herausgegebenen **oder** gesicherten Daten zu gewährleisten, und sehen [...] davon ab, die Person, deren Daten angefordert werden, hiervon in Kenntnis zu setzen, um das betreffende Strafverfahren nicht zu behindern. **Die Person, deren Daten** […] **angefordert werden, wird von ihnen nur informiert, wenn die Anordnungsbehörde dies ausdrücklich verlangt hat**. **In diesem Fall stellt die Anordnungsbehörde dem Adressaten oder, falls abweichend, dem Diensteanbieter auch Informationen gemäß Absatz 4 zur Verfügung.**

(2) Wenn die Anordnungsbehörde den **Diensteanbieter nicht aufgefordert hat**, die Person, deren Daten angefordert wurden, [...] **hiervon gemäß Absatz 1 in Kenntnis zu setzen**, unterrichtet die Anordnungsbehörde diese Person. Die **Anordnungsbehörde kann die Unterrichtung der Person, deren Daten [...] angefordert wurden, in dem Maße aufschieben, in dem diese Maßnahme** notwendig und verhältnismäßig ist, um eine Behinderung von Strafverfahren zu vermeiden.

3. **Die Anordnungsbehörde kann davon absehen, die Person, deren Teilnehmer- oder Zugangsdaten angefordert wurden, zu informieren, wenn das zum Schutz der Grundrechte und der berechtigten Interessen einer anderen Person notwendig und verhältnismäßig ist und insbesondere, wenn diese Rechte und Interessen gegenüber dem Interesse der Person, deren Daten angefordert wurden, an einer entsprechenden Unterrichtung überwiegen.** […]

(4) Informationen über die zur Verfügung stehenden Rechtsbehelfe gemäß Artikel 17 werden aufgenommen.

---

37 Finnland und Deutschland haben Vorbehalte und sprechen sich für eine höhere Detailstufe aus (Bestimmungen zu Sprache, Rechtshilfe, detaillierte Informationen zu Rechtsbehelfen usw.); außerdem ist Deutschland der Auffassung, dass betroffene Personen (nicht nur die Person, deren Daten angefordert werden) informiert werden sollten.

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. **[…] Die Mitgliedstaaten teilen der Kommission die Regeln für die Kostenerstattung mit, die von der Kommission veröffentlicht werden.**

Artikel **12a** […]
[…] **Beschränkungen für die Nutzung eingeholter Daten**

1. […] **Wenn die Person, deren Daten angefordert werden, ihren Wohnsitz nicht im Hoheitsgebiet des Anordnungsstaats hat und** durch die Europäische Herausgabeanordnung [...] Transaktions- oder Inhaltsdaten **eingeholt wurden und die Anordnungsbehörde darüber informiert wird, dass diese Daten** durch Immunitäten oder Vorrechte nach dem Recht des **Vollstreckungsstaats** geschützt sind **oder Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien unterliegen** oder sich **die Offenlegung dieser Daten, sofern sich dieser Mitgliedstaat darauf beruft,** auf grundlegende Interessen dieses Mitgliedstaats wie die nationale Sicherheit und Verteidigung auswirken **würde**, stellen die zuständigen Behörden des Anordnungsstaats [...] während des Strafverfahrens […] sicher, dass diese Gründe genauso berücksichtigt werden als wären sie im nationalem Recht vorgesehen. [...] **Die zuständigen Behörden** können die Behörden des betreffenden Mitgliedstaats, das Europäische Justizielle Netz für Strafsachen oder Eurojust konsultieren.

(2) **Wenn eine Behörde des Vollstreckungsstaats für die Aufhebung des Vorrechts oder der Immunität zuständig ist, kann die zuständige Behörde des Anordnungsstaats die Vollstreckungsbehörde oder die notifizierte Behörde ersuchen, die zuständige Behörde des Vollstreckungsstaats zu kontaktieren, um sie unverzüglich um die Ausübung ihrer Zuständigkeit zu ersuchen. Ist eine Behörde eines anderen Mitgliedstaats oder eines Drittstaats oder eine internationale Organisation für die Aufhebung des Vorrechts oder der Immunität zuständig, so kann die zuständige Behörde des Anordnungsstaats die betreffende Behörde um Ausübung dieser Zuständigkeit ersuchen.**

Artikel 12b
Grundsatz der Spezialität

1. Elektronische Beweismittel werden nur für die Zwecke der Verfahren verwendet, für die sie im Einklang mit dieser Verordnung eingeholt wurden, es sei denn, sie werden verwendet:

a) für die Zwecke von Verfahren, für die gemäß Artikel 5 Absätze 3 und 4 eine Europäische Herausgabeanordnung hätte erlassen werden können, oder

b) um eine unmittelbare und schwere Bedrohung der öffentlichen Sicherheit oder der grundlegenden Interessen des Anordnungsstaats abzuwenden.

2. Im Einklang mit dieser Verordnung eingeholte elektronische Beweismittel dürfen einem anderen Mitgliedstaat nur übermittelt werden:

a) für die Zwecke von Verfahren, für die gemäß Artikel 5 Absätze 3 und 4 eine Europäische Herausgabeanordnung hätte erlassen werden können, oder oder

b) um eine unmittelbare und schwere Bedrohung der öffentlichen Sicherheit oder der grundlegenden Interessen dieses Mitgliedstaats abzuwenden.

3. **Im Einklang mit dieser Verordnung eingeholte elektronische Beweismittel dürfen einem Drittstaat oder einer internationalen Organisation nur unter den Bedingungen gemäß Absatz 2 Buchstaben a und b dieses Artikels und Kapitel V der Richtlinie (EU) 2016/680 übermittelt werden.**

Kapitel 3: Sanktionen und Vollstreckung

Artikel 13
Sanktionen[38]

Unbeschadet nationaler Rechtsvorschriften, die die Verhängung strafrechtlicher Sanktionen vorsehen, erlassen die Mitgliedstaaten Vorschriften über finanzielle Sanktionen, die bei Verstößen gegen die Verpflichtungen aus Artikel 9, Artikel 10 und Artikel 11 **Absatz 1** zu verhängen sind, und treffen alle für die Anwendung finanzieller Sanktionen erforderlichen Maßnahmen. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen sowie diesbezügliche spätere Änderungen unverzüglich mit.

Die **Mitgliedstaaten stellen sicher, dass die** finanziellen Sanktionen [...] wirksam, verhältnismäßig und abschreckend **sind**.

Die Mitgliedstaaten stellen sicher, dass finanzielle Sanktionen in Höhe von bis zu 2 % des im vorhergehenden Geschäftsjahr weltweit erzielten Jahresgesamtumsatzes des Diensteanbieters verhängt werden können.

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 [...] **von dem** betreffenden Mitgliedstaat **akzeptierten Sprachen** und setzt den Adressaten von der Übermittlung in Kenntnis.

(2) Nach dem Erhalt erkennt die Vollstreckungsbehörde **die Vollstreckung der folgenden Anordnungen** ohne weitere Formalitäten an und ergreift die zu ihrer Vollstreckung erforderlichen Maßnahmen**:**

a) **eine** Europäische Herausgabeanordnung**, es sei denn, die Vollstreckungsbehörde ist der Auffassung, dass einer der in Absatz 4 genannten Gründe zutrifft** oder

b) eine Europäische Sicherungsanordnung [...], es sei denn, die Vollstreckungsbehörde ist der Auffassung, dass einer der in [...] Absatz 5 genannten Gründe zutrifft [...].

Die Vollstreckungsbehörde beschließt die Anerkennung der Anordnung unverzüglich, spätestens jedoch fünf Arbeitstage nach Erhalt der Anordnung.

---

38 Finnland, Deutschland und Lettland haben Vorbehalte bezüglich der Harmonisierung von Sanktionen.

(2a) Artikel 5 Absatz 8 gilt entsprechend.

(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 [...] Absatz 4 **Buchstaben a bis e** oder Absatz 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. [...] **Die Anerkennung oder** Vollstreckung der Europäischen Herausgabeanordnung kann nur aus folgenden Gründen **abgelehnt werden**:

(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 [...] 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) **einer der Gründe gemäß Artikel 12a Absatz 1 findet Anwendung**[39]**.**

5. [...] **Die Anerkennung oder** Vollstreckung der Europäischen Sicherungsanordnung **kann** nur aus folgenden Gründen **abgelehnt werden**:

(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 [...] 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) […]

---

39 Die Tschechische Republik, Finnland, Ungarn, Deutschland und Lettland haben Vorbehalte bezüglich der Streichung von Artikel 14 Absatz 4 Buchstabe f und Artikel 14 Absatz 5 Buchstabe e; die Streichung ist aus ihrer Sicht nur hinnehmbar, wenn in Artikel 5, Artikel 7a Absatz 2 und Artikel 12a Absatz 1 eine Klausel über Grundrechte und über die Wahrung der nationalen verfassungsrechtlichen Bestimmungen aufgenommen wird.

(6) Erhebt der Adressat **gemäß Absatz 4 Buchstaben a bis e und Absatz 5** 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 **oder durch Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien** 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
[…]

[…]

[…]

Artikel 16
Überprüfungsverfahren bei einander widersprechenden Verpflichtungen […]

1. Ist der Adressat der Ansicht, dass die Befolgung einer Europäischen Herausgabeanordnung im Widerspruch zu den geltenden Rechtsvorschriften eines Drittstaats stehen würde, [...] so teilt er der Anordnungsbehörde gemäß dem Verfahren des Artikels 9 **Absätze** 5 **und 6** 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. **Er wird spätestens zehn Tage nach Eingang des EPOC beim Adressaten erhoben. Die Fristen werden im Einklang mit dem nationalen Recht der Anordnungsbehörde berechnet.**

(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 **aufzuheben** ist [...]**. Diese Bewertung** stützt sich [...] insbesondere auf folgende Faktoren, **wobei den Faktoren nach den Buchstaben a und b besondere Bedeutung beigemessen wird**:

a) das nach den einschlägigen Rechtsvorschriften des Drittstaats geschützte Interesse, einschließlich **der Grundrechte und anderer Interessen** des Drittstaats**, insbesondere der nationalen Sicherheit, die eine** Offenlegung der Daten **verhindern**;

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.

(5b) **Das Gericht kann die zuständige Behörde des Drittstaats unter Berücksichtigung der Richtlinie (EU) 2016/680, insbesondere des Kapitels V, um Informationen ersuchen, soweit das betreffende Strafverfahren dadurch nicht behindert wird.**

(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[40]

1. **Unbeschadet weiterer Rechtsbehelfe, die nach dem innerstaatlichen Recht zur Verfügung stehen, haben Personen**, deren Daten im Wege einer Europäischen Herausgabeanordnung **angefordert** wurden, [...] das Recht, [...] wirksame Rechtsbehelfe gegen die Europäische Herausgabeanordnung einzulegen. Handelt es sich bei der Person [...] um einen [...] Beschuldigten [...], so hat der Betreffende [...] das Recht, **während des Strafverfahrens, in dem die Daten verwendet wurden,** wirksame Rechtsbehelfe [...] einzulegen. **Diese Rechtsbehelfe stehen** unbeschadet der nach der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 verfügbaren Rechtsbehelfe **zur Verfügung.**

(2) […]

(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.

---

40 Deutschland hat einen Vorbehalt, weil aus seiner Sicht nicht nur jede Person, deren Daten angefordert wurden, sondern jede von einer Anordnung betroffene Person Anspruch auf Rechtsbehelfe haben sollte und auch in Strafverfahren gegen Herausgabeanordnungen Rechtsbehelfe zur Verfügung stehen sollten.

(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
[…]

[…]

Kapitel 5: Schlussbestimmungen

Artikel 18a
Sprachenregelung

Jeder Mitgliedstaat gibt an, ob und in welcher Sprache bzw. welchen Sprachen, die in seinem Hoheitsgebiet keine Amtssprache(n) ist bzw. sind, er die Übermittlung des EPOC oder des EPOC-PR und/oder – im Fall der Vollstreckung – einer Europäischen Herausgabeanordnung und einer Europäischen Sicherungsanordnung akzeptiert.

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 **nach Möglichkeit**:

(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**, Ex-post-Validierung**);

(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**;**

(f) **die Zahl der Fälle, in denen keine Ex-post-Validierung gewährt wurde**.

(3) Diensteanbieter können Statistiken erfassen, führen und veröffentlichen, und gegebenenfalls erfasste Daten für das vorangegangene Kalenderjahr bis zum 31. März der Kommission übermitteln; dazu können, soweit möglich, die folgenden Daten gehören:

(a) die Zahl der eingegangenen EPOC und EPOC-PR, aufgeschlüsselt nach Art der angeforderten Daten, Mitgliedstaat und Situation (Notfall oder nicht);

(b) die Zahl der EPOC, denen Folge geleistet und denen nicht Folge geleistet wurde, aufgeschlüsselt nach Art der angeforderten Daten, Mitgliedstaat und Situation (Notfall oder nicht);

(c) im Falle von EPOC, denen Folge geleistet wurde, die Zeit, die im Durchschnitt bis zum Erhalt der angeforderten Daten – vom Zeitpunkt des Eingangs eines EPOC bis zum Zeitpunkt der Bereitstellung der Daten – vergeht, aufgeschlüsselt nach Art der angeforderten Daten, Mitgliedstaat und Situation (Notfall oder nicht).

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[41] 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.

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

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 **oder diesbezügliche Notifizierungen** zu erlassen**,** zu validieren**, zu übermitteln und/oder zu empfangen**;

(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 [...] Artikel [...] 16 zu befassen;

(d) **die Sprachen, die bei der Übermittlung des EPOC oder des EPOC-PR und/oder – im Fall der Vollstreckung – einer Europäischen Herausgabeanordnung und einer Europäischen Sicherungsanordnung gemäß Artikel 18a akzeptiert werden**.

(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[42] Bezug nimmt, öffentlich zugänglich.

Artikel 23
Bezug zu […] ***anderen Instrumenten, Abkommen und Vereinbarungen***

EU- und sonstige internationale Instrumente, Abkommen und Vereinbarungen über die Erhebung von Beweismitteln [...], die auch unter diese Verordnung fallen würden**, bleiben von dieser Verordnung unberührt**.

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

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 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 … [***24** 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*