VERORDNUNG (EU) 2023/1543 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 12. Juli 2023

über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

gemäß dem ordentlichen Gesetzgebungsverfahren ([2]),

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 der Kriminalität unerlässlich und sollten bestimmten Bedingungen und Garantien unterliegen, welche die uneingeschränkte Einhaltung der in Artikel 6 des Vertrags über die Europäische Union (EUV) und der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) anerkannten Grundrechte und Grundsätze sicherstellen, insbesondere der Grundsätze der Notwendigkeit und Verhältnismäßigkeit, des ordnungsgemäßen Verfahrens, des Schutzes der Privatsphäre und der personenbezogenen Daten sowie der Vertraulichkeit der Kommunikation.

(3) In der Gemeinsamen Erklärung der Minister für Justiz und Inneres und der Vertreter der Organe der Union vom 24. März 2016 zu den Terroranschlägen in Brüssel wurde betont, dass vorrangig digitale Beweismittel schneller und wirksamer gesichert und erlangt werden müssen und dass konkrete Maßnahmen hierfür ermittelt werden müssen.

(4) In den Schlussfolgerungen des Rates vom 9. Juni 2016 wurden die zunehmende Bedeutung elektronischer Beweismittel in Strafverfahren und die Tatsache, dass der Schutz des Cyberspace vor Missbrauch und kriminellen Aktivitäten maßgeblich für das Wohl der Volkswirtschaften und Gesellschaften ist und die Strafverfolgungsbehörden und die 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 der Kommission und des Hohen Vertreters der Union für Außen- und Sicherheitspolitik an das Europäische Parlament und den Rat vom 13. September 2017 mit dem Titel „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“ 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 Geschwindigkeit von Cyber-Angriffen kann die aktuellen Verfahren mitunter überfordern und schafft so einen besonderen Bedarf für eine zügige grenzüberschreitende Zusammenarbeit.

(6) Das Europäische Parlament hob in seiner Entschließung vom 3. Oktober 2017 zur Bekämpfung der Cyberkriminalität ([3]) hervor, dass Mittel und Wege für eine schnellere Sicherung und Erlangung von elektronischen Beweismitteln gefunden werden müssen und dass die enge Zusammenarbeit zwischen den Strafverfolgungsbehörden, Drittstaaten und im Gebiet der Union tätigen Diensteanbietern im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([4]), der Richtlinie (EU) 2016/680 des Europäischen Parlaments und

([1]) ABl. C 367 vom 10.10.2018, S. 88.
([2]) Standpunkt des Europäischen Parlaments vom 13. Juni 2023 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 27. Juni 2023.
([3]) ABl. C 346 vom 27.9.2018, S. 29.
([4]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

des Rates ([5]) und bestehender Rechtshilfeabkommen wichtig ist. Das Europäische Parlament betonte in seiner Entschließung außerdem, dass die derzeit fragmentierten rechtlichen Rahmenbedingungen Herausforderungen für Diensteanbieter schaffen können, die darum bemüht sind, den Ersuchen von Strafverfolgungsbehörden nachzukommen, forderte die Kommission auf, einen Vorschlag für einen Rechtsrahmen der Union für elektronische Beweismittel mit ausreichenden Garantien hinsichtlich der Rechte und Freiheiten aller Betroffenen vorzulegen, und begrüßte die laufenden Arbeiten der Kommission an einer Kooperationsplattform, die einen sicheren Kommunikationskanal für den digitalen Austausch von Europäischen Ermittlungsanordnungen zu elektronischen Beweismitteln umfassen und der Kommunikation zwischen den Justizbehörden in der Union dienen soll.

(7) Netzbasierte Dienstleistungen können von einem beliebigen Ort aus erbracht werden und erfordern keine physische Infrastruktur, Räumlichkeiten oder Personal in dem Land, in dem die betreffende Dienstleistung angeboten wird. Daher werden relevante elektronische Beweismittel häufig außerhalb des ermittelnden Staates oder von einem außerhalb dieses Staates niedergelassenen Diensteanbieter gespeichert, was Herausforderungen bezüglich der Einholung elektronischer Beweismittel in Strafverfahren schafft.

(8) Aufgrund der Art und Weise, in der netzbasierte Dienstleistungen erbracht werden, werden Ersuchen um justizielle Zusammenarbeit häufig an Staaten gerichtet, in denen viele Diensteanbieter niedergelassen sind. Zudem hat sich die Zahl der Ersuchen aufgrund der Tatsache, dass netzbasierte Dienstleistungen immer stärker genutzt werden, vervielfacht. Die Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates ([6]) sieht die Möglichkeit vor, dass eine Europäische Ermittlungsanordnung zur Erlangung von Beweismitteln in einem anderen Mitgliedstaat erlassen wird. Ferner ist auch in dem gemäß Artikel 34 des Vertrags über die Europäische Union vom Rat erstellten Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union ([7]) (im Folgenden: „Übereinkommen über die Rechtshilfe in Strafsachen“) die Möglichkeit vorgesehen, einen anderen Mitgliedstaat um Beweismittel zu ersuchen. Die in der Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung und im Übereinkommen über die Rechtshilfe in Strafsachen vorgesehenen Verfahren und Fristen sind jedoch für elektronische Beweismittel, die vergänglicher sind und leichter und schneller gelöscht werden könnten, möglicherweise nicht geeignet. Die Einholung elektronischer Beweismittel über Kanäle der justiziellen Zusammenarbeit dauert häufig lange, was dazu führen kann, dass die sich daraus ergebenden Indizien unter Umständen nicht mehr zur Verfügung stehen. Zudem gibt es keinen harmonisierten Rahmen für die Zusammenarbeit mit Diensteanbietern, während einige Anbieter aus Drittstaaten direkte Ersuchen um andere Daten als Inhaltsdaten, die nach geltendem nationalem Recht zulässig sind, akzeptieren. Folglich stützen sich Mitgliedstaaten nach Möglichkeit zunehmend auf Kanäle für die freiwillige direkte Zusammenarbeit mit Diensteanbietern, wobei sie unterschiedliche nationale Instrumente, Voraussetzungen und Verfahren zugrunde legen. In Bezug auf Inhaltsdaten haben einige Mitgliedstaaten einseitige Maßnahmen ergriffen, wohingegen andere sich weiterhin auf die justizielle Zusammenarbeit verlassen.

(9) Der fragmentierte Rechtsrahmen stellt Strafverfolgungsbehörden, Justizbehörden und Diensteanbieter, die zulässigen Ersuchen um elektronische Beweismittel Folge leisten wollen, vor Probleme, da sie sich zunehmend mit Rechtsunsicherheit und möglichen Gesetzeskollisionen konfrontiert sehen. Daher müssen gesonderte Vorschriften für die grenzüberschreitende justizielle Zusammenarbeit zur Sicherung und Herausgabe elektronischer Beweismittel eingeführt werden, die dem besonderen Charakter elektronischer Beweismittel gerecht werden. Diese Vorschriften sollten eine Verpflichtung für die in den Anwendungsbereich dieser Verordnung fallenden Diensteanbieter umfassen, direkt auf Ersuchen von Behörden in einem anderen Mitgliedstaat zu antworten. Diese Verordnung wird somit das bestehende Unionsrecht ergänzen und die für Strafverfolgungsbehörden, Justizbehörden und Diensteanbieter im Bereich elektronischer Beweismittel geltenden Vorschriften verdeutlichen und gleichzeitig die uneingeschränkte Achtung der Grundrechte sicherstellen.

(10) Diese Verordnung wahrt die Grundrechte und steht im Einklang mit den Grundsätzen, die in Artikel 6 EUV und in der Charta, im Völkerrecht und in internationalen Übereinkünften, bei denen die Union oder alle Mitgliedstaaten Vertragsparteien sind, darunter die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten, sowie in den Verfassungen der Mitgliedstaaten in ihren jeweiligen Anwendungsbereichen anerkannt sind. Zu diesen Rechten und Grundsätzen gehören insbesondere 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.

([5]) Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

([6]) 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).

([7]) Übereinkommen – gemäß Artikel 34 des Vertrags über die Europäische Union vom Rat erstellt – über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (ABl. C 197 vom 12.7.2000, S. 3).

(11) Diese Verordnung sollte nicht dahin gehend ausgelegt werden, dass sie es einer Vollstreckungsbehörde verbietet, eine Europäische Herausgabeanordnung abzulehnen, wenn es aufgrund objektiver Anhaltspunkte Gründe zu der Annahme gibt, dass die Europäische Herausgabeanordnung zum Zwecke der Verfolgung oder Bestrafung einer Person wegen ihres Geschlechts, ihrer Rasse, ihrer ethnischen Herkunft, ihrer Religion, ihrer sexuellen Ausrichtung oder ihrer Geschlechtsidentität, ihrer Staatsangehörigkeit, ihrer Sprache oder ihrer politischen Überzeugungen erlassen wurde oder dass die Stellung dieser Person aus einem dieser Gründe beeinträchtigt werden könnte.

(12) Der Mechanismus der Europäischen Herausgabeanordnung und der Europäischen Sicherungsanordnung für elektronische Beweismittel in Strafverfahren beruht auf dem Grundsatz des gegenseitigen Vertrauens zwischen den Mitgliedstaaten und der Vermutung der Einhaltung des Unionsrechts und der Rechtsstaatlichkeit, und zwar insbesondere der Grundrechte, die wesentliche Elemente des Raums der Freiheit, der Sicherheit und des Rechts der Union sind, durch Mitgliedstaaten. Dieser Mechanismus ermöglicht es den zuständigen nationalen Behörden, diese Anordnungen direkt den Diensteanbietern zu übermitteln.

(13) Die Achtung des Privat- und Familienlebens und der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sind Grundrechte. Gemäß Artikel 7 und Artikel 8 Absatz 1 der Charta hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation sowie auf den Schutz der sie betreffenden personenbezogenen Daten.

(14) Bei der Durchführung dieser Verordnung sollten die Mitgliedstaaten sicherstellen, dass personenbezogene Daten im Einklang mit der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 sowie der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([8]) geschützt und verarbeitet werden, und zwar auch im Falle einer Weiterverwendung, Übermittlung und Weitergabe erlangter Daten.

(15) Gemäß dieser Verordnung erlangte personenbezogene Daten sollten nur verarbeitet werden, wenn dies erforderlich ist, und die Verarbeitung sollte so erfolgen, dass sie für den Zweck der Prävention, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen und der Ausübung des Rechts auf Verteidigung verhältnismäßig ist. Insbesondere sollten die Mitgliedstaaten sicherstellen, dass für die Übermittlung personenbezogener Daten von den jeweiligen Behörden an die Diensteanbieter für die Zwecke dieser Verordnung geeignete Datenschutzvorkehrungen und -maßnahmen gelten, unter anderem Maßnahmen zur Wahrung der Datensicherheit. Die Diensteanbieter sollten sicherstellen, dass für die Übermittlung personenbezogener Daten an die jeweiligen Behörden dieselben Garantien gelten. Der Zugang zu Informationen mit personenbezogenen Daten sollte befugten Personen vorbehalten sein, wofür durch Authentifizierungsverfahren gesorgt werden kann.

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

(17) Zur Gewährleistung der uneingeschränkten Achtung der Grundrechte sollte die Beweiskraft von in Anwendung dieser Verordnung erlangten Beweismitteln während des Verfahrens von der zuständigen Justizbehörde im Einklang mit dem nationalen Recht und insbesondere unter Wahrung des Rechts auf ein faires Verfahren und des Rechts auf Verteidigung geprüft werden.

([8]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

([9]) 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).

([10]) 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).

([11]) 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).

([12]) 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).

([13]) 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).

([14]) Richtlinie (EU) 2016/1919 des Europäischen Parlaments und des Rates vom 26. Oktober 2016 über Prozesskostenhilfe für Verdächtige und beschuldigte Personen in Strafverfahren sowie für gesuchte Personen in Verfahren zur Vollstreckung eines Europäischen Haftbefehls (ABl. L 297 vom 4.11.2016, S. 1).

(18) Mit dieser Verordnung werden die Regeln festgelegt, nach denen eine zuständige Justizbehörde in der Union in Strafverfahren einschließlich strafrechtliche Ermittlungen oder zur Vollstreckung einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung nach einem Strafverfahren gemäß dieser Verordnung mittels einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung von einem Diensteanbieter, der in der Union Dienste anbietet, verlangen kann, elektronische Beweismittel herauszugeben oder zu sichern. Diese Verordnung sollte in allen grenzüberschreitenden Fällen gelten, in denen der Diensteanbieter seine benannte Niederlassung oder seinen Vertreter in einem anderen Mitgliedstaat hat. Diese Verordnung berührt nicht die Befugnisse nationaler Behörden, sich an Diensteanbieter, die in dem betreffenden Hoheitsgebiet niedergelassen oder vertreten sind, zu richten, damit sie vergleichbaren nationalen Maßnahmen nachkommen.

(19) Diese Verordnung sollte nur die Erhebung von Daten regeln, die ein Diensteanbieter zum Zeitpunkt des Erhalts einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung gespeichert hat. Sie sollte keine allgemeine Verpflichtung von Diensteanbietern zur Datenspeicherung vorsehen und nicht dazu führen, dass Daten allgemein und unterschiedslos gespeichert werden. Außerdem sollte mit dieser Verordnung das Abfangen von Daten oder die Einholung von Daten, die nach Erhalt einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung gespeichert werden, nicht genehmigt werden.

(20) Die Anwendung dieser Verordnung sollte die Verwendung von Verschlüsselungstechniken durch Diensteanbieter oder deren Nutzer nicht berühren. Im Wege einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung angeforderte Daten sollten unabhängig davon, ob sie verschlüsselt sind, herausgegeben oder gesichert werden. Diese Verordnung sollte jedoch keine Verpflichtung der Diensteanbieter vorsehen, Daten zu entschlüsseln.

(21) In vielen Fällen werden die Daten nicht mehr auf dem Gerät eines Nutzers gespeichert oder anderweitig verarbeitet, sondern über eine Cloud-Infrastruktur, die den Zugang von jedem beliebigen Ort aus ermöglicht, 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.

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

(23) Da Rechtshilfeverfahren nach dem in den Mitgliedstaaten geltenden nationalen Recht unter Umständen als Strafverfahren gelten, sollte klargestellt werden, dass eine Europäische Herausgabeanordnung oder eine Europäische Sicherungsanordnung nicht erlassen werden sollte, um einem anderen Mitgliedstaat oder einem Drittland Rechtshilfe zu leisten. In solchen Fällen sollte das Rechtshilfeersuchen an den Mitgliedstaat oder das Drittland gerichtet werden, der nach seinem nationalen Recht Rechtshilfe leisten kann.

(24) Im Rahmen von Strafverfahren sollten die Europäische Herausgabeanordnung und die Europäische Sicherungsanordnung nur für bestimmte Strafverfahren, die eine konkrete, bereits begangene Straftat betreffen, und nach einer individuellen Bewertung der Notwendigkeit und der Verhältnismäßigkeit dieser Anordnungen in jedem Einzelfall erlassen werden, wobei den Rechten des Verdächtigen oder des Beschuldigten Rechnung getragen werden sollte.

(25) Diese Verordnung sollte auch für Verfahren gelten, die von einer Anordnungsbehörde eingeleitet wurden, um Verurteilte, die sich der Justiz entzogen haben, im Hinblick auf die Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung im Anschluss an ein Strafverfahren zu lokalisieren. Allerdings sollte, wenn die Freiheitsstrafe oder die freiheitsentziehende Maßregel der Sicherung im Wege einer Entscheidung in Abwesenheit ergangen ist, nicht die Möglichkeit bestehen, eine Europäische Herausgabeanordnung oder eine Europäische Sicherungsanordnung zu erlassen, da es im jeweiligen nationale Recht der Mitgliedstaaten in Bezug auf Abwesenheitsurteile in der Union große Unterschiede gibt.

(26) Diese Verordnung sollte für Diensteanbieter gelten, die in der Union Dienste anbieten, und es sollte nur möglich sein, die in dieser Verordnung vorgesehenen Anordnungen für Daten zu erlassen, die in der Union angebotene Dienste betreffen. Dienste, die ausschließlich außerhalb der Union angeboten werden, sollten nicht in den Geltungsbereich dieser Verordnung fallen, selbst wenn der Diensteanbieter in der Union niedergelassen ist. Diese Verordnung sollte daher keinen Zugang zu Daten erlauben, bei denen es sich nicht um Daten im Zusammenhang mit den dem Nutzer von den Diensteanbietern in der Union angebotenen Diensten handelt.

(27) Die für die Beweiserhebung in 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 in der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates ([15]) definiert und

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

umfassen interpersonelle Kommunikationsdienste wie die Internet-Telefonie („Voice-over-IP"), die Übermittlung von Sofortnachrichten und E-Mail-Dienste. Diese Verordnung sollte auch für Anbieter von Diensten der Informationsgesellschaft im Sinne der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ([16]) gelten, die zwar nicht als Anbieter elektronischer Kommunikationsdienste gelten, ihren Nutzern aber ermöglichen, miteinander zu kommunizieren, oder ihnen Dienste anbieten, die für die Speicherung oder anderweitige Verarbeitung von Daten in ihrem Namen genutzt werden können. Dies stünde im Einklang mit den Begriffen des am 23. November 2001 in Budapest unterzeichneten Übereinkommens des Europarats über Computerkriminalität (im Folgenden „Budapester Übereinkommen") (ETS Nr. 185). Der Begriff der Datenverarbeitung sollte im technischen Sinne ausgelegt werden und die Erstellung oder Bearbeitung von Daten bezeichnen, also technische Vorgänge, bei denen Daten mithilfe der Rechenleistung von Computern erzeugt oder verändert werden. Zu den in den Anwendungsbereich dieser Verordnung fallenden Kategorien von Diensteanbietern gehören beispielsweise Online-Marktplätze, die es 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 eine Kommunikation mit dem Diensteanbieter bietet, oder ihnen nicht ermöglicht, Daten zu speichern oder anderweitig zu verarbeiten, oder wenn die Datenspeicherung kein bestimmender, also kein wesentlicher Bestandteil der für den Nutzer erbrachten Dienstleistung ist, wie im Fall online erbrachter Rechts-, Architektur-, Ingenieur- und Buchführungsleistungen, so sollte er selbst dann nicht unter die Begriffsbestimmung des „Diensteanbieters" gemäß dieser Verordnung fallen, wenn es sich bei den von dem Diensteanbieter erbrachten Diensten um Dienste der Informationsgesellschaft im Sinne der Richtlinie (EU) 2015/1535 handelt.

(28) Anbieter von Internetinfrastrukturdiensten im Zusammenhang mit der Zuweisung von Namen und Nummern wie Domänennamen-Register und -Registrierungsstellen 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 die Identifizierung einer Person oder eines Rechtsträgers hinter einer für kriminelle Aktivitäten verwendeten Website oder des Opfers einer kriminellen Aktivität ermöglichen könnten.

(29) Damit festgestellt werden kann, ob ein Diensteanbieter Dienste in der Union anbietet, muss geprüft werden, ob der Diensteanbieter natürliche oder juristische Personen in einem oder mehreren Mitgliedstaaten in die Lage versetzt, seine Dienste in Anspruch zu nehmen. Allerdings sollte die bloße Zugänglichkeit einer Online-Schnittstelle in der Union, beispielsweise die Zugänglichkeit einer Website oder einer E-Mail-Adresse oder anderer Kontaktdaten eines Diensteanbieters oder eines Vermittlers, für sich genommen nicht als ausreichend angesehen werden, um festzustellen, ob ein Diensteanbieter Dienste im Sinne dieser Verordnung in der Union anbietet.

(30) Eine wesentliche Verbindung zur Union sollte für die Feststellung, ob ein Diensteanbieter in der Union Dienste anbietet, ebenfalls relevant sein. Eine solche wesentliche Verbindung zur Union sollte dann als gegeben gelten, wenn der Diensteanbieter eine Niederlassung in der Union hat. Gibt es eine solche Niederlassung nicht, sollte die Feststellung einer wesentlichen Verbindung auf Kriterien beruhen, die an bestimmte sachliche Gegebenheiten anknüpfen, wie beispielsweise eine erhebliche Zahl von Nutzern in einem oder mehreren Mitgliedstaaten oder die Ausrichtung der Tätigkeit eines Diensteanbieters auf einen oder mehrere Mitgliedstaaten. Die Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten sollte auf der Grundlage aller relevanten Umstände bestimmt werden, einschließlich Faktoren wie der Verwendung einer in dem betreffenden Mitgliedstaat gebräuchlichen Sprache oder Währung oder der Möglichkeit, Waren oder Dienste zu bestellen. Ferner ließe sich die Ausrichtung von Tätigkeiten auf einen Mitgliedstaat auch aus der Verfügbarkeit einer Anwendung („App") im jeweiligen nationalen App-Store, der Schaltung lokaler Werbung oder von Werbung in der im betreffenden Mitgliedstaat gebräuchlichen Sprache oder dem Management der Kundenbeziehungen, zum Beispiel durch die Bereitstellung eines Kundendienstes in der im betreffenden Mitgliedstaat gebräuchlichen Sprache, ableiten. Das Vorhandensein einer wesentlichen Verbindung sollte auch dann angenommen werden, wenn ein Diensteanbieter seine Tätigkeit gemäß der Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates ([17]) auf einen oder mehrere Mitgliedstaaten ausrichtet. Andererseits sollte die Erbringung einer Dienstleistung zum Zwecke der bloßen Einhaltung des in der Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates ([18]) festgelegten Verbots der Diskriminierung nicht allein aus diesem Grund als Ausrichtung von Tätigkeiten auf ein bestimmtes Gebiet innerhalb der Union betrachtet werden. Bei der Feststellung, ob ein Diensteanbieter Dienste in einem Mitgliedstaat anbietet, sollten dieselben Kriterien herangezogen werden.

([16]) 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).

([17]) 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).

([18]) 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 60 I vom 2.3.2018, S. 1).

(31) Diese Verordnung sollte die Datenkategorien der Teilnehmerdaten, der Verkehrsdaten und der Inhaltsdaten abdecken. Diese Kategorisierung steht im Einklang mit dem Recht vieler Mitgliedstaaten, dem Unionsrecht, wie der Richtlinie 2002/58/EG, und der Rechtsprechung des Gerichtshofs sowie dem Völkerrecht, insbesondere dem Budapester Übereinkommen.

(32) IP-Adressen sowie Zugangsnummern und damit zusammenhängende Informationen können einen entscheidenden Ausgangspunkt für strafrechtliche Ermittlungen darstellen, bei denen die Identität eines Verdächtigen nicht bekannt ist. Sie gehören üblicherweise zu einer Aufzeichnung von Ereignissen, dem sogenannten „Server-Protokoll", die den Beginn und die Beendigung der Zugangssitzung eines Nutzers in Bezug auf einen Dienst anzeigt. Welche Netzschnittstelle während der Zugangssitzung verwendet wird, wird häufig durch eine individuelle (statische oder dynamische) IP-Adresse oder eine andere Kennung gekennzeichnet. Es werden mit dem Beginn und der Beendigung der Zugangssitzung eines Nutzers in Bezug auf einen Dienst zusammenhängende Informationen wie etwa Quellports und Zeitstempel benötigt, da IP-Adressen häufig von Nutzern gemeinsam genutzt werden, wenn beispielsweise eine Netzwerkadressübersetzung auf Betreiberebene (CGN) oder technische Entsprechungen zum Einsatz kommen. Nach Maßgabe des Besitzstands der Union sind IP-Adressen jedoch als personenbezogene Daten zu betrachten und müssen in vollem Umfang durch den Unionsbesitzstand im Bereich des Datenschutzes geschützt werden. Darüber hinaus können IP-Adressen unter bestimmten Umständen als Verkehrsdaten gelten. In einigen Mitgliedstaaten gelten auch Zugangsnummern und damit zusammenhängende Informationen als Verkehrsdaten. Für den Zweck einer bestimmten strafrechtlichen Ermittlung müssen die Strafverfolgungsbehörden jedoch unter Umständen eine IP-Adresse sowie Zugangsnummern und damit zusammenhängende Informationen ausschließlich zum Zweck der Identifizierung des Nutzers anfordern, bevor die Teilnehmerdaten für diese Kennung beim Diensteanbieter angefordert werden können. In solchen Fällen sollte die gleiche Regelung wie für Teilnehmerdaten im Sinne dieser Verordnung gelten.

(33) Wenn IP-Adressen, Zugangsnummern und damit zusammenhängende Informationen nicht ausschließlich zum Zweck der Identifizierung des Nutzers in einer bestimmten strafrechtlichen Ermittlung angefordert werden, so werden sie üblicherweise angefordert, um Informationen zu erlangen, die eher in die Persönlichkeitssphäre der Betroffenen eingreifen, wie zum Beispiel die Kontakte und den Aufenthaltsort des Nutzers. Daten dieser Art könnten zur Erstellung eines umfassenden Profils einer betroffenen Person herangezogen werden, können aber auch einfacher verarbeitet und analysiert werden als Inhaltsdaten, weil sie in einem strukturierten und standardisierten Format dargestellt werden. Es ist daher unabdingbar, dass in solchen Fällen IP-Adressen, Zugangsnummern und damit zusammenhängende Informationen, wenn sie nicht ausschließlich zum Zweck der Identifizierung des Nutzers in einer bestimmten strafrechtlichen Ermittlung angefordert werden, wie Verkehrsdaten behandelt werden und nach derselben Regelung wie Inhaltsdaten im Sinne dieser Verordnung angefordert werden.

(34) Alle Datenkategorien enthalten personenbezogene Daten und fallen somit unter die Garanien im Rahmen der Datenschutzvorschriften der Union. Die Intensität der Auswirkungen auf die Grundrechte variiert jedoch zwischen den Kategorien, insbesondere zwischen Teilnehmerdaten und Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, einerseits und Verkehrsdaten, mit Ausnahme von Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, und Inhaltsdaten andererseits. Während Teilnehmerdaten sowie IP-Adressen, Zugangsnummern und damit zusammenhängende Informationen, sofern sie ausschließlich zum Zweck der Identifizierung des Nutzers angefordert werden, nützlich sein könnten, um bei einer Untersuchung erste Hinweise zur Identität eines Verdächtigen zu erhalten, sind Verkehrsdaten mit Ausnahme von Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, und Inhaltsdaten als Beweismittel häufig relevanter. Daher ist es von wesentlicher Bedeutung, dass alle diese Datenkategorien von dieser Verordnung abgedeckt werden. Wegen des unterschiedlichen Ausmaßes des Eingriffs in die Grundrechte sollten entsprechende Garantien und Voraussetzungen für die Einholung solcher Daten festgelegt werden.

(35) Situationen, in denen eine unmittelbare Gefahr für das Leben, die körperliche Unversehrtheit oder die Sicherheit einer Person besteht, sollten als Notfälle behandelt werden und kürzere Fristen für den Diensteanbieter und die Vollstreckungsbehörde vorsehen. Wenn die Störung oder Zerstörung einer kritischen Infrastruktur im Sinne der Richtlinie 2008/114/EG des Rates ([19]) eine solche Gefahr birgt, einschließlich der schweren Beeinträchtigung der Bereitstellung der Grundversorgung für die Bevölkerung oder der Wahrnehmung der Kernfunktionen des Staates, sollte eine solche Situation ebenfalls als Notfall gemäß dem Unionsrecht behandelt werden.

(36) Wenn eine Europäische Herausgabeanordnung oder eine Europäische Sicherungsanordnung erlassen wird, sollte stets eine Justizbehörde entweder am Erlass oder an der Validierung der Anordnung beteiligt sein. Da Verkehrsdaten mit Ausnahme von Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, und Inhaltsdaten sensibler sind, muss der Erlass oder die Validierung einer Europäischen Herausgabeanordnung zur Erlangung von Daten dieser Kategorien von einem Richter überprüft werden. Da Teilnehmerdaten und Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne

([19]) 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).

dieser Verordnung angefordert werden, weniger sensibel sind, kann eine Europäische Herausgabeanordnung zur Erlangung dieser Daten auch von einem zuständigen Staatsanwalt erlassen oder validiert werden. Im Einklang mit dem in der Charta und der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten geschützten Recht auf ein faires Verfahren nehmen Staatsanwälte ihre Aufgaben objektiv wahr, treffen ihre Entscheidung über den Erlass oder die Validierung einer Europäischen Herausgabeanordnungen oder einer Europäischen Sicherungsanordnung ausschließlich auf der Grundlage des in der Verfahrensakte dargelegten Sachverhalts und berücksichtigen sämtliche belastenden und entlastenden Beweismittel.

(37) Im Interesse der uneingeschränkten Wahrung der Grundrechte sollte die Validierung von Europäischen Herausgabeanordnungen oder Europäischen Sicherungsanordnungen durch die Justizbehörden grundsätzlich vor dem Erlass der jeweiligen Anordnung erwirkt werden. Von diesem Grundsatz sollte nur in hinreichend begründeten Notfällen abgewichen werden, wenn die Herausgabe von Teilnehmerdaten oder Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, oder die Sicherung von Daten angestrebt werden 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. Diese Ausnahmen sollten jedoch nur gemacht werden, wenn die die betreffende Anordnung erlassende Behörde in einem vergleichbaren nationalen Fall nach nationalem Recht ohne vorherige Validierung eine Anordnung erlassen könnte.

(38) Eine Europäische Herausgabeanordnung sollte nur erlassen werden, wenn dies notwendig, verhältnismäßig, angemessen und für den vorliegenden Fall geeignet ist. Die Anordnungsbehörde sollte den Rechten des Verdächtigen oder des Beschuldigten in Verfahren im Zusammenhang mit einer Straftat Rechnung tragen und nur dann eine Europäische Herausgabeanordnung erlassen, wenn diese Anordnung in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen hätte erlassen werden können. Bei der Prüfung der Frage, ob eine Europäische Herausgabeanordnung zu erlassen ist, sollte berücksichtigt werden, ob die Anordnung auf das Maß beschränkt ist, das unbedingt erforderlich ist, um das rechtmäßige Ziel der Erlangung von Daten, die in einem Einzelfall als Beweismittel relevant und notwendig sind, zu erreichen.

(39) Wenn eine Europäische Herausgabeanordnung zur Erlangung von Daten verschiedener Datenkategorien erlassen wird, sollte die Anordnungsbehörde sicherstellen, dass die Voraussetzungen und Verfahren, beispielsweise die Unterrichtung der Vollstreckungsbehörde, für alle betroffenen Datenkategorien eingehalten werden.

(40) Da Verkehrsdaten mit Ausnahme von Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, und Inhaltsdaten sensibler sind, sollte in Bezug auf den sachlichen Anwendungsbereich dieser Verordnung eine Unterscheidung getroffen werden. Es sollte möglich sein, für jegliche Straftat eine Europäische Herausgabeanordnung zu erlassen, um Teilnehmerdaten oder Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, zu erlangen, während für eine Europäische Herausgabeanordnung zur Erlangung von Verkehrsdaten mit Ausnahme von Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, oder zur Erlangung von Inhaltsdaten strengere Anforderungen gelten sollten, um dem sensibleren Charakter dieser Daten Rechnung zu tragen. In dieser Verordnung sollte ein Mindeststrafmaß in Bezug auf ihren Anwendungsbereich vorgesehen sein, das ein verhältnismäßigeres Vorgehen ermöglicht; außerdem sind 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 dieses Mindeststrafmaß die Wirksamkeit dieser Verordnung und ihre Anwendung durch die Praktiker nicht einschränken. Den Erlass von Europäischen Herausgabeanordnungen in Strafverfahren nur für Straftaten zuzulassen, die mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden, begrenzt den Anwendungsbereich dieser Verordnung auf schwerere Straftaten, ohne die Möglichkeiten ihrer Anwendung durch die Praktiker übermäßig zu beeinträchtigen. Diese Begrenzung schließt eine erhebliche Zahl von Straftaten vom Anwendungsbereich dieser Verordnung aus, die, wie sich an einem niedrigeren Höchststrafmaß zeigt, von den Mitgliedstaaten als weniger schwerwiegend eingestuft werden. Diese Begrenzung hat auch den Vorteil der leichten Anwendbarkeit in der Praxis.

(41) 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 könnten, insbesondere Straftaten 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 dazu führen, dass Straftaten in großem Umfang ungeahndet bleiben. Dies rechtfertigt die Anwendung dieser Verordnung bei solchen Straftaten auch dann, wenn diese mit einer Freiheitsstrafe im Höchstmaß von weniger als drei Jahren geahndet werden. Zudem sollte bei Straftaten im Zusammenhang mit Terrorismus im Sinne der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates ([20]) sowie bei Straftaten im Zusammenhang mit dem sexuellen Missbrauch und der

([20]) 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).

sexuellen Ausbeutung von Kindern im Sinne der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates ([21]) kein Mindeststrafmaß in Form einer Freiheitsstrafe im Höchstmaß von drei Jahren erforderlich sein.

(42) Eine Europäische Herausgabeanordnung sollte grundsätzlich an den Diensteanbieter gerichtet werden, der als Verantwortlicher fungiert. Unter bestimmten Umständen kann sich die Feststellung, ob ein Diensteanbieter als Verantwortlicher oder als Auftragsverarbeiter fungiert, jedoch als besonders schwierig erweisen, was insbesondere dann zutrifft, wenn mehrere Diensteanbieter an der Verarbeitung von Daten beteiligt sind oder wenn Diensteanbieter die Daten für eine natürliche Person verarbeiten. Für die Unterscheidung zwischen der Funktion des Verantwortlichen und der Funktion des Auftragsverarbeiters für einen bestimmten Datensatz bedarf es nicht nur spezieller Kenntnisse des Rechtsrahmens, sondern es müssen möglicherweise auch häufig sehr komplexe Vertragswerke ausgelegt werden, in denen in einem bestimmten Fall verschiedene Aufgaben und Funktionen mit Blick auf einen bestimmten Datensatz verschiedenen Diensteanbietern zugewiesen werden. Wenn Diensteanbieter für eine natürliche Person Daten verarbeiten, kann die Feststellung, wer der Verantwortliche ist, mitunter auch dann schwierig sein, wenn nur ein Diensteanbieter beteiligt ist. Wenn die betreffenden Daten von einem Diensteanbieter gespeichert oder anderweitig verarbeitet werden und es trotz verhältnismäßiger Bemühungen seitens der Anordnungsbehörde nicht klar ist, wer der Verantwortliche ist, sollte es daher möglich sein, eine Europäische Herausgabeanordnung direkt an den Diensteanbieter zu richten. Mitunter könnte es außerdem die Ermittlungen in dem jeweiligen Fall gefährden, wenn die Anordnung an den Verantwortlichen gerichtet wird, weil der Verantwortliche beispielsweise Verdächtiger, Angeklagter oder Verurteilter ist oder es Hinweise darauf gibt, dass der Verantwortliche möglicherweise im Interesse der Person handelt, gegen die ermittelt wird. Auch in diesen Fällen sollte es möglich sein, eine Europäische Herausgabeanordnung unmittelbar an den Diensteanbieter zu richten, der die Daten für den Verantwortlichen verarbeitet. Dies sollte nicht das Recht der Anordnungsbehörde berühren, vom Diensteanbieter die Sicherung der Daten zu verlangen.

(43) Im Einklang mit der Verordnung (EU) 2016/679 sollte der Auftragsverarbeiter, der die Daten für den Verantwortlichen speichert oder anderweitig verarbeitet, den Verantwortlichen über die Herausgabe der Daten informieren, es sei denn, die Anordnungsbehörde hat den Diensteanbieter aufgefordert, diese Information des Verantwortlichen so lange wie notwendig und verhältnismäßig aufzuschieben, um das einschlägige Strafverfahren nicht zu behindern. In diesem Fall sollte die Anordnungsbehörde in der Verfahrensakte die Gründe für die Aufschiebung bei der Information des Verantwortlichen angeben, und der begleitenden Bescheinigung, das dem Adressaten übermittelt wird, sollte eine kurze Begründung beigefügt werden.

(44) Wenn die Daten im Rahmen einer Infrastruktur, die ein Diensteanbieter einer Behörde bereitstellt, gespeichert oder anderweitig verarbeitet werden, sollte nur dann eine Europäische Herausgabeanordnung oder eine Europäische Sicherungsanordnung erlassen werden können, wenn sich die Behörde, für die die Daten gespeichert oder anderweitig verarbeitet werden, im Anordnungsstaat befindet.

(45) In Fällen, in denen Daten, die gemäß dem Recht des Anordnungsstaats vom Berufsgeheimnis geschützt sind, von einem Diensteanbieter im Rahmen einer Infrastruktur gespeichert oder anderweitig verarbeitet werden, die Geschäftspersonen in ihrer Geschäftstätigkeit bereitgestellt wird, die dem Berufsgeheimnis unterliegen (im Folgenden „Berufsgeheimnisträger“), sollte eine Europäische Herausgabeanordnung nur für die Erlangung von Verkehrsdaten, mit Ausnahme von Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, oder für die Erlangung von Inhaltsdaten erlassen werden können, wenn der Berufsgeheimnisträger im Anordnungsstaat wohnhaft ist, wenn es der Ermittlung schaden könnte, wenn die Anordnung an den Berufsgeheimnisträger gerichtet wird, oder wenn das Berufsgeheimnis im Einklang mit dem geltenden Recht aufgehoben wurde.

(46) Der Grundsatz „ne bis in idem“ ist ein wesentlicher Rechtsgrundsatz der Union, der in der Charta anerkannt wird und durch die Rechtsprechung des Gerichtshofs der Europäischen Union weiterentwickelt wurde. Hat die Anordnungsbehörde Grund zu der Annahme, dass in einem anderen Mitgliedstaat möglicherweise ein paralleles Strafverfahren im Gange ist, sollte sie die Behörden dieses Mitgliedstaats gemäß dem Rahmenbeschluss 2009/948/JI des Rates ([22]) konsultieren. In keinem Fall darf eine Europäische Herausgabeanordnung oder eine Europäische Sicherungsanordnung erlassen werden, wenn die Anordnungsbehörde Grund zu der Annahme hat, dass dies dem Grundsatz „ne bis in idem“ zuwiderlaufen würde.

(47) 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 von Journalisten auf Quellenschutz) wird in anderen Instrumenten zur gegenseitigen Anerkennung wie der Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung eingegangen. Der Umfang und die Auswirkungen von Immunitäten und Vorrechten unterscheiden sich je nach dem geltenden nationalen Recht, das bei Erlass einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung berücksichtigt werden sollte, da die Anordnungsbehörde die Anordnung nur dann erlassen können sollte, wenn diese in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen hätte erlassen werden können. Es gibt im Unionsrecht keine

([21]) 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).

([22]) 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).

einheitliche Definition dessen, was eine Immunität oder ein Vorrecht darstellt. Die genaue Bestimmung dieser Begriffe bleibt daher dem nationalen Recht überlassen, wobei die Bestimmung Schutzvorschriften für beispielsweise medizinische Berufe und Rechtsberufe umfassen kann, und zwar auch dann, wenn spezielle Plattformen von diesen Berufsgruppen genutzt werden. Die genaue Bestimmung der Begriffe „Immunitäten" und „Vorrechte" kann auch Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien umfassen.

(48) Wenn die Anordnungsbehörde Verkehrsdaten, mit Ausnahme von Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, oder Inhaltsdaten erlangen möchte, indem sie eine Europäische Herausgabeanordnung erlässt, und hinreichende Gründe für die Annahme hat, dass die angeforderten Daten durch Immunitäten oder Vorrechte nach dem Recht des Vollstreckungsstaats geschützt sind oder dass diese Daten in diesem Staat Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Pressefreiheit und die Freiheit der Meinungsäußerung in anderen Medien unterliegen, so sollte die Anordnungsbehörde die Möglichkeit haben, vor dem Erlass der Europäischen Herausgabeanordnung um Klärung zu ersuchen, indem sie etwa die zuständigen Behörden des Vollstreckungsstaats entweder direkt oder über Eurojust oder das Europäische Justizielle Netz konsultiert.

(49) Eine Europäische Sicherungsanordnung sollte wegen jeder Straftat erlassen werden können. Die Anordnungsbehörde sollte den Rechten des Verdächtigen oder des Beschuldigten in Verfahren im Zusammenhang mit einer Straftat Rechnung tragen und nur dann eine Europäische Sicherungsanordnung erlassen, wenn diese Anordnung in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen hätte erlassen werden können und wenn sie notwendig, verhältnismäßig, angemessen und durchführbar ist. Bei der Prüfung der Frage, ob eine Europäische Sicherungsanordnung zu erlassen ist, sollte berücksichtigt werden, ob die Anordnung auf das Maß beschränkt ist, das unbedingt erforderlich ist, um in Situationen, in denen mehr Zeit für die Erwirkung dieser Daten benötigt werden könnte, das rechtmäßige Ziel zu erreichen, das darin besteht, die Entfernung, Löschung oder Änderung von Daten, die als Beweismittel in einem bestimmten Fall relevant und notwendig sind, zu verhindern.

(50) Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen sollten unmittelbar an die benannte Niederlassung oder den vom Diensteanbieter gemäß der Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates ([23]) bestellten Vertreter gerichtet werden. In Notfällen im Sinne der vorliegenden Verordnung, in denen die benannte Niederlassung oder der Vertreter eines Diensteanbieters nicht innerhalb der Fristen auf die begleitende Bescheinigung über eine Europäische Herausgabeanordnung (European Production Order Certificate – EPOC) oder die begleitende Bescheinigung über eine Europäische Sicherungsanordnung (European Preservation Order Certificate – EPOC-PR) reagiert oder nicht innerhalb der Fristen gemäß der Richtlinie (EU) 2023/1544 benannt beziehungsweise bestellt wurde, sollte es ausnahmsweise möglich sein, das EPOC oder das EPOC-PR an eine andere Niederlassung oder einen anderen Vertreter des Diensteanbieters in der Union zu richten, und zwar zusätzlich zu oder anstatt der Betreibung der Vollstreckung der ursprünglichen Anordnung gemäß dieser Verordnung. In Anbetracht dieser verschiedenen möglichen Szenarien wird in den Bestimmungen der vorliegenden Verordnung der allgemeine Begriff „Adressat" verwendet.

(51) In Anbetracht des sensibleren Charakters einer Europäischen Herausgabeanordnung zur Erlangung von Verkehrsdaten mit Ausnahme von Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, oder zur Erlangung von Inhaltsdaten sollte ein Unterrichtungsmechanismus für Europäische Herausgabeanordnungen, mit denen Daten dieser Kategorien angefordert werden, vorgesehen werden. Dieser Unterrichtungsmechanismus sollte eine Vollstreckungsbehörde einbinden und darin bestehen, dass das EPOC zur selben Zeit dem Adressaten und dieser Behörde übermittelt wird. Wenn eine Europäische Herausgabeanordnung erlassen wird, um elektronische Beweismittel in Strafverfahren zu erlangen, bei denen eine wesentliche und enge Verbindung zum Anordnungsstaat besteht, sollte jedoch keine Unterrichtung der Vollstreckungsbehörde erforderlich sein. Von einer solchen Verbindung sollte ausgegangen werden, wenn die Anordnungsbehörde zum Zeitpunkt des Erlasses der Europäischen Herausgabeanordnung hinreichende Gründe für die Annahme hat, dass die Straftat im Anordnungsstaat begangen wurde, dort gerade begangen wird oder vermutlich dort begangen werden wird, und wenn die Person, deren Daten angefordert werden, ihren Wohnsitz im Anordnungsstaat hat.

(52) Für die Zwecke dieser Verordnung sollte davon ausgegangen werden, dass eine Straftat im Anordnungsstaat begangen wurde, gerade begangen wird oder wahrscheinlich begangen werden wird, wenn nach dem nationalen Recht des Anordnungsstaats davon auszugehen ist. Insbesondere im Bereich der Cyberkriminalität sind in einigen Fällen einige Fakten wie etwa der Wohnsitz des Opfers in der Regel wichtige Anhaltspunkte, die bei der Bestimmung des Ortes, an dem die Straftat begangen wurde, zu berücksichtigen sind. So können beispielsweise Straftaten im Zusammenhang mit Ransomware häufig als dort begangen angesehen werden, wo das Opfer der entsprechenden Straftat seinen Wohnsitz hat, und zwar selbst dann, wenn ungewiss ist, von wo aus die Ransomware gestartet wurde. Jede Bestimmung des Ortes, an dem die Straftat begangen wurde, sollte die Vorschriften über die gerichtliche Zuständigkeit für die betreffenden Straftaten nach dem anwendbaren nationalen Recht unberührt lassen.

([23]) Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren (siehe Seite 181 dieses Amtsblatts).

(53) Es ist Sache der Anordnungsbehörde, zum Zeitpunkt des Erlasses der Europäischen Herausgabeanordnung zur Erlangung von Verkehrsdaten, die nicht ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, oder zur Erlangung von Inhaltsdaten auf der Grundlage des ihr vorliegenden Materials zu beurteilen, ob hinreichende Gründe für die Annahme bestehen, dass die Person, deren Daten angefordert werden, ihren Wohnsitz im Anordnungsstaat hat. In diesem Zusammenhang können verschiedene objektive Umstände maßgeblich sein, die darauf hindeuten könnten, dass die betreffende Person den gewöhnlichen Mittelpunkt ihrer Interessen in einem bestimmten Mitgliedstaat begründet hat oder die Absicht hat, dies zu tun. Aus der Notwendigkeit einer einheitlichen Anwendung des Unionsrechts und aus dem Gleichheitsgrundsatz ergibt sich, dass der Begriff „Wohnsitz" in diesem besonderen Zusammenhang in der gesamten Union einheitlich ausgelegt werden sollte. Berechtigte Gründe für die Annahme, dass eine Person ihren Wohnsitz in einem Anordnungsstaat hat, könnten insbesondere dann vorliegen, wenn eine Person als in einem Anordnungsstaat wohnhaft gemeldet ist, worauf der Besitz eines Personalausweises, oder die Inhaberschaft eines Aufenthaltstitels oder der Eintragung in einem amtlichen Wohnsitzregister hinweist. In Ermangelung einer Registrierung im Anordnungsstaat könnte auch die Tatsache auf einen Wohnsitz hindeuten, dass eine Person ihre Absicht bekundet hat, sich in diesem Mitgliedstaat niederzulassen, oder dass sie nach einer durchgehenden Aufenthaltszeit in diesem Mitgliedstaat bestimmte Bindungen zu diesem Staat erworben hat, die ebenso stark sind wie diejenigen, welche sich aus der Begründung eines förmlichen Wohnsitzes in diesem Mitgliedstaat ergeben. Um festzustellen, ob in einer bestimmten Situation hinreichende Bindungen zwischen der betreffenden Person und dem Anordnungsstaat bestehen, die Anlass zu der Annahme geben, dass die betreffende Person in diesem Staat wohnt, könnten verschiedene objektive Faktoren berücksichtigt werden, die die Situation dieser Person kennzeichnen und zu denen insbesondere die Dauer, die Art und die Umstände ihres Aufenthalts im Anordnungsstaat oder die familiären oder wirtschaftlichen Bindungen, die diese Person in diesem Mitgliedstaat unterhält, gehören. Ein zugelassenes Fahrzeug, ein Bankkonto, die Tatsache, dass sich die Person ununterbrochen im Anordnungsstaat aufgehalten hat, oder andere objektive Faktoren könnten für die Feststellung, dass hinreichende Gründe für die Annahme vorliegen, dass die betreffende Person im Anordnungsstaat wohnhaft ist, maßgeblich sein. Ein Kurzbesuch, ein Urlaubsaufenthalt – auch in einer Ferienwohnung oder einem Ferienhaus – oder ein ähnlich gearteter Aufenthalt im Anordnungsmitgliedstaat ohne jegliche weitere wesentliche Verbindung dürfen für die Feststellung eines Wohnsitzes in diesem Mitgliedstaat nicht als ausreichend gelten. In Fällen, in denen die Anordnungsbehörde zum Zeitpunkt des Erlasses der Europäischen Herausgabeanordnung zur Erlangung von Verkehrsdaten, die nicht ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, oder zur Erlangung von Inhaltsdaten keinen hinreichenden Grund zu der Annahme hat, dass die Person, deren Daten angefordert werden, im Anordnungsstaat wohnhaft ist, sollte die Anordnungsbehörde die Vollstreckungsbehörde davon unterrichten.

(54) Um eine zügige Abwicklung des Verfahrens zu ermöglichen, sollte bereits zum Zeitpunkt des Erlasses der Europäischen Herausgabeanordnung festgestellt werden, ob eine Unterrichtung an die Vollstreckungsbehörde erforderlich ist. Eine anschließende Änderung des Wohnsitzes sollte keinen Einfluss auf das Verfahren haben. Die betreffenden Personen sollten ihre Rechte sowie die Vorschriften über die Feststellung und Beschränkung der strafrechtlichen Verantwortlichkeit im Zusammenhang mit der Pressefreiheit und dem Recht auf freie Meinungsäußerung in anderen Medien während des gesamten Strafverfahrens geltend machen können, und die Vollstreckungsbehörde sollte in der Lage sein, einen Ablehnungsgrund geltend zu machen, wenn in Ausnahmefällen aufgrund konkreter und objektiver Belege berechtigte Gründe für die Annahme bestehen, dass die Vollstreckung der Anordnung unter den besonderen Umständen des Einzelfalls eine offensichtliche Verletzung eines einschlägigen Grundrechts nach Artikel 6 EUV und der Charta bedeuten würde. Darüber hinaus sollte es auch möglich sein, diese Gründe während des Vollstreckungsverfahrens geltend zu machen.

(55) Eine Europäische Herausgabeanordnung sollte in Form eines EPOC und eine Europäische Sicherungsanordnung sollte in Form eines EPOC-PR übermittelt werden. Im Bedarfsfall sollte das EPOC oder das EPOC-PR in eine vom Adressaten akzeptierte Amtssprache der Union übersetzt werden. Hat der Diensteanbieter keine Sprache angegeben, so sollte das EPOC oder das EPOC-PR in eine der Amtssprachen des Mitgliedstaats, in dem sich die benannte Niederlassung oder der Vertreter des Diensteanbieters befindet, oder in eine andere Amtssprache, der die benannte Niederlassung oder der Vertreter des Diensteanbieters zugestimmt hat, übersetzt werden. Ist nach dieser Verordnung eine Unterrichtung der Vollstreckungsbehörde erforderlich, so sollte das an diese Behörde zu übermittelnde EPOC in eine Amtssprache des Vollstreckungsstaats oder in eine andere von diesem Staat akzeptierte Amtssprache der Union übersetzt werden. In diesem Zusammenhang sollte jeder Mitgliedstaat aufgefordert werden, jederzeit in einer schriftlichen Erklärung, die der Kommission vorgelegt wird, anzugeben, ob und in welchen Amtssprachen der Union neben der Amtssprache oder den Amtssprachen dieses Mitgliedstaats Übersetzungen von EPOC und EPOC-PR akzeptiert werden. Die Kommission sollte die Erklärungen allen Mitgliedstaaten und dem Europäischen Justiziellen Netz zur Verfügung stellen.

(56) Wurde ein EPOC ausgestellt und ist die Unterrichtung der Vollstreckungsbehörde nach dieser Verordnung nicht erforderlich, so sollte der Adressat nach Erhalt des EPOC sicherstellen, dass die angeforderten Daten spätestens innerhalb von zehn Tagen nach Erhalt des EPOC direkt an die Anordnungsbehörde oder die im EPOC angegebenen Strafverfolgungsbehörden übermittelt werden. Ist nach dieser Verordnung eine Unterrichtung der Vollstreckungsbehörde erforderlich, so sollte der Diensteanbieter nach Erhalt des EPOC zügig tätig werden, um die Daten zu sichern. Hat die Vollstreckungsbehörde nicht innerhalb von zehn Tagen nach Erhalt des EPOC einen der in

dieser Verordnung genannten Ablehnungsgründe geltend gemacht, so sollte der Adressat dafür sorgen, dass die angeforderten Daten nach Ablauf dieser zehntägigen Frist direkt an die Anordnungsbehörde oder die im EPOC angegebenen Strafverfolgungsbehörden übermittelt werden. Bestätigt die Vollstreckungsbehörde bereits vor Ablauf der zehntägigen Frist der Anordnungsbehörde und dem Adressaten, dass sie keine Ablehnungsgründe geltend machen wird, so sollte der Adressat nach dieser Bestätigung so bald wie möglich, spätestens jedoch zum Ende dieser zehntägigen Frist, tätig werden. Die in dieser Verordnung festgelegten kürzeren Fristen für Notfälle sollten vom Adressaten und gegebenenfalls von der Vollstreckungsbehörde eingehalten werden. Der Adressat und gegebenenfalls die Vollstreckungsbehörde sollten das EPOC schnellstmöglich, spätestens jedoch innerhalb der in dieser Verordnung festgelegten Fristen vollstrecken, wobei die Verfahrensfristen und andere vom Anordnungsstaat angegebene Fristen weitestmöglich zu berücksichtigen sind.

(57) Ist der Adressat allein aufgrund der im EPOC oder im EPOC-PR enthaltenen Informationen der Auffassung, dass die Vollstreckung des EPOC oder des EPOC-PR Immunitäten oder Vorrechte oder sich auf die Pressefreiheit oder das Recht auf freie Meinungsäußerung in anderen Medien beziehende Vorschriften über die Festlegung oder Beschränkung der strafrechtlichen Verantwortlichkeit, die nach dem Recht des Vollstreckungsstaats bestehen, beeinträchtigen könnte, so sollte der Adressat die Anordnungsbehörde und die Vollstreckungsbehörde davon in Kenntnis setzen. In Bezug auf das EPOC sollte die Anordnungsbehörde in Fällen, in denen keine Unterrichtung der Vollstreckungsbehörde gemäß dieser Verordnung erfolgt ist, die vom Adressaten erhaltenen Informationen berücksichtigen und von sich aus oder auf Ersuchen der Vollstreckungsbehörde entscheiden, ob die Europäische Herausgabeanordnung zurückgenommen, angepasst oder aufrechterhalten wird. Ist eine Unterrichtung der Vollstreckungsbehörde gemäß dieser Verordnung erfolgt, sollte die Anordnungsbehörde die vom Adressaten erhaltenen Informationen berücksichtigen und entscheiden, ob die Europäische Herausgabeanordnung zurückgenommen, angepasst oder aufrechterhalten wird. Die Vollstreckungsbehörde sollte auch die Möglichkeit haben, die in dieser Verordnung genannten Ablehnungsgründe geltend zu machen.

(58) Damit der Adressat formale Probleme mit einem EPOC oder einem EPOC-PR lösen kann, muss ein Verfahren für die Kommunikation zwischen dem Adressaten und der Anordnungsbehörde sowie – wenn eine Unterrichtung der Vollstreckungsbehörde gemäß dieser Verordnung erfolgt ist – zwischen dem Adressaten und der Vollstreckungsbehörde für die Fälle festgelegt werden, in denen das EPOC oder das EPOC-PR unvollständig ist oder offensichtliche Fehler enthält oder keine ausreichenden Informationen zur Ausführung der betreffenden Anordnung enthält. Sollte der Adressat 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 Drittlands besteht oder dass die Europäische Herausgabeanordnung oder die Europäische Sicherungsanordnung nicht gemäß den in dieser Verordnung festgelegten Voraussetzungen erlassen wurde, so sollte er die Anordnungsbehörde und – wenn eine Unterrichtung der Vollstreckungsbehörde erfolgt ist – die Vollstreckungsbehörde davon in Kenntnis setzen und begründen, warum er das EPOC oder das EPOC-PR nicht fristgerecht ausführt. Das Kommunikationsverfahren sollte daher die Berichtigung oder erneute Prüfung der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung durch die Anordnungsbehörde in einem frühen Stadium ermöglichen. Um die Verfügbarkeit der angeforderten Daten zu gewährleisten, sollte der Adressat diese Daten sichern, wenn er die angeforderten Daten identifizieren kann.

(59) Der Adressat sollte nicht zur Befolgung der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung verpflichtet sein, wenn dies aufgrund von Umständen, die nicht dem Adressaten oder, falls abweichend, dem Diensteanbieter angelastet werden können, zum Zeitpunkt des Eingangs der Europäischen Herausgabeanordnung oder der Europäischen Sicherungsanordnung 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 bei der Anordnungsbehörde nicht als solcher identifiziert werden kann oder wenn die Daten vor Eingang der betreffenden Anordnung rechtmäßig gelöscht wurden.

(60) Nach Erhalt eines EPOC-PR sollte der Adressat die angeforderten Daten für höchstens 60 Tage sichern, es sei denn, die Anordnungsbehörde bestätigt, dass ein entsprechendes Ersuchen um Herausgabe gestellt wurde; in diesem Fall sollte die Sicherung der Daten fortgesetzt werden. Die Anordnungsbehörde sollte in der Lage sein, die Dauer der Sicherung erforderlichenfalls um weitere 30 Tage zu verlängern, damit ein anschließendes Ersuchen um Herausgabe ausgestellt werden kann, wobei das Formular aus dieser Verordnung zu verwenden ist. Wenn die Anordnungsbehörde während der Sicherungsfrist bestätigt, dass ein entsprechendes Ersuchen um Herausgabe gestellt wurde, sollte der Adressat die Daten so lange sichern, wie dies erforderlich ist, um die Daten nach Eingang des entsprechenden Ersuchens um Herausgabe herauszugeben. Eine solche Bestätigung sollte dem Adressaten innerhalb der entsprechenden Frist in einer Amtssprache des Vollstreckungsstaats oder in einer anderen vom Adressaten akzeptierten Sprache unter Verwendung des in dieser Verordnung vorgesehenen Formulars übermittelt werden. Um zu verhindern, dass die Sicherung beendet wird, sollte es ausreichen, dass das entsprechende Ersuchen um Herausgabe gestellt und die Bestätigung von der Anordnungsbehörde versandt wurde; es sollte nicht erforderlich sein, zu diesem Zeitpunkt weitere für die Übermittlung erforderliche Formalitäten wie die Übersetzung von Schriftstücken abzuschließen. Wenn die Sicherung nicht mehr erforderlich ist, sollte die Anordnungsbehörde den Adressaten unverzüglich hiervon in Kenntnis setzen, und die auf der Europäischen Sicherungsanordnung beruhende Sicherungspflicht sollte erlöschen.

(61) Ungeachtet des Grundsatzes des gegenseitigen Vertrauens sollte es der Vollstreckungsbehörde möglich sein, Gründe für die Ablehnung einer Europäischen Herausgabeanordnung geltend zu machen, wenn auf der Grundlage der in dieser Verordnung vorgesehenen Liste der Ablehnungsgründe gemäß dieser Verordnung eine Unterrichtung der Vollstreckungsbehörde erfolgt ist. Der Vollstreckungsstaat könnte in seinem nationalen Recht bestimmen, dass, wenn im Einklang mit dieser Verordnung eine Unterrichtung der Vollstreckungsbehörde oder die Vollstreckung erfolgt, die Ausführung einer Europäischen Herausgabeanordnung die Einbeziehung eines Gerichts im Vollstreckungsstaat erfordert.

(62) Wird die Vollstreckungsbehörde von einer Europäischen Herausgabeanordnung zur Erlangung von Verkehrsdaten, die nicht ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne dieser Verordnung angefordert werden, oder zur Erlangung von Inhaltsdaten in Kenntnis gesetzt, so sollte sie das Recht haben, die in der Anordnung angegebenen Informationen zu bewerten und diese gegebenenfalls abzulehnen, wenn sie auf der Grundlage einer obligatorischen und pflichtgemäßen Prüfung der in dieser Anordnung enthaltenen Informationen und unter Einhaltung der geltenden Vorschriften des Primärrechts der Union und insbesondere der Charta zu dem Schluss kommt, dass einer oder mehrere der in dieser Verordnung vorgesehenen Ablehnungsgründe geltend gemacht werden könnten. Die Notwendigkeit, die Unabhängigkeit der Justizbehörden zu wahren, erfordert, dass diesen bei Entscheidungen über die Ablehnungsgründe ein gewisser Ermessensspielraum eingeräumt wird.

(63) Bei Erhalt einer Unterrichtung gemäß dieser Verordnung sollte es der Vollstreckungsbehörde möglich sein, eine Europäische Herausgabeanordnung abzulehnen, wenn die angeforderten Daten durch Immunitäten oder Vorrechte geschützt sind, die nach dem Recht des Vollstreckungsstaats gewährt werden und der Ausführung oder Vollstreckung der Europäischen Herausgabeanordnung im Wege stehen, oder wenn die angeforderten Daten unter Vorschriften über die Festlegung oder Beschränkung der strafrechtlichen Verantwortlichkeit fallen, die sich auf die Pressefreiheit oder das Recht auf freie Meinungsäußerung in anderen Medien beziehen und der Ausführung oder Vollstreckung der Europäischen Herausgabeanordnung im Wege stehen.

(64) Der Vollstreckungsbehörde sollte es möglich sein, eine Anordnung in Ausnahmefällen abzulehnen, wenn auf der Grundlage konkreter und objektiver Belege berechtigte Gründe für die Annahme bestehen, dass die Ausführung der Europäischen Herausgabeanordnung unter den besonderen Umständen des Einzelfalls eine offensichtliche Verletzung eines einschlägigen Grundrechts nach Artikel 6 EUV und der Charta bedeuten würde. Insbesondere sollte die Vollstreckungsbehörde bei der Prüfung dieses Ablehnungsgrundes – wenn ihr Beweise oder Unterlagen vorliegen, wie sie etwa in einem begründeten Vorschlag eines Drittels der Mitgliedstaaten, des Europäischen Parlaments oder der Europäischen Kommission, der gemäß Artikel 7 Absatz 1 EUV angenommen wurde, dargelegt sind und aus denen hervorgeht, dass aufgrund systemischer oder allgemeiner Mängel in Bezug auf die Unabhängigkeit der Justiz des Anordnungsstaats im Falle der Ausführung der Anordnung die eindeutige Gefahr einer schwerwiegenden Verletzung des Grundrechts auf einen wirksamen Rechtsbehelf und ein faires Verfahren gemäß Artikel 47 der Charta besteht – konkret und genau feststellen, ob unter Berücksichtigung der persönlichen Situation der betreffenden Person, der Art der Straftat, die Gegenstand des Strafverfahrens ist, und des Sachverhalts, der der Anordnung zugrunde liegt, und angesichts der von der Anordnungsbehörde übermittelten Informationen wesentliche Gründe für die Annahme vorliegen, dass die Gefahr einer Verletzung des Rechts einer Person auf ein faires Verfahren besteht.

(65) Der Vollstreckungsbehörde sollte es möglich sein, eine Anordnung abzulehnen, wenn die Ausführung dieser Anordnung gegen den Grundsatz ne bis in idem verstoßen würde.

(66) Im Falle einer Unterrichtung gemäß dieser Verordnung sollte es der Vollstreckungsbehörde möglich sein, eine Europäische Herausgabeanordnung abzulehnen, wenn die Handlung, aufgrund deren die Anordnung erlassen wurde, nach dem Recht des Vollstreckungsstaats keine Straftat darstellt, es sei denn, sie betrifft eine Straftat, die unter den in einem Anhang zu dieser Verordnung aufgeführten Kategorien von Straftaten genannt wird – wie von der Anordnungsbehörde im EPOC angegeben –, sofern die Straftat im Anordnungsstaat mit einer Freiheitsstrafe oder freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren geahndet wird.

(67) Da die Information der Person, deren Daten angefordert werden, ein wesentliches Element im Hinblick auf die Datenschutzrechte und die Verteidigungsrechte insofern ist, als sie eine wirksame Überprüfung und einen wirksamen Rechtsbehelf gemäß Artikel 6 EUV und der Charta ermöglicht, sollte die Anordnungsbehörde die Person, deren Daten angefordert werden, unverzüglich über die Herausgabe von Daten auf der Grundlage einer Europäischen Herausgabeanordnung informieren. Die Anordnungsbehörde sollte jedoch im Einklang mit dem nationalen Recht die Möglichkeit haben, die Information der Person, deren Daten angefordert werden, aufzuschieben, einzuschränken oder zu unterlassen, soweit und solange die Bedingungen der Richtlinie (EU) 2016/680 erfüllt sind, wobei die Anordnungsbehörde in diesem Fall die Gründe für die Aufschiebung, Einschränkung oder Unterlassung in der Verfahrensakte vermerken und im EPOC eine kurze Begründung angeben sollte. Die Adressaten und, falls abweichend, die Diensteanbieter sollten die erforderlichen, dem neuesten Stand der Technik entsprechenden betrieblichen und technischen Maßnahmen treffen, um die Vertraulichkeit, Geheimhaltung und Integrität des EPOC oder des EPOC-PR sowie der herausgegebenen oder gesicherten Daten sicherzustellen.

(68) Einem Diensteanbieter sollte es möglich sein, vom Anordnungsstaat die Erstattung seiner Kosten für die Beantwortung einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung zu verlangen, wenn diese Möglichkeit im nationalen Recht des Anordnungsstaats für nationale Anordnungen in vergleichbaren Situationen im Einklang mit dem nationalen Recht dieses Staates vorgesehen ist. Die Mitgliedstaaten sollten der Kommission ihre nationalen Vorschriften für die Kostenerstattung mitteilen, die dann von der Kommission veröffentlicht werden. Diese Verordnung enthält gesonderte Vorschriften für die Erstattung von Kosten im Zusammenhang mit dem dezentralen IT-System.

(69) Unbeschadet nationaler Rechtsvorschriften, die die Verhängung strafrechtlicher Sanktionen vorsehen, sollten die Mitgliedstaaten Vorschriften über finanzielle Sanktionen erlassen, die bei Verstößen gegen diese Verordnung zu verhängen sind, und alle für die Anwendung dieser Sanktionen erforderlichen Maßnahmen treffen. Die Mitgliedstaaten sollten sicherstellen, dass die in ihrem nationalen Recht vorgesehenen finanziellen Sanktionen wirksam, verhältnismäßig und abschreckend sind. Die Mitgliedstaaten sollten der Kommission diese Vorschriften und Maßnahmen unverzüglich mitteilen und ihr unverzüglich alle diesbezüglichen Änderungen melden.

(70) Wenn im Einzelfall die angemessenen finanziellen Sanktionen bewertet 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. Unter außergewöhnlichen Umständen könnte diese Bewertung die Vollstreckungsbehörde zu dem Beschluss veranlassen, von der Verhängung finanzieller Sanktionen abzusehen. Ein besonderes Augenmerk ist in dieser Hinsicht auf Kleinstunternehmen zu richten, die einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung in einem Notfall aufgrund der Nichtverfügbarkeit von Personal außerhalb der üblichen Geschäftszeiten nicht Folge leisten, sofern die Daten unverzüglich übermittelt werden.

(71) Unbeschadet ihrer Datenschutzpflichten sollten die Diensteanbieter in den Mitgliedstaaten nicht für Schäden haftbar gemacht werden, die ihren Nutzern oder Dritten ausschließlich aufgrund der gutgläubigen Befolgung eines EPOC oder eines EPOC-PR entstehen. Die Verantwortung für die Gewährleistung der Rechtmäßigkeit der betreffenden Anordnung, insbesondere für ihre Notwendigkeit und Verhältnismäßigkeit, sollte bei der Anordnungsbehörde liegen.

(72) Leistet der Adressat ohne Angabe von Gründen, die von der Anordnungsbehörde akzeptiert werden, einem EPOC nicht fristgerecht oder einem EPOC-PR nicht Folge und hat die Vollstreckungsbehörde, sofern anwendbar, keinen der Ablehnungsgründe gemäß der vorliegenden Verordnung geltend gemacht, so sollte die Anordnungsbehörde die Möglichkeit haben, die Vollstreckungsbehörde darum zu ersuchen, die Europäische Herausgabeanordnung oder die Europäische Sicherungsanordnung zu vollstrecken. Zu diesem Zweck sollte die Anordnungsbehörde der Vollstreckungsbehörde die betreffende Anordnung, das in der vorliegenden Verordnung vorgesehene, vom Adressaten ausgefüllte entsprechende Formular sowie alle einschlägigen Unterlagen übermitteln. Die Anordnungsbehörde sollte die betreffende Anordnung und alle zu übermittelnden Unterlagen in eine der von dem Vollstreckungsstaat akzeptierten Sprachen übersetzen und den Adressaten von der Übermittlung in Kenntnis setzen. Dieser Staat sollte die betreffende Anordnung gemäß seinen nationalen Rechtsvorschriften vollstrecken.

(73) Das Vollstreckungsverfahren sollte es dem Adressaten ermöglichen, Gründe gegen die Vollstreckung auf der Grundlage einer Liste bestimmter in der vorliegenden Verordnung vorgesehener Gründe geltend zu machen, zu denen auch gehören sollte, dass die betreffende Anordnung nicht von einer zuständigen Behörde gemäß der vorliegenden Verordnung erlassen oder validiert wurde, oder wenn die Anordnung keine Daten betrifft, die zum Zeitpunkt des Eingangs der betreffenden Bescheinigung vom Diensteanbieter oder für ihn gespeichert waren. Die Vollstreckungsbehörde sollte die Anerkennung und Vollstreckung einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung aus denselben Gründen sowie in Ausnahmefällen auch aufgrund einer offensichtlichen Verletzung eines einschlägigen Grundrechts gemäß Artikel 6 EUV und der Charta ablehnen können. Bevor die Vollstreckungsbehörde die Ablehnung der Anerkennung oder Vollstreckung der Anordnung aus diesen Gründen beschließt, sollte sie die Anordnungsbehörde konsultieren. Kommt der Adressat seinen Verpflichtungen aus einer anerkannten Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung, deren Vollstreckbarkeit von der Vollstreckungsbehörde bestätigt wurde, nicht nach, so sollte diese Behörde eine finanzielle Sanktion verhängen. Diese Sanktion sollte insbesondere angesichts bestimmter Umstände wie einer wiederholten oder systematischen Nichtbefolgung verhältnismäßig sein.

(74) Die Befolgung einer Europäischen Herausgabeanordnung könnte im Widerspruch zu einer Verpflichtung nach den geltenden Rechtsvorschriften eines Drittlands stehen. 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 einen Diensteanbieter daran hindern würde, rechtlichen Verpflichtungen aus dem Recht eines Drittlands nachzukommen.

(75) Wenn der Adressat der Auffassung ist, dass eine Europäische Herausgabeanordnung in einem konkreten Fall eine Verletzung einer aus dem Recht eines Drittlands abgeleiteten rechtlichen Verpflichtung zur Folge hätte, sollte er die Anordnungsbehörde und die Vollstreckungsbehörde durch einen unter Verwendung des in der vorliegenden Verordnung vorgesehenen Formulars erstellten begründeten Einwand über die Gründe für die Nichtausführung der Anordnung in Kenntnis setzen. Die Anordnungsbehörde sollte die Europäische Herausgabeanordnung auf der Grundlage des begründeten Einwands und etwaiger Beiträge des Vollstreckungsstaats überprüfen und hierbei dieselben Kriterien berücksichtigen, die das zuständige Gericht des Anordnungsstaats zugrunde legen müsste. Beabsichtigt die Anordnungsbehörde, die Anordnung aufrechtzuerhalten, so sollte sie eine Überprüfung durch das vom betreffenden Mitgliedstaat benannte zuständige Gericht des Anordnungsstaats beantragen, das die Anordnung überprüfen sollte.

(76) Bei der Prüfung, ob in dem betreffenden Fall ein Widerspruch zwischen verschiedenen Verpflichtungen besteht, könnte sich das zuständige Gericht gegebenenfalls auf angemessenes externes Fachwissen stützen, beispielsweise zur Auslegung des Rechts des betreffenden Drittlands. Zu diesem Zweck könnte das zuständige Gericht unter Berücksichtigung der Richtlinie (EU) 2016/680 beispielsweise die zentrale Behörde des Drittlands konsultieren. Der Anordnungsstaat sollte insbesondere die zuständige Behörde des Drittlands um Informationen ersuchen, wenn der Widerspruch Grundrechte oder andere grundlegende Interessen des Drittlands im Zusammenhang mit der nationalen Sicherheit und Verteidigung betrifft.

(77) Das Fachwissen über die Auslegung könnte gegebenenfalls auch durch Sachverständigengutachten eingeholt werden. Informationen und die Rechtsprechung zur Auslegung des Rechts eines Drittlands und zu Verfahren des Kollisionsrechts in den Mitgliedstaaten sollten auf einer zentralen Plattform wie dem Projekt SIRIUS oder dem Europäischen Justiziellen Netz zur Verfügung gestellt werden, um von den Erfahrungen und dem Fachwissen zu denselben oder ähnlichen Fragen profitieren zu können. Ungeachtet der Verfügbarkeit dieser Informationen auf einer zentralen Plattform sollte eine erneute Konsultation des Drittlands gegebenenfalls aber dennoch möglich sein.

(78) Bei der Bewertung der Frage, ob einander widersprechende Verpflichtungen bestehen, sollte das zuständige Gericht prüfen, ob das Recht des Drittlands anwendbar ist und, wenn ja, ob das Recht des Drittlands die Offenlegung der betreffenden Daten verbietet. Stellt das zuständige Gericht fest, dass das Recht des Drittlands die Offenlegung der betreffenden Daten verbietet, sollte dieses Gericht prüfen, ob die Europäische Herausgabeanordnung aufrechterhalten oder aufgehoben werden soll, 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 Adressaten oder für den Diensteanbieter, wenn er der Anordnung Folge leistet, festzustellen sind. Bei der Bewertung sollte dem Schutz der Grundrechte im Rahmen der einschlägigen Rechtsvorschriften des Drittlands und anderen grundlegenden Interessen beispielsweise im Zusammenhang mit der nationalen Sicherheit des Drittlands sowie dem Grad der Verbindung der Strafsache zu einem der beiden Rechtssysteme besondere Bedeutung und besonderes Gewicht beigemessen werden. Beschließt das 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 sollte es dies der Anordnungsbehörde und dem Adressaten mitteilen, der sodann die Anordnung ausführen sollte. Die Anordnungsbehörde sollte die Vollstreckungsbehörde über das Ergebnis des Überprüfungsverfahrens informieren.

(79) Die in der vorliegenden Verordnung genannten Voraussetzungen für die Vollstreckung eines EPOC sollten auch dann gelten, wenn sich aufgrund des Rechts eines Drittlands kollidierende Verpflichtungen ergeben. Daher sollten im Rahmen der gerichtlichen Überprüfung, wenn die Einhaltung einer Europäischen Herausgabeanordnung Diensteanbieter daran hindern würde, einer rechtlichen Verpflichtung nachzukommen, die sich aus dem Recht eines Drittlands ergibt, die mit dieser Anordnung angeforderten Daten gesichert werden. Beschließt das zuständige Gericht im Anschluss an die gerichtliche Überprüfung, eine Europäische Herausgabeanordnung aufzuheben, sollte es möglich sein, eine Europäische Sicherungsanordnung zu erlassen, damit die Anordnungsbehörde die Herausgabe der Daten über andere Kanäle, beispielsweise im Wege der Rechtshilfe, erwirken kann.

(80) 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 einen wirksamen Rechtsbehelf einlegen können. Gemäß dieser Anforderung und unbeschadet weiterer Rechtsbehelfe, die nach dem nationalen Recht zur Verfügung stehen, sollten Personen, deren Daten im Wege einer Europäischen Herausgabeanordnung angefordert wurden, das Recht haben, wirksame Rechtsbehelfe gegen diese Anordnung einzulegen. Handelt es sich bei der Person um einen Verdächtigen oder einen Beschuldigten, so sollte die betreffende Person das Recht haben, während des Strafverfahrens, in dem die Daten als Beweismittel verwendet werden, wirksame Rechtsbehelfe einzulegen. Das Recht auf Einlegung wirksamer Rechtsbehelfe sollte vor einem Gericht des Anordnungsstaats nach dessen nationalem Recht ausgeübt werden und die Möglichkeit umfassen, die Rechtmäßigkeit der Maßnahme, einschließlich ihrer Notwendigkeit und Verhältnismäßigkeit, anzufechten, unbeschadet der Grundrechtsgarantien im Vollstreckungsstaat oder anderer zusätzlicher Rechtsbehelfe nach nationalem Recht. Die vorliegende Verordnung sollte die möglichen Gründe für die Anfechtung der Rechtmäßigkeit einer Anordnung nicht beschränken. Das in der vorliegenden Verordnung vorgesehene Recht auf wirksame Rechtsbehelfe sollte das Recht auf Einlegung von Rechtsbehelfen gemäß der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 unberührt lassen. Es sollten rechtzeitig Informationen darüber bereitgestellt werden, welche Möglichkeiten nach nationalem Recht bestehen, Rechtsmittel einzulegen, und es sollte sichergestellt werden, dass diese wirksam ausgeübt werden können.

(81) Es sollten geeignete Kanäle entwickelt werden, um sicherzustellen, dass alle Parteien mit digitalen Mitteln effizient zusammenarbeiten können, und zwar über ein dezentrales Informationstechnologie-System (IT-System), das einen raschen, direkten, interoperablen, nachhaltigen, zuverlässigen und sicheren grenzüberschreitenden elektronischen Austausch von fallbezogenen Formularen, Daten und Informationen ermöglicht.

(82) Um eine effiziente und sichere schriftliche Kommunikation zwischen den zuständigen Behörden und den benannten Niederlassungen oder den Vertretern von Diensteanbietern gemäß dieser Verordnung zu ermöglichen, sollte diesen benannten Niederlassungen oder Vertretern ein elektronischer Zugang zu den nationalen IT-Systemen gewährt werden, die Teil des dezentralen IT-Systems sind, das von den Mitgliedstaaten betrieben wird.

(83) Das dezentrale IT-System sollte sich aus den IT-Systemen der Mitgliedstaaten und der Einrichtungen und sonstigen Stellen der Union sowie aus interoperablen Zugangspunkten zusammensetzen, über die diese IT-Systeme miteinander vernetzt sind. Die Zugangspunkte des dezentralen IT-Systems sollten auf dem mit der Verordnung (EU) 2022/850 des Europäischen Parlaments und des Rates ([24]) eingerichteten e-CODEX-System beruhen.

(84) Diensteanbietern, die maßgeschneiderte IT-Lösungen für den Austausch von Informationen und Daten im Zusammenhang mit Ersuchen um elektronische Beweismittel nutzen, sollten mittels eines gemeinsamen Datenaustauschstandards automatisierte Mittel für den Zugang zu den dezentralen IT-Systemen bereitgestellt werden.

(85) In der Regel sollte jede schriftliche Kommunikation zwischen den zuständigen Behörden oder zwischen den zuständigen Behörden und benannten Niederlassungen oder Vertretern über das dezentrale IT-System erfolgen. Alternative Mittel sollten nur dann verwendet werden können, wenn die Nutzung des dezentralen IT-Systems nicht möglich ist, z. B. wegen besonderer forensischer Erfordernisse, weil das Volumen der zu übermittelnden Daten durch technische Kapazitätsengpässe behindert wird oder, weil man sich in einem Notfall an eine andere Niederlassung, die nicht mit dem dezentralen IT-System verbunden ist, wenden muss. In solchen Fällen sollte die Übermittlung mit den am besten geeigneten alternativen Mitteln erfolgen, wobei der Notwendigkeit Rechnung zu tragen ist, einen raschen, sicheren und zuverlässigen Informationsaustausch zu gewährleisten.

(86) Um sicherzustellen, dass das dezentrale IT-System eine vollständige Aufzeichnung des schriftlichen Austauschs gemäß der vorliegenden Verordnung enthält, sollte jede auf andere Weise erfolgte Übermittlung unverzüglich im dezentralen IT-System erfasst werden.

(87) Der Einsatz von Mechanismen zur Sicherstellung der Echtheit, wie sie in der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([25]) vorgesehen sind, sollte in Betracht gezogen werden.

(88) Dienstleistern, insbesondere kleinen und mittleren Unternehmen, sollten keine unverhältnismäßig hohen Kosten im Zusammenhang mit der Einrichtung und dem Betrieb des dezentralen IT-Systems entstehen. Im Rahmen der Schaffung, Wartung und Weiterentwicklung der Referenzimplementierung sollte die Kommission daher auch eine webbasierte Schnittstelle bereitstellen, die es den Diensteanbietern ermöglicht, sicher mit den Behörden zu kommunizieren, ohne eine eigene Infrastruktur einrichten zu müssen, um Zugang zum dezentralen IT-System zu erhalten.

(89) Die Mitgliedstaaten sollten von der Kommission entwickelte Software, d. h. die Referenzimplementierungssoftware, anstelle eines nationalen IT-Systems verwenden können. Diese Referenzimplementierungssoftware sollte modular aufgebaut sein, d. h. die Software sollte getrennt von den e-CODEX-Komponenten, die für den Anschluss an das dezentrale IT-System erforderlich sind, geliefert werden und in separaten Paketen enthalten sein. Mit dieser Struktur sollten die Mitgliedstaaten ihre jeweilige bestehende nationale Infrastruktur für die Kommunikation im Justizbereich für die grenzüberschreitende Kommunikation weiter nutzen oder dafür ausbauen können.

(90) Die Kommission sollte für die Schaffung, Wartung und Weiterentwicklung der Referenzimplementierungssoftware zuständig sein. Die Kommission sollte die Referenzimplementierungssoftware gemäß den Datenschutzanforderungen und -grundsätzen der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([26]), der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 – insbesondere den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen und unter Berücksichtigung eines hohen Cybersicherheitsniveaus – konzipieren, entwickeln und warten. Es ist wichtig, dass die Referenzimplementierungssoftware auch geeignete technische Maßnahmen umfasst und es ermöglicht, die organisatorischen Maßnahmen zu ergreifen, die erforderlich sind, um ein angemessenes Maß an Sicherheit und Interoperabilität zu gewährleisten.

([24]) Verordnung (EU) 2022/850 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über ein EDV-System für den grenzüberschreitenden elektronischen Datenaustausch im Bereich der justiziellen Zusammenarbeit in Zivil- und Strafsachen (e-CODEX-System) und zur Änderung der Verordnung (EU) 2018/1726 (ABl. L 150 vom 1.6.2022, S. 1).

([25]) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

([26]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

(91) Zur Gewährleistung einheitlicher Voraussetzungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([27]) ausgeübt werden.

(92) Für den Datenaustausch, der über das dezentrale IT-System erfolgt oder im dezentralen IT-System erfasst wird, sollten die Mitgliedstaaten Statistiken erheben können, um ihren Überwachungs- und Berichterstattungspflichten gemäß dieser Verordnung über ihre nationalen Portale nachzukommen.

(93) Für das Monitoring der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung sollte die Kommission auf der Grundlage der von den Mitgliedstaaten eingegangenen Daten einen Jahresbericht über das vorangegangene Kalenderjahr veröffentlichen. Zu diesem Zweck sollten die Mitgliedstaaten umfassende Statistiken über die verschiedenen Aspekte dieser Verordnung erheben und der Kommission übermitteln, aufgeschlüsselt nach Art der angeforderten Daten, Adressaten und der Frage, ob es sich um einen Notfall handelte oder nicht.

(94) Die Verwendung vorübersetzter und standardisierter Formulare würde die Zusammenarbeit und den Informationsaustausch gemäß der vorliegenden Verordnung erleichtern, sodass die Kommunikation schneller und wirksamer und gleichzeitig in benutzerfreundlicher Weise erfolgen kann. Solche Formulare würden die Übersetzungskosten senken und zu einem hohen Qualitätsstandard der Kommunikation beitragen. Antwortformulare würden einen standardisierten Informationsaustausch ermöglichen, insbesondere wenn Diensteanbieter die Anordnung nicht befolgen können, weil das Nutzerkonto nicht existiert oder weil keine Daten verfügbar sind. Zudem würden die gemäß der vorliegenden Verordnung bereitgestellten Formulare auch die Erhebung von Statistiken erleichtern.

(95) Damit 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 Vollstreckung eines EPOC oder eines EPOC-PR, zur Bestätigung, dass ein Ersuchen um Herausgabe infolge einer Europäischen Sicherungsanordnung gestellt wurde, und zur Verlängerung der Sicherung elektronischer Beweismittel wirksam entsprochen werden kann, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) Rechtsakte im Hinblick auf die Änderung der gemäß dieser Verordnung bereitgestellten Formulare zu erlassen. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung niedergelegt wurden ([28]). 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.

(96) Die vorliegende Verordnung sollte Unions- und sonstige internationale Instrumente, Abkommen und Vereinbarungen über die in den Anwendungsbereich der vorliegenden Verordnung fallende Erhebung von Beweismitteln unberührt lassen. Die Behörden der Mitgliedstaaten sollten das für den vorliegenden Fall am besten geeignete Instrument auswählen. In einigen Fällen könnten sie Unions- und andere internationale Instrumente, Abkommen und Vereinbarungen vorziehen, wenn sie um eine Reihe verschiedener Arten von Ermittlungsmaßnahmen ersuchen, die nicht auf die Herausgabe elektronischer Beweismittel aus einem anderen Mitgliedstaat beschränkt sind. Die Mitgliedstaaten sollten die Kommission spätestens drei Jahre nach Inkrafttreten der vorliegenden Verordnung über die in der vorliegenden Verordnung genannten bestehenden Instrumente, Abkommen und Vereinbarungen unterrichten, die sie weiterhin anwenden werden. Die Mitgliedstaaten sollten die Kommission ferner binnen drei Monaten nach der Unterzeichnung über alle neuen Abkommen oder Vereinbarungen im Sinne der vorliegenden Verordnung unterrichten.

(97) Angesichts 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 Bewertung ihrer Anwendung vorzusehen.

(98) Die Kommission sollte eine Bewertung dieser Verordnung vornehmen, die sich auf die fünf Kriterien Effizienz, Wirksamkeit, Relevanz, Kohärenz und EU-Mehrwert stützen sollte, und diese Bewertung sollte die Grundlage für Folgenabschätzungen für mögliche weitere Maßnahmen bilden. Der Bewertungsbericht sollte eine Bewertung der Anwendung der vorliegenden Verordnung und der im Hinblick auf ihre Ziele erreichten Ergebnisse sowie eine Bewertung der Auswirkungen der vorliegenden Verordnung auf die Grundrechte enthalten. Die Kommission sollte regelmäßig Informationen einholen, die in die Bewertung dieser Verordnung einfließen.

([27]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

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

(99) 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 EUV verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Erreichung dieses Ziels erforderliche Maß hinaus.

(100) Gemäß Artikel 3 des dem EUV und dem AEUV beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts hat Irland mitgeteilt, dass es sich an der Annahme und der Anwendung dieser Verordnung beteiligen möchte.

(101) Nach den Artikeln 1 und 2 des dem EUV und dem AEUV beigefügten Protokolls Nr. 22 über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Verordnung, und ist weder durch diese Verordnung gebunden noch zu ihrer Anwendung verpflichtet.

(102) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 angehört und hat am 6. November 2019 eine Stellungnahme ([29]) abgegeben.

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

GEGENSTAND, ANWENDUNGSBEREICH UND BEGRIFFSBESTIMMUNGEN

Artikel 1

Gegenstand

(1) Mit dieser Verordnung werden die Regeln festgelegt, nach denen eine Behörde eines Mitgliedstaats im Rahmen eines Strafverfahrens eine Europäische Herausgabeanordnung oder eine Europäische Sicherungsanordnung erlassen und damit von einem Diensteanbieter, der in der Union Dienste anbietet und in einem anderen Mitgliedstaat niedergelassen ist oder – falls er dort nicht niedergelassen ist – durch einen Vertreter in einem anderen Mitgliedstaat vertreten ist, verlangen kann, elektronische Beweismittel herauszugeben oder zu sichern, unabhängig davon, wo sich die Daten befinden.

Diese Verordnung lässt die Befugnisse der nationalen Behörden unberührt, sich an in dem in ihrem Hoheitsgebiet niedergelassene oder vertretene Diensteanbieter zu wenden um dafür zu sorgen, dass diese Diensteanbieter nationale Maßnahmen einhalten, die mit den in Unterabsatz 1 genannten vergleichbar sind.

(2) Der Erlass einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung kann auch von einem Verdächtigen oder einem Beschuldigten oder in deren Namen von einem Rechtsanwalt im Rahmen der geltenden Verteidigungsrechte im Einklang mit dem nationalen Strafverfahrensrecht beantragt werden.

(3) Diese Verordnung lässt die Verpflichtung zur Achtung der Grundrechte und der Rechtsgrundsätze, die in der Charta und in Artikel 6 EUV verankert sind, und die diesbezüglichen Verpflichtungen der Strafverfolgungs- oder Justizbehörden unberührt. Diese Verordnung gilt unbeschadet grundlegender Prinzipien, insbesondere der Freiheit der Meinungsäußerung und Informationsfreiheit einschließlich der Achtung der Freiheit der Medien und ihrer Pluralität, der Achtung des Privat- und Familienlebens, des Schutzes personenbezogener Daten und des Rechts auf einen wirksamen Rechtsschutz.

Artikel 2

Anwendungsbereich

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

(2) Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen dürfen im Rahmen von und für Strafverfahren und zur Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung mit einer Mindestdauer von vier Monaten, deren Anordnung aufgrund eines Strafverfahrens durch ein Urteil erfolgte, sofern sie in dem Fall, dass sich der Verurteilte der Justiz entzogen hat, nicht in Abwesenheit ergangen ist, erlassen werden. Diese Anordnungen können auch in Verfahren wegen einer Straftat erlassen werden, für die eine juristische Person im Anordnungsstaat zur Verantwortung gezogen oder bestraft werden könnte.

(3) Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen dürfen nur für Daten erlassen werden, die Dienste im Sinne des Artikels 3 Nummer 3 betreffen, die in der Union angeboten werden.

(4) Diese Verordnung gilt nicht für Verfahren, die eingeleitet wurden, um einem anderen Mitgliedstaat oder einem Drittland Rechtshilfe zu leisten.

([29]) ABl. C 32 vom 31.1.2020, S. 11.

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Europäische Herausgabeanordnung“ eine Entscheidung, mit der die Herausgabe elektronischer Beweismittel angeordnet wird, die von einer Justizbehörde eines Mitgliedstaats im Einklang mit Artikel 4 Absätze 1, 2, 4 und 5 erlassen oder validiert wird und die an eine benannte Niederlassung oder einen Vertreter eines Diensteanbieters, der in der Union Dienste anbietet, gerichtet ist, sofern sich die benannte Niederlassung oder der Vertreter in einem durch diese Verordnung gebundenen anderen Mitgliedstaat befindet;

2. „Europäische Sicherungsanordnung“ eine Entscheidung, mit der die Sicherung elektronischer Beweismittel zum Zweck eines späteren Ersuchens um Herausgabe angeordnet wird, die von einer Justizbehörde eines Mitgliedstaats im Einklang mit Artikel 4 Absätze 3, 4 und 5 erlassen oder validiert wird und die an eine benannte Niederlassung oder einen Vertreter eines Diensteanbieters, der in der Union Dienste anbietet, gerichtet ist, sofern sich die benannte Niederlassung oder der Vertreter in einem durch diese Verordnung gebundenen anderen Mitgliedstaat befindet;

3. „Diensteanbieter“ jede natürliche oder juristische Person, die eine oder mehrere der folgenden Dienstleistungskategorien anbietet, ausgenommen Finanzdienstleistungen im Sinne des Artikels 2 Absatz 2 Buchstabe b der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates ([30]):

   a) elektronische Kommunikationsdienste im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972;

   b) Internetdomänennamen- und IP-Nummerierungsdienste wie Dienste der IP-Adressenzuweisung und der Domänennamen-Registrierung, Domänennamen-Registrierungsstellendienste und mit Domänennamen verbundene Datenschutz- und Proxy-Dienste;

   c) andere Dienste der Informationsgesellschaft im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535,

      i) die es ihren Nutzern ermöglichen, miteinander zu kommunizieren, oder

      ii) die es ermöglichen, für Nutzer, für welche die Dienstleistung erbracht wird, Daten zu speichern oder auf sonstige Weise zu verarbeiten, sofern die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung ist;

4. „Anbieten von Diensten in der Union“

   a) die Schaffung einer Möglichkeit für natürliche oder juristische Personen in einem Mitgliedstaat, die in Nummer 3 genannten Dienste in Anspruch zu nehmen, und

   b) eine aufgrund konkreter faktischer Kriterien gegebene wesentliche Verbindung zu dem unter Buchstabe a genannten Mitgliedstaat; dabei gilt eine solche wesentliche Verbindung dann als unterhalten, wenn der Diensteanbieter eine Niederlassung in einem Mitgliedstaat hat oder wenn es – in Ermangelung einer solchen – in einem oder mehreren Mitgliedstaaten eine erhebliche Zahl von Nutzern gibt oder wenn die Tätigkeiten auf einen oder mehrere Mitgliedstaaten ausgerichtet sind;

5. „Niederlassung“ einen Rechtsträger, der tatsächlich eine wirtschaftliche Tätigkeit auf unbestimmte Zeit durch eine stabile Infrastruktur ausübt, von der aus die Geschäftstätigkeit der Dienstleistungserbringung ausgeübt oder die Geschäftstätigkeit verwaltet wird;

6. „benannte Niederlassung“ eine Niederlassung mit Rechtspersönlichkeit, die ein Dienstleister, der in einem Mitgliedstaat niedergelassenen ist, der sich an einem in Artikel 1 Absatz 2 der Richtlinie (EU) 2023/1544 genannten Rechtsinstrument beteiligt, für die in Artikel 1 Absatz 1 und Artikel 3 Absatz 1 der genannten Richtlinie genannten Zwecke schriftlich benannt hat;

7. „Vertreter“ eine natürliche oder juristische Person, die ein Dienstleister, der nicht in einem Mitgliedstaat niedergelassen ist, der sich an einem in Artikel 1 Absatz 2 der Richtlinie (EU) 2023/1544 genannten Rechtsinstrument beteiligt, für die in Artikel 1 Absatz 1 und Artikel 3 Absatz 1 der genannten Richtlinie genannten Zwecke schriftlich bestellt hat;

8. „elektronische Beweismittel“ Teilnehmerdaten, Verkehrsdaten oder Inhaltsdaten, die zum Zeitpunkt des Erhalts einer Bescheinigung über eine Europäische Herausgabeanordnung (EPOC) oder einer Bescheinigung über eine Europäische Sicherungsanordnung (EPOC-PR) in elektronischer Form von einem Diensteanbieter oder in seinem Auftrag gespeichert werden;

([30]) Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (ABl. L 376 vom 27.12.2006, S. 36).

9. „Teilnehmerdaten“ alle Daten, die bei einem Diensteanbieter über die Teilnahme an seinen Diensten vorliegen und 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 verbundene technische Maßnahmen oder Schnittstellen identifiziert werden, die von einem Teilnehmer oder Kunden zum Zeitpunkt der erstmaligen Registrierung/Anmeldung oder Aktivierung 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;

10. „ausschließlich zum Zweck der Identifizierung des Nutzers angeforderte Daten“ die IP-Adressen und, falls notwendig, die relevanten Quellports und Zeitstempel, nämlich Datum und Uhrzeit, oder die technischen Äquivalente dieser Kennungen und die damit zusammenhängenden Informationen, sofern sie von Strafverfolgungs- oder Justizbehörden ausschließlich zum Zweck der Identifizierung des Nutzers in einer bestimmten strafrechtlichen Ermittlung angefordert werden;

11. „Verkehrsdaten“ Daten, die sich auf die Erbringung einer von einem Diensteanbieter angebotenen Dienstleistung beziehen, dazu dienen, Kontext- oder Zusatzinformationen über eine solche Dienstleistung zu liefern und von einem Informationssystem des Diensteanbieters generiert oder verarbeitet werden, beispielsweise Ursprung und Ziel 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, sowie andere Metadaten der elektronischen Kommunikation und Daten, die keine Teilnehmerdaten sind, über den Beginn und die Beendigung der Nutzersitzung für einen Dienst, etwa das Datum und die Uhrzeit der Nutzung, die Anmeldung bei und die Abmeldung von dem Dienst;

12. „Inhaltsdaten“ alle Daten in einem digitalen Format wie Text, Sprache, Videos, Bilder und Tonaufzeichnungen, die nicht Teilnehmer- oder Verkehrsdaten sind;

13. „Informationssystem“ ein Informationssystem im Sinne des Artikels 2 Buchstabe a der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates ([31]);

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

15. „Anordnungsbehörde“ die zuständige Behörde im Anordnungsstaat, die im Einklang mit Artikel 4 eine Europäische Herausgabeanordnung oder eine Europäische Sicherungsanordnung erlassen kann;

16. „Vollstreckungsstaat“ den Mitgliedstaat, in dem die benannte Niederlassung niedergelassen oder der Vertreter ansässig ist und an den eine Europäische Herausgabeanordnung und ein EPOC oder eine Europäische Sicherungsanordnung und ein EPOC-PR von der Anordnungsbehörde zur Mitteilung oder zur Vollstreckung im Einklang mit dieser Verordnung übermittelt werden;

17. „Vollstreckungsbehörde“ die Behörde im Vollstreckungsstaat, die im Einklang mit dem nationalen Recht dieses Staates für die Entgegennahme einer Europäischen Herausgabeanordnung und eines EPOC oder einer Europäischen Sicherungsanordnung und eines EPOC-PR zuständig ist, die von der Anordnungsbehörde zur Mitteilung oder zur Vollstreckung im Einklang mit dieser Verordnung übermittelt werden;

18. „Notfall“ eine Situation, in der eine unmittelbare Gefahr für das Leben, die körperliche Unversehrtheit oder die Sicherheit einer Person oder für eine kritische Infrastruktur im Sinne des Artikels 2 Buchstabe a der Richtlinie 2008/114/EG besteht, wenn die Störung oder Zerstörung einer kritischen Infrastruktur zu einer unmittelbaren Gefahr für das Leben, die körperliche Unversehrtheit oder die Sicherheit einer Person führen würde, auch durch die schwere Beeinträchtigung der Bereitstellung der Grundversorgung für die Bevölkerung oder der Wahrnehmung der Kernfunktionen des Staates;

19. „Verantwortlicher“ den Verantwortlichen im Sinne des Artikels 4 Nummer 7 der Verordnung (EU) 2016/679;

20. „Auftragsverarbeiter“ den Auftragsverarbeiter im Sinne des Artikels 4 Nummer 8 der Verordnung (EU) 2016/679;

([31]) 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).

21. „dezentrales IT-System“ ein Netzwerk von IT-Systemen und interoperablen Zugangspunkten, die unter der jeweiligen Verantwortung und Verwaltung jedes Mitgliedstaats oder jeder Einrichtung oder jeder sonstigen Stelle der Union betrieben werden, wodurch der sichere und zuverlässige grenzübergreifende Informationsaustausch ermöglicht wird.

KAPITEL II

EUROPÄISCHE HERAUSGABEANORDNUNG, EUROPÄISCHE SICHERUNGSANORDNUNG UND BESCHEINIGUNGEN

Artikel 4

Anordnungsbehörde

(1) Eine Europäische Herausgabeanordnung zur Erlangung von Teilnehmerdaten oder zur Erlangung von ausschließlich zum Zweck der Identifizierung des Nutzers angeforderten Daten im Sinne des Artikels 3 Nummer 10 kann nur 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; in solch einem Fall wird die Europäische Herausgabeanordnung von einem Richter, einem Gericht, einem Ermittlungsrichter oder einem Staatsanwalt im Anordnungsstaat validiert, nachdem er bzw. es überprüft hat, ob die Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung nach dieser Verordnung eingehalten sind.

(2) Eine Europäische Herausgabeanordnung zur Erlangung von Verkehrsdaten mit Ausnahme von ausschließlich zum Zweck der Identifizierung des Nutzers angeforderten Daten im Sinne des Artikels 3 Nummer 10 oder zur Erlangung von Inhaltsdaten kann nur 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; in solch einem Fall wird die Europäische Herausgabeanordnung von einem Richter, einem Gericht oder einem Ermittlungsrichter im Anordnungsstaat validiert, nachdem er bzw. es überprüft hat, ob die Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung nach dieser Verordnung eingehalten sind.

(3) Eine Europäische Sicherungsanordnung zur Erlangung sämtlicher Datenkategorien kann nur 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; in solch einem Fall wird die Europäische Sicherungsanordnung von einem Richter, einem Gericht, einem Ermittlungsrichter oder einem Staatsanwalt im Anordnungsstaat validiert, nachdem er bzw. es überprüft hat, ob die Voraussetzungen für den Erlass einer Europäischen Sicherungsanordnung nach dieser Verordnung eingehalten sind.

(4) Wenn eine Europäische Herausgabeanordnung oder eine Europäische Sicherungsanordnung 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 EPOC und des EPOC-PR angesehen werden.

(5) In einem begründeten Notfall im Sinne des Artikels 3 Nummer 18 können die in Absatz 1 Buchstabe b und in Absatz 3 Buchstabe b des vorliegenden Artikels genannten zuständigen Behörden ausnahmsweise eine Europäische Herausgabeanordnung für Teilnehmerdaten oder für ausschließlich zum Zweck der Identifizierung des Nutzers angeforderte Daten im Sinne des Artikels 3 Nummer 10 oder eine Europäische Sicherungsanordnung ohne vorherige Validierung der betreffenden Anordnung erlassen, wenn die Validierung nicht rechtzeitig eingeholt werden kann und wenn diese Behörden in einem vergleichbaren nationalen Fall eine Anordnung ohne vorherige Validierung erlassen könnten. Die Anordnungsbehörde fordert unverzüglich, spätestens innerhalb von 48 Stunden, eine Ex-post-Validierung der betreffenden Anordnung an. Wird eine solche Ex-post-Validierung der betreffenden Anordnung nicht gewährt, so zieht die Anordnungsbehörde die Anordnung sofort zurück und löscht die erlangten Daten oder beschränkt deren Verwendung anderweitig.

(6) Jeder Mitgliedstaat kann für die administrative Übermittlung von EPOC und EPOC-PR, von Europäischen Herausgabeanordnungen und Europäischen Sicherungsanordnungen und von Unterrichtungen sowie für den Empfang von Daten und Unterrichtungen und für die Übermittlung anderer offizieller Korrespondenz in Bezug auf diese Bescheinigungen oder Anordnungen eine oder mehrere zentrale Behörden benennen.

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) Eine Europäische Herausgabeanordnung muss für die Zwecke eines in Artikel 2 Absatz 3 genannten Verfahrens notwendig und verhältnismäßig sein, wobei den Rechten des Verdächtigen oder des Beschuldigten Rechnung zu tragen ist, und darf nur erlassen werden, wenn in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen eine ähnliche Anordnung hätte erlassen werden können.

(3) Eine Europäische Herausgabeanordnung zur Erlangung von Teilnehmerdaten oder zur Erlangung von ausschließlich zum Zweck der Identifizierung des Nutzers angeforderten Daten im Sinne des Artikels 3 Nummer 10 kann für alle Straftaten und zur Vollstreckung von in Strafverfahren ergangenen, mindestens viermonatigen Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung erlassen werden, sofern diese in dem Fall, dass sich der Verurteilte der Justiz entzogen hat, nicht in Abwesenheit ergangen sind.

(4) Eine Europäische Herausgabeanordnung zur Erlangung von Verkehrsdaten mit Ausnahme von ausschließlich zum Zweck der Identifizierung des Nutzers angeforderten Daten im Sinne des Artikels 3 Nummer 10 der vorliegenden Verordnung oder zur Erlangung von Inhaltsdaten darf nur erlassen werden

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

b) bei den folgenden Straftaten, wenn sie ganz oder teilweise mittels eines Informationssystems begangen werden:

   i) Straftaten im Sinne der Artikel 3 bis 8 der Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates ([32]);

   ii) Straftaten im Sinne der Artikel 3 bis 7 der Richtlinie 2011/93/EU;

   iii) Straftaten im Sinne der Artikel 3 bis 8 der Richtlinie 2013/40/EU;

c) bei Straftaten im Sinne der Artikel 3 bis 12 und 14 der Richtlinie (EU) 2017/541;

d) bei unter den Buchstaben a, b und c genannten Straftaten zur Vollstreckung von in Strafverfahren ergangenen, mindestens viermonatigen Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung, sofern sie in dem Fall, dass sich der Verurteilte der Justiz entzogen hat, nicht in Abwesenheit ergangen sind.

(5) Eine Europäische Herausgabeanordnung enthält folgende Angaben:

a) die Anordnungsbehörde und die etwaige validierende Behörde;

b) den Adressaten der Europäischen Herausgabeanordnung gemäß Artikel 7;

c) den Nutzer, es sei denn, der einzige Zweck der Anordnung besteht darin, den Nutzer zu identifizieren, oder andere eindeutige Kennungen wie Nutzername, Anmeldekennung oder Kontobezeichnung zur Bestimmung der angeforderten Daten;

d) die Kategorie der angeforderten Daten im Sinne des Artikels 3 Nummern 9 bis 12;

e) erforderlichenfalls die Zeitspanne der Daten, für die deren Herausgabe angefordert wird;

f) die anwendbaren Bestimmungen des Strafrechts des Anordnungsstaats;

g) in Notfällen im Sinne des Artikels 3 Nummer 18 die hinreichend dargelegten Gründe für den Notfall;

h) wenn die Europäische Herausgabeanordnung unmittelbar an den Diensteanbieter, der die Daten im Auftrag des Verantwortlichen speichert oder auf sonstige Weise verarbeitet, gerichtet ist, eine Bestätigung, dass die in Absatz 6 des vorliegenden Artikels enthaltenen Bedingungen erfüllt sind;

i) die Gründe für die Feststellung, dass die Europäische Herausgabeanordnung die Voraussetzungen der Notwendigkeit und Verhältnismäßigkeit gemäß Absatz 2 des vorliegenden Artikels erfüllt;

j) eine zusammenfassende Beschreibung des Falls.

([32]) Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates (ABl. L 123 vom 10.5.2019, S. 18).

(6) Eine Europäische Herausgabeanordnung ist an den Diensteanbieter zu richten, der als Verantwortliche im Sinne der Verordnung (EU) 2016/679 handelt.

Ausnahmsweise kann die Europäische Herausgabeanordnung unmittelbar an den Diensteanbieter gerichtet werden, der die Daten im Auftrag des Verantwortlichen speichert oder auf sonstige Weise verarbeitet, sofern

a) der Verantwortliche trotz angemessener Bemühungen der Anordnungsbehörde nicht ermittelt werden kann oder

b) es die Ermittlungen gefährden könnte, wenn die Anordnung an den Verantwortlichen gerichtet würde.

(7) Im Einklang mit der Verordnung (EU) 2016/679 informiert der Auftragsverarbeiter, der die Daten für den Verantwortlichen speichert oder anderweitig verarbeitet, den Verantwortlichen über die Herausgabe der Daten, es sei denn, die Anordnungsbehörde hat den Diensteanbieter aufgefordert, diese Information so lange wie notwendig und verhältnismäßig nicht vorzunehmen, um das einschlägige Strafverfahren nicht zu behindern. In diesem Fall hat die Anordnungsbehörde in der Verfahrensakte die Gründe für den Aufschub der Information des Verantwortlichen anzugeben. Zudem ist dem EPOC eine kurze Begründung beizufügen.

(8) Wenn die Daten im Rahmen einer Infrastruktur, die ein Diensteanbieter einer Behörde bereitstellt, gespeichert oder anderweitig verarbeitet werden, darf eine Europäische Herausgabeanordnung nur dann erlassen werden, wenn sich die Behörde, für die die Daten gespeichert oder anderweitig verarbeitet werden, im Anordnungsstaat befindet.

(9) In Fällen, in denen gemäß dem Recht des Anordnungsstaats vom Berufsgeheimnis geschützte Daten von einem Diensteanbieter im Rahmen einer Infrastruktur gespeichert oder anderweitig verarbeitet werden, die Geschäftspersonen in ihrer Geschäftstätigkeit bereitgestellt wird, die dem Berufsgeheimnis unterliegen (im Folgenden „Berufsgeheimnisträger"), darf eine Europäische Herausgabeanordnung nur zur Erlangung von Verkehrsdaten, mit Ausnahme von Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne des Artikels 3 Nummer 10 angefordert werden, oder zur Erlangung von Inhaltsdaten erlassen werden,

a) sofern der Berufsgeheimnisträger im Anordnungsstaat wohnhaft ist,

b) sofern es die Ermittlungen gefährden könnte, wenn die Anordnung an den Berufsgeheimnisträger gerichtet wird, oder

c) sofern das Berufsgeheimnis im Einklang mit dem anwendbaren Recht aufgehoben wurde.

(10) Wenn die Anordnungsbehörde Grund zu der Annahme hat, dass die Verkehrsdaten – mit Ausnahme von Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne des Artikels 3 Nummer 10 angefordert werden – oder die Inhaltsdaten, die mit der Europäischen Herausgabeanordnung angefordert werden, durch Immunitäten oder Vorrechte geschützt sind, die nach dem Recht des Vollstreckungsstaats gewährt werden, oder dass diese Daten in diesem Staat Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Freiheit der Presse und das Recht auf freie Meinungsäußerung in anderen Medien unterliegen, kann die Anordnungsbehörde vor dem Erlass der Europäischen Herausgabeanordnung den Sachverhalt klären, unter anderem indem sie die zuständigen Behörden des Vollstreckungsstaats entweder unmittelbar oder über Eurojust oder das Europäische Justizielle Netz konsultiert.

Stellt die Anordnungsbehörde fest, dass die angeforderten Verkehrsdaten – mit Ausnahme von Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers im Sinne des Artikels 3 Nummer 10 angefordert werden – oder die angeforderten Inhaltsdaten durch Immunitäten oder Vorrechte geschützt sind, die nach dem Recht des Vollstreckungsstaats gewährt werden, oder dass diese Daten in diesem Staat Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Freiheit der Presse und das Recht auf freie Meinungsäußerung in anderen Medien unterliegen, so erlässt sie die Europäische Herausgabeanordnung nicht.

Artikel 6

Voraussetzungen für den Erlass einer Europäischen Sicherungsanordnung

(1) Eine Anordnungsbehörde darf nur dann eine Europäische Sicherungsanordnung erlassen, wenn die in diesem Artikel genannten Voraussetzungen erfüllt sind. Artikel 5 Absatz 8 gilt entsprechend.

(2) Eine Europäische Sicherungsanordnung muss für die Zwecke der Verhinderung der 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 notwendig und verhältnismäßig sein, wobei den Rechten des Verdächtigen oder des Beschuldigten Rechnung zu tragen ist.

(3) Eine Europäische Sicherungsanordnung kann für alle Straftaten erlassen werden, wenn sie in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen hätte erlassen werden können, und sie kann zur Vollstreckung von in Strafverfahren ergangenen, mindestens viermonatigen Freiheitsstrafen oder freiheitsentziehenden Maßregeln der Sicherung erlassen werden, sofern diese in dem Fall, dass sich der Verurteilte der Justiz entzogen hat, nicht in Abwesenheit ergangen sind.

(4) Eine Europäische Sicherungsanordnung enthält folgende Angaben:

a) die Anordnungsbehörde und die etwaige validierende Behörde;

b) den Adressaten der Europäischen Sicherungsanordnung gemäß Artikel 7;

c) den Nutzer, es sei denn, der einzige Zweck der Anordnung besteht darin, den Nutzer zu identifizieren, oder andere eindeutige Kennungen wie Nutzername, Anmeldekennung oder Kontobezeichnung zur Bestimmung der Daten, für welche die Sicherung angefordert wird;

d) die Kategorie der angeforderten Daten im Sinne des Artikels 3 Nummern 9 bis 12;

e) erforderlichenfalls die Zeitspanne der Daten, für welche die Sicherung angefordert wird;

f) die anwendbaren Bestimmungen des Strafrechts des Anordnungsstaats;

g) die Gründe für die Feststellung, dass die Europäische Sicherungsanordnung die Voraussetzungen der Notwendigkeit und Verhältnismäßigkeit gemäß Absatz 2 des vorliegenden Artikels erfüllt;

Artikel 7

Adressaten von Europäischen Herausgabeanordnungen und Europäischen Sicherungsanordnungen

(1) Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen werden unmittelbar an eine benannte Niederlassung oder einen Vertreter des betroffenen Diensteanbieters gerichtet.

(2) Ausnahmsweise können in Notfällen im Sinne des Artikels 3 Nummer 18, in denen die benannte Niederlassung oder der Vertreter eines Diensteanbieters nicht innerhalb der Fristen auf ein EPOC oder ein EPOC-PR reagiert, ein EPOC oder ein EPOC-PR an jede andere Niederlassung oder jeden anderen Vertreter des Diensteanbieters in der Union gerichtet werden.

Artikel 8

Unterrichtung der Vollstreckungsbehörde

(1) Wird eine Europäische Herausgabeanordnung zur Erlangung von Verkehrsdaten mit Ausnahme von ausschließlich zum Zweck der Identifizierung des Nutzers angeforderten Daten im Sinne des Artikels 3 Nummer 10 oder zur Erlangung von Inhaltsdaten erlassen, so unterrichtet die Anordnungsbehörde die Vollstreckungsbehörde hiervon, indem sie ihr gemäß Artikel 9 Absatz 1 und 2 das EPOC zur gleichen Zeit wie dem Adressaten übermittelt.

(2) Absatz 1 findet keine Anwendung, wenn die Anordnungsbehörde zum Zeitpunkt des Erlasses der Anordnung hinreichende Gründe zu der Annahme hat, dass

a) die Straftat im Anordnungsstaat begangen wurde, begangen wird oder wahrscheinlich begangen werden wird und

b) die Person, deren Daten angefordert werden, im Anordnungsstaat ansässig ist.

(3) Bei der in Absatz 1 genannten Übermittlung des EPOC an die Vollstreckungsbehörde fügt die Anordnungsbehörde alle etwaigen zusätzlichen Informationen bei, die für die Prüfung der Möglichkeit der Geltendmachung eines Ablehnungsgrundes gemäß Artikel 12 erforderlich sein könnten.

(4) Die in Absatz 1 des vorliegenden Artikels genannte Unterrichtung der Vollstreckungsbehörde hat außer in Notfällen im Sinne des Artikels 3 Nummer 18 aufschiebende Wirkung für die in Artikel 10 Absatz 2 festgelegten Verpflichtungen des Adressaten.

Artikel 9

Bescheinigung über eine Europäische Herausgabeanordnung (EPOC) und Bescheinigung über eine Europäische Sicherungsanordnung (EPOC-PR)

(1) Eine Europäische Herausgabeanordnung oder eine Europäische Sicherungsanordnung wird dem Adressaten im Sinne des Artikels 7 in Form eines EPOC beziehungsweise eines EPOC-PR übermittelt.

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

(2) Ein EPOC enthält die in Artikel 5 Absatz 5 Buchstaben a bis h aufgeführten Angaben, einschließlich ausreichender Informationen, die es dem Adressaten ermöglichen, erforderlichenfalls die Anordnungsbehörde und die Vollstreckungsbehörde festzustellen und Kontakt zu ihnen aufzunehmen.

Ist gemäß Artikel 8 eine Unterrichtung der Vollstreckungsbehörde erforderlich, so muss das dieser Behörde übermittelte EPOC die in Artikel 5 Absatz 5 Buchstaben a bis j aufgeführten Angaben enthalten.

(3) Ein EPOC-PR enthält die in Artikel 6 Absatz 4 Buchstaben a bis f aufgeführten Angaben, einschließlich ausreichender Informationen, um es dem Adressaten zu ermöglichen, die Anordnungsbehörde festzustellen und Kontakt zu ihr aufzunehmen.

(4) Im Bedarfsfall sind das EPOC oder das EPOC-PR in eine vom Adressaten akzeptierte Amtssprache der Union gemäß Artikel 4 der Richtlinie (EU) 2023/1544 zu übersetzen. Hat der Diensteanbieter keine Sprache angegeben, so ist das EPOC oder das EPOC-PR in eine Amtssprache des Mitgliedstaats zu übersetzen, in dem sich die benannte Niederlassung oder der Vertreter des Diensteanbieters befindet.

Ist gemäß Artikel 8 eine Unterrichtung der Vollstreckungsbehörde erforderlich, so ist das an diese Behörde zu übermittelnde EPOC in eine Amtssprache des Vollstreckungsstaats oder in eine andere von diesem Staat akzeptierte Amtssprache der Union zu übersetzen.

Artikel 10

Ausführung eines EPOC

(1) Nach Erhalt eines EPOC wird der Adressat umgehend zur Sicherung der angeforderten Daten tätig.

(2) Ist gemäß Artikel 8 eine Unterrichtung der Vollstreckungsbehörde erforderlich und hat diese Behörde nicht innerhalb von zehn Tagen nach Erhalt des EPOC einen der in Artikel 12 genannten Ablehnungsgründe geltend gemacht, so stellt der Adressat sicher, dass die angeforderten Daten nach Ablauf dieser zehntägigen Frist unmittelbar der Anordnungsbehörde oder den im EPOC angegebenen Strafverfolgungsbehörden übermittelt werden. Bestätigt die Vollstreckungsbehörde bereits vor Ablauf der zehntägigen Frist der Anordnungsbehörde und dem Adressaten, dass sie keinen Ablehnungsgrund geltend machen wird, so muss der Adressat nach dieser Bestätigung so bald wie möglich, spätestens jedoch nach Ablauf dieser zehntägigen Frist, tätig werden.

(3) Ist gemäß Artikel 8 keine Unterrichtung der Vollstreckungsbehörde erforderlich, so muss der Adressat nach Erhalt eines EPOC dafür sorgen, dass die angeforderten Daten spätestens innerhalb von zehn Tagen nach Erhalt des EPOC unmittelbar der Anordnungsbehörde oder den im EPOC angegebenen Strafverfolgungsbehörden übermittelt werden.

(4) In Notfällen übermittelt der Adressat die angeforderten Daten unverzüglich, spätestens jedoch innerhalb von acht Stunden nach Erhalt des EPOC. Ist gemäß Artikel 8 eine Unterrichtung der Vollstreckungsbehörde erforderlich, so kann die Vollstreckungsbehörde, wenn sie im Einklang mit Artikel 12 Absatz 1 die Geltendmachung eines Ablehnungsgrundes beschließt, unverzüglich und spätestens innerhalb von 96 Stunden nach Erhalt der Unterrichtung die Anordnungsbehörde und den Adressaten davon in Kenntnis setzen, dass sie Einwände gegen die Verwendung der Daten hat oder dass die Daten nur unter bestimmten Voraussetzungen, die die Vollstreckungsbehörde anzugeben hat, verwendet werden dürfen. Macht die Vollstreckungsbehörde einen Ablehnungsgrund geltend und hat der Adressat die Daten bereits der Anordnungsbehörde übermittelt, so muss die Anordnungsbehörde die Daten löschen oder deren Verwendung anderweitig beschränken, oder hat die Vollstreckungsbehörde Voraussetzungen für die Verwendung angegeben, so muss die Anordnungsbehörde diese Voraussetzungen bei der Verwendung der Daten erfüllen.

(5) Ist der Adressat allein aufgrund der im EPOC enthaltenen Informationen der Auffassung, dass die Vollstreckung des EPOC Immunitäten oder Vorrechte oder die Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Freiheit der Presse und das Recht auf freie Meinungsäußerung in anderen Medien gemäß dem Recht des Vollstreckungsstaats beeinträchtigen könnte, so setzt der Adressat die Anordnungsbehörde und die Vollstreckungsbehörde unter Verwendung des in Anhang III festgelegten Formulars davon in Kenntnis.

Ist gemäß Artikel 8 keine Unterrichtung der Vollstreckungsbehörde erfolgt, so trägt die Anordnungsbehörde den in Unterabsatz 1 des vorliegenden Absatzes genannten Informationen Rechnung und entscheidet von sich aus oder auf Ersuchen der Vollstreckungsbehörde, ob die Europäische Herausgabeanordnung zurückgenommen, angepasst oder aufrechterhalten wird.

Ist gemäß Artikel 8 eine Unterrichtung der Vollstreckungsbehörde erfolgt, so trägt die Anordnungsbehörde den in Unterabsatz 1 des vorliegenden Absatzes genannten Informationen Rechnung und entscheidet, ob die Europäische Herausgabeanordnung zurückgenommen, angepasst oder aufrechterhalten wird. Die Vollstreckungsbehörde kann beschließen, die in Artikel 12 genannten Ablehnungsgründe geltend zu machen.

(6) Kann der Adressat seiner Verpflichtung zur Herausgabe der angeforderten Daten nicht nachkommen, weil das EPOC unvollständig ist, offensichtliche Fehler enthält oder keine ausreichenden Informationen zur Ausführung des EPOC enthält, so setzt er die im EPOC angegebene Anordnungsbehörde und, sofern gemäß Artikel 8 eine Unterrichtung der Vollstreckungsbehörde erfolgt ist, die Vollstreckungsbehörde unverzüglich hiervon in Kenntnis und ersucht unter Verwendung des in Anhang III festgelegten Formulars um Klarstellung. Gleichzeitig teilt der Adressat der Anordnungsbehörde mit, ob die in Absatz 9 genannte Identifizierung der angeforderten Daten und deren Sicherung möglich war.

Die Anordnungsbehörde reagiert umgehend, spätestens jedoch innerhalb von fünf Tagen nach Erhalt des Formulars. Der Adressat stellt sicher, dass er die notwendige Klarstellung oder Berichtigung durch die Anordnungsbehörde erhalten kann, damit er seinen in den Absätzen 1 bis 4 genannten Verpflichtungen nachkommen kann. Die in den Absätzen 1 bis 4 genannten Verpflichtungen gelten erst, wenn diese Klarstellung oder Berichtigung durch die Anordnungsbehörde oder die Vollstreckungsbehörde erfolgt ist.

(7) Kann der Adressat seiner Verpflichtung zur Herausgabe der angeforderten Daten aufgrund einer faktischen Unmöglichkeit infolge von Umständen, die nicht dem Adressaten angelastet werden können, nicht nachkommen, so setzt er die im EPOC angegebene Anordnungsbehörde und, sofern gemäß Artikel 8 eine Mitteilung an die Vollstreckungsbehörde erfolgt ist, die Vollstreckungsbehörde unverzüglich hiervon in Kenntnis und legt unter Verwendung des in Anhang III festgelegten Formulars die Gründe hierfür dar. Kommt die Anordnungsbehörde zu dem Schluss, dass eine solche faktische Unmöglichkeit besteht, so teilt sie dem Adressaten und, sofern gemäß Artikel 8 eine Unterrichtung der Vollstreckungsbehörde erfolgt ist, der Vollstreckungsbehörde mit, dass das EPOC nicht mehr ausgeführt werden muss.

(8) In allen Fällen, in denen der Adressat die angeforderten Daten aus anderen als den in den Absätzen 5, 6 und 7 des vorliegenden Artikels genannten Gründen überhaupt nicht, nicht vollständig oder nicht innerhalb der genannten Frist bereitstellt, setzt er die Anordnungsbehörde und, sofern gemäß Artikel 8 eine Unterrichtung an die Vollstreckungsbehörde erfolgt ist, die im EPOC genannte Vollstreckungsbehörde unverzüglich, spätestens jedoch innerhalb der in den Absätzen 2, 3 und 4 des vorliegenden Artikels genannten Fristen unter Verwendung des in Anhang III festgelegten Formulars von den Gründen hierfür in Kenntnis. Die Anordnungsbehörde überprüft die Europäische Herausgabeanordnung im Lichte der vom Adressaten übermittelten Informationen und setzt erforderlichenfalls eine neue Frist für die Herausgabe der Daten durch den Adressaten fest.

(9) Die Daten werden weitest möglich gesichert, bis sie herausgegeben werden, unabhängig davon, ob die Herausgabe letztendlich auf der Grundlage einer klargestellten Europäischen Herausgabeanordnung und des dazugehörigen EPOC oder über andere Kanäle wie die Rechtshilfe oder bis zum Widerruf der Europäischen Herausgabeanordnung erfolgt.

Ist die Herausgabe von Daten und ihre Sicherung nicht mehr erforderlich, so setzen die Anordnungsbehörde und, falls einschlägig, gemäß Artikel 16 Absatz 8, die Vollstreckungsbehörde den Adressaten unverzüglich hiervon in Kenntnis.

Artikel 11

Ausführung eines EPOC-PR

(1) Nach Erhalt einer EPOC-PR sichert der Adressat unverzüglich die angeforderten Daten. Die Verpflichtung zur Sicherung der Daten endet nach 60 Tagen, es sei denn, die Anordnungsbehörde bestätigt unter Verwendung des in Anhang V festgelegten Formulars, dass ein entsprechendes Ersuchen um Herausgabe gestellt wurde. Während dieses Zeitraums von 60 Tagen kann die Anordnungsbehörde unter Verwendung des in Anhang VI festgelegten Formblatts die Dauer der Verpflichtung zur Sicherung der Daten um einen weiteren Zeitraum von 30 Tagen verlängern, wenn dies erforderlich ist, um ein entsprechendes Ersuchen um Herausgabe zu ermöglichen.

(2) Bestätigt die Anordnungsbehörde während des in Absatz 1 festgelegten Zeitraums der Sicherung, dass ein entsprechendes Ersuchen um Herausgabe gestellt wurde, so sichert der Adressat die Daten so lange, wie dies erforderlich ist, um die Daten nach Erhalt des entsprechenden Ersuchens um Herausgabe herauszugeben.

(3) Ist die Sicherung nicht mehr erforderlich, so setzt die Anordnungsbehörde den Adressaten unverzüglich hiervon in Kenntnis, und die auf der betreffenden Europäischen Sicherungsanordnung beruhende Verpflichtung zur Sicherung erlischt.

(4) Ist der Adressat allein aufgrund der im EPOC-PR enthaltenen Informationen der Auffassung, dass die Vollstreckung des EPOC-PR Immunitäten oder Vorrechte oder die Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Freiheit der Presse und das Recht auf freie Meinungsäußerung in anderen Medien gemäß dem Recht des Vollstreckungsstaats beeinträchtigen könnte, so setzt der Adressat die Anordnungsbehörde und die Vollstreckungsbehörde unter Verwendung des in Anhang III festgelegten Formulars davon in Kenntnis.

Die Anordnungsbehörde trägt den in Unterabsatz 1 genannten Informationen Rechnung und entscheidet von sich aus oder auf Ersuchen der Vollstreckungsbehörde, ob die Europäische Sicherungsanordnung zurückgenommen, angepasst oder aufrechterhalten wird.

(5) Kann der Adressat seiner Verpflichtung zur Sicherung der angeforderten Daten nicht nachkommen, weil die Bescheinigung unvollständig ist, offensichtliche Fehler enthält oder keine ausreichenden Informationen zur Ausführung des EPOC-PR enthält, so setzt er die im EPOC-PR angegebene Anordnungsbehörde unverzüglich hiervon in Kenntnis und ersucht unter Verwendung des Formulars in Anhang III um Klarstellung.

Die Anordnungsbehörde reagiert umgehend, spätestens jedoch innerhalb von fünf Tagen nach Erhalt des Formulars. Der Adressat stellt sicher, dass er die notwendige Klarstellung oder Berichtigung durch die Anordnungsbehörde erhalten kann, damit er seinen in den Absätzen 1, 2 und 3 festgelegten Verpflichtungen nachkommen kann. Reagiert die Anordnungsbehörde innerhalb der Fünftagesfrist nicht, so ist der Diensteanbieter von den in den Absätzen 1 und 2 festgelegten Verpflichtungen befreit.

(6) Kann der Adressat seiner Verpflichtung zur Sicherung der angeforderten Daten aufgrund einer faktischen Unmöglichkeit infolge von Umständen, die nicht dem Adressaten angelastet werden können, nicht nachkommen, so setzt er die im EPOC-PR angegebene Anordnungsbehörde unverzüglich hiervon in Kenntnis und legt unter Verwendung des in Anhang III festgelegten Formulars die Gründe hierfür dar. Kommt die Anordnungsbehörde zu dem Schluss, dass eine solche Unmöglichkeit besteht, so teilt sie dem Adressaten mit, dass das EPOC-PR nicht mehr ausgeführt werden muss.

(7) In allen Fällen, in denen der Adressat die angeforderten Daten aus anderen als den in den Absätzen 4, 5 und 6 genannten Gründen nicht sichert, setzt er die Anordnungsbehörde unverzüglich unter Verwendung des in Anhang III festgelegten Formulars von den Gründen hierfür in Kenntnis. Die Anordnungsbehörde überprüft die Europäische Sicherungsanordnung im Lichte der vom Adressaten übermittelten Begründung.

Artikel 12

Gründe für die Ablehnung von Europäischen Herausgabeanordnungen

(1) Hat die Anordnungsbehörde gemäß Artikel 8 eine Unterrichtung der Vollstreckungsbehörde vorgenommen, so prüft die Vollstreckungsbehörde unbeschadet des Artikels 1 Absatz 3 so bald wie möglich, spätestens jedoch innerhalb von zehn Tagen nach Erhalt der Unterrichtung oder in Notfällen spätestens innerhalb von 96 Stunden nach deren Erhalt, die in der Anordnung enthaltenen Informationen und macht gegebenenfalls einen oder mehrere der folgenden Ablehnungsgründe geltend:

a) die angeforderten Daten sind durch Immunitäten oder Vorrechte geschützt, die nach dem Recht des Vollstreckungsstaats gewährt werden, wodurch die Ausführung oder Vollstreckung der Anordnung verhindert wird, oder die angeforderten Daten unterliegen Vorschriften zur Bestimmung und Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Freiheit der Presse und das Recht auf freie Meinungsäußerung in anderen Medien, wodurch die Ausführung oder Vollstreckung der Anordnung verhindert wird;

b) in Ausnahmefällen bestehen aufgrund genauer und objektiver Belege berechtigte Gründe zu der Annahme, dass die Ausführung der Anordnung unter den besonderen Umständen des Falles eine offensichtliche Verletzung eines einschlägigen in Artikel 6 EUV und der Charta verankerten Grundrechts zur Folge hätte;

c) die Ausführung der Anordnung würde dem Grundsatz „ne bis in idem“ zuwiderlaufen;

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

(2) Macht die Vollstreckungsbehörde gemäß Absatz 1 einen Ablehnungsgrund geltend, so setzt sie den Adressaten und die Anordnungsbehörde hiervon in Kenntnis. Der Adressat beendet die Vollstreckung der Europäischen Herausgabeanordnung und darf die Daten nicht übermitteln, und die Anordnungsbehörde widerruft die Anordnung.

(3) Bevor die nach Artikel 8 unterrichtete Vollstreckungsbehörde beschließt, einen Ablehnungsgrund geltend zu machen, setzt sie sich in geeigneter Weise mit der Anordnungsbehörde in Verbindung, um die zu treffenden angemessenen Maßnahmen zu erörtern. Auf dieser Grundlage kann die Anordnungsbehörde beschließen, die Europäische Herausgabeanordnung anzupassen oder zurückzuziehen. Wird im Anschluss an diese Erörterung keine Einigung erzielt, so kann die nach Artikel 8 unterrichtete Vollstreckungsbehörde beschließen, Gründe für die Ablehnung der Europäischen Herausgabeanordnung geltend zu machen, und muss dementsprechend die Anordnungsbehörde und den Adressaten hiervon in Kenntnis setzen.

(4) Beschließt die Vollstreckungsbehörde, gemäß Absatz 1 Ablehnungsgründe geltend zu machen, so kann sie angeben, ob sie Einwände gegen die Übermittlung sämtlicher Daten hat oder ob die Daten nur teilweise übermittelt oder nur unter bestimmten Bedingungen, die die Vollstreckungsbehörde gegebenenfalls anzugeben hat, verwendet werden dürfen.

(5) Hat eine Behörde des Vollstreckungsstaats die Befugnis für die Aufhebung der Immunität oder des Vorrechts im Sinne des Absatzes 1 Buchstabe a des vorliegenden Artikels, so kann die Anordnungsbehörde die gemäß Artikel 8 unterrichtete Vollstreckungsbehörde darum ersuchen, Verbindung mit der zuständigen Behörde des Vollstreckungsstaats aufzunehmen, um diese zu ersuchen, Ihre Befugnis unverzüglich auszuüben. Ist eine Behörde eines anderen Mitgliedstaats oder eines Drittlands oder eine internationale Organisation für die Aufhebung der Immunität oder des Vorrechts zuständig, so kann die Anordnungsbehörde, die betreffende Behörde um Ausübung dieser Befugnis zu ersuchen.

Artikel 13

Nutzerinformationen und Vertraulichkeit

(1) Die Anordnungsbehörde informiert die Person, deren Daten angefordert werden, unverzüglich über die Herausgabe von Daten auf der Grundlage einer Europäischen Herausgabeanordnung.

(2) Die Anordnungsbehörde kann im Einklang mit dem nationalen Recht des Anordnungsstaats die Information der Person, deren Daten angefordert werden, aufschieben, einschränken oder unterlassen, soweit und solange die Bedingungen von Artikel 13 Absatz 3 der Richtlinie (EU) 2016/680 erfüllt sind, wobei die Anordnungsbehörde in diesem Fall die Gründe für die Aufschiebung, Einschränkung oder Unterlassung in der Verfahrensakte anzugeben hat. Zudem ist dem EPOC eine kurze Begründung beizufügen.

(3) Bei der in Absatz 1 genannten Information der Person, deren Daten angefordert werden, übermittelt die Anordnungsbehörde auch Informationen über die gemäß Artikel 18 verfügbaren Rechtsbehelfe.

(4) Die Adressaten und, falls abweichend, die Diensteanbieter treffen die erforderlichen, dem neuesten Stand der Technik entsprechenden betrieblichen und technischen Maßnahmen, um die Vertraulichkeit, Geheimhaltung und Integrität des EPOC oder des EPOC-PR sowie der herausgegebenen oder gesicherten Daten sicherzustellen.

Artikel 14

Kostenerstattung

(1) Der Diensteanbieter kann beim Anordnungsstaat eine Erstattung seiner Kosten beantragen, wenn diese Möglichkeit im nationalen Recht des Anordnungsstaats für nationale Anordnungen in vergleichbaren Situationen vorgesehen ist; die Erstattung erfolgt nach Maßgabe des nationalen Rechts dieses Staates. Die Mitgliedstaaten teilen der Kommission ihre nationalen Vorschriften für die Kostenerstattung mit, und die Kommission veröffentlicht diese.

(2) Dieser Artikel gilt nicht für die Erstattung der Kosten für das dezentrale IT-System gemäß Artikel 25.

KAPITEL III

SANKTIONEN UND VOLLSTRECKUNG

Artikel 15

Sanktionen

(1) Unbeschadet nationaler Rechtsvorschriften, die die Verhängung strafrechtlicher Sanktionen vorsehen, erlassen die Mitgliedstaaten Vorschriften über finanzielle Sanktionen gemäß Artikel 16 Absatz 10, die bei Verstößen gegen die Artikel 10 und 11 und Artikel 13 Absatz 4 zu verhängen sind, und treffen alle für die Anwendung finanzieller Sanktionen erforderlichen Maßnahmen. Die vorgesehenen finanziellen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten stellen sicher, dass finanzielle Sanktionen in Höhe von bis zu 2 % des im vorhergehenden Geschäftsjahr weltweit erzielten Jahresgesamtumsatzes des Diensteanbieters verhängt werden können. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen unverzüglich mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.

(2) Unbeschadet ihrer Datenschutzpflichten dürfen die Diensteanbieter in den Mitgliedstaaten nicht für Schäden haftbar gemacht werden, die ihren Nutzern oder Dritten ausschließlich aufgrund der gutgläubigen Befolgung eines EPOC oder eines EPOC-PR entstehen.

Artikel 16

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 und hat die Vollstreckungsbehörde, sofern anwendbar, keinen der in Artikel 12 vorgesehenen Ablehnungsgründe geltend gemacht, so kann die Anordnungsbehörde die Vollstreckungsbehörde darum ersuchen, die Europäische Herausgabeanordnung oder die Europäische Sicherungsanordnung zu vollstrecken.

Für die Zwecke der Vollstreckung gemäß Unterabsatz 1 übermittelt die Anordnungsbehörde die betreffende Anordnung, das in Anhang III festgelegte, vom Adressaten ausgefüllte Formular und alle einschlägigen Dokumente gemäß Artikel 19. Die Anordnungsbehörde übersetzt die betreffende Anordnung und alle zu übermittelnden Unterlagen in eine der von dem Vollstreckungsstaat akzeptierten Sprachen und setzt den Adressaten von der Übermittlung in Kenntnis.

(2) Nach dem Erhalt erkennt die Vollstreckungsbehörde die 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 trifft die Entscheidung über die Anerkennung der betreffenden Anordnung unverzüglich, spätestens jedoch fünf Arbeitstage nach Erhalt der Anordnung.

(3) Die Vollstreckungsbehörde fordert die Adressaten förmlich auf, ihren entsprechenden Verpflichtungen nachzukommen, und setzt sie von Folgendem in Kenntnis:

a) der Möglichkeit, gegen die Ausführung der betreffenden Anordnung unter Geltendmachung eines oder mehrerer der in Absatz 4 Buchstaben a bis f oder Absatz 5 Buchstaben a bis e aufgeführten Gründe Einwände zu erheben,

b) den bei Nichtbefolgung anwendbaren Sanktionen und

c) der Frist für die Befolgung oder die Erhebung von Einwänden.

(4) Die Vollstreckung der Europäischen Herausgabeanordnung kann nur aus einem oder mehreren der folgenden Gründe 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 aufgrund von Umständen, die nicht dem Adressaten angelastet werden können, nicht möglich war oder weil das EPOC offensichtliche Fehler enthält;

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

e) die Dienstleistung fällt nicht unter diese Verordnung;

f) die angeforderten Daten sind durch Immunitäten oder Vorrechte geschützt, die nach dem Recht des Vollstreckungsstaats gewährt werden, oder die angeforderten Daten unterliegen Vorschriften über die Bestimmung oder Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Freiheit der Presse und die freie Meinungsäußerung in anderen Medien, wodurch die Ausführung oder Vollstreckung der Europäischen Sicherungsanordnung verhindert wird;

g) es ist in Ausnahmefällen ausschließlich anhand der in dem EPOC enthaltenen Informationen ersichtlich, dass aufgrund genauer und objektiver Belege berechtigte Gründe zu der Annahme bestehen, dass die Ausführung der Europäischen Herausgabeanordnung unter den besonderen Umständen des Falles eine offensichtliche Verletzung eines einschlägigen in Artikel 6 EUV und der Charta verankerten Grundrechts bedeuten würde.

(5) Die Vollstreckung der Europäischen Sicherungsanordnung kann nur aus einem oder mehreren der folgenden Gründe abgelehnt werden:

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

b) der Adressat konnte dem EPOC-PR nicht Folge leisten, weil dies faktisch aufgrund von Umständen, die nicht dem Adressaten angelastet werden können, nicht möglich war oder weil das EPOC-PR offensichtliche Fehler enthält;

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

d) die Dienstleistung fällt nicht unter diese Verordnung;

e) die angeforderten Daten sind durch Immunitäten oder Vorrechte geschützt, die nach dem Recht des Vollstreckungsstaats gewährt werden, oder die angeforderten Daten unterliegen Vorschriften über die Bestimmung oder Beschränkung der strafrechtlichen Verantwortlichkeit in Bezug auf die Freiheit der Presse und die freie Meinungsäußerung in anderen Medien, wodurch die Ausführung oder Vollstreckung der Europäischen Sicherungsanordnung verhindert wird;

f) es ist in Ausnahmefällen ausschließlich anhand der in dem EPOC-PR enthaltenen Informationen ersichtlich, dass aufgrund genauer und objektiver Belege berechtigte Gründe zu der Annahme bestehen, dass die Ausführung der Europäischen Sicherungsanordnung unter den besonderen Umständen des Falles eine offensichtliche Verletzung eines einschlägigen in Artikel 6 EUV und der Charta verankerten Grundrechts bedeuten würde.

(6) Erhebt der Adressat gemäß Absatz 3 Buchstabe a Einwände, so entscheidet die Vollstreckungsbehörde auf der Grundlage etwaiger von dem Adressaten bereitgestellter Informationen und erforderlichenfalls der von der Anordnungsbehörde gemäß Absatz 7 erhaltenen zusätzlichen Informationen, ob sie die Europäische Herausgabeanordnung bzw. die Europäische Sicherungsanordnung vollstreckt.

(7) Bevor die Vollstreckungsbehörde beschließt, die Europäische Herausgabeanordnung bzw. die Europäische Sicherungsanordnung gemäß Absatz 2 bzw. Absatz 6 nicht anzuerkennen oder nicht zu vollstrecken, konsultiert sie in geeigneter Weise die Anordnungsbehörde. Erforderlichenfalls ersucht sie die Anordnungsbehörde um weitere Auskünfte. Die Anordnungsbehörde beantwortet ein solches Ersuchen innerhalb von fünf Arbeitstagen.

(8) Die Vollstreckungsbehörde teilt der Anordnungsbehörde und dem Adressaten alle ihre Beschlüsse unverzüglich mit.

(9) Erhält die Vollstreckungsbehörde die im Wege einer Europäischen Herausgabeanordnung angeforderten Daten von dem Adressaten, so übermittelt sie diese Daten unverzüglich der Anordnungsbehörde.

(10) Kommt der Adressat seinen Verpflichtungen aus einer anerkannten Europäischen Herausgabeanordnung oder Europäischen Sicherungsanordnung, deren Vollstreckbarkeit von der Vollstreckungsbehörde bestätigt wurde, nicht nach, so verhängt diese Behörde eine finanzielle Sanktion gemäß Artikel 15. Gegen einen Beschluss zur Verhängung einer finanziellen Sanktion muss ein wirksamer Rechtsbehelf eingelegt werden können.

KAPITEL IV

GESETZESKOLLISIONEN UND RECHTSBEHELFE

Artikel 17

Überprüfungsverfahren bei einander widersprechenden Verpflichtungen

(1) Ist ein Adressat der Ansicht, dass die Befolgung einer Europäischen Herausgabeanordnung im Widerspruch zu einer Verpflichtung stehen würde, die sich aus dem anwendbaren Recht eines Drittlands ergibt, so teilt er der Anordnungsbehörde und der Vollstreckungsbehörde gemäß dem in Artikel 10 Absätze 8 und 9 festgelegten Verfahren seine Gründe für die Nichtausführung der Europäischen Herausgabeanordnung mit, wobei das in Anhang III festgelegte Formular (im Folgenden „begründeter Einwand“) zu verwenden ist.

(2) Der begründete Einwand muss alle erheblichen Einzelheiten zu den betreffenden Rechtsvorschriften des Drittlands, zu ihrer Anwendbarkeit auf den vorliegenden Fall und zur Art der einander widersprechenden Verpflichtungen enthalten. Der begründete Einwand darf sich nicht auf Folgendes stützen:

a) die Tatsache, dass es in den geltenden Rechtsvorschriften des Drittlands keine vergleichbaren Bestimmungen über die Voraussetzungen, Formvorschriften und Verfahren für den Erlass einer Herausgabeanordnung gibt, oder

b) allein die Tatsache, dass die Daten in einem Drittland gespeichert sind.

Der begründete Einwand muss spätestens zehn Tage nach Eingang des EPOC beim Adressaten erhoben werden.

(3) Die Anordnungsbehörde überprüft die Europäische Herausgabeanordnung auf der Grundlage des begründeten Einwands und der etwaigen Anmerkungen des Vollstreckungsstaats. Beabsichtigt die Anordnungsbehörde, die Europäische Herausgabeanordnung aufrechtzuerhalten, so beantragt sie eine Überprüfung durch das zuständige Gericht des Anordnungsstaats. Die Ausführung der Europäischen Herausgabeanordnung wird bis zum Abschluss des Überprüfungsverfahrens ausgesetzt.

(4) Das zuständige Gericht beurteilt zunächst, ob eine Kollision von Verpflichtungen vorliegt, und prüft dazu, ob

a) das Recht des Drittlands aufgrund der spezifischen Umstände des betreffenden Falls anwendbar ist und

b) die Rechtsvorschriften des Drittlands – sofern sie gemäß Buchstabe a anwendbar sind – die Offenlegung der betreffenden Daten verbieten, wenn sie auf die spezifischen Umstände des betreffenden Falls angewandt werden.

(5) Stellt das zuständige Gericht fest, dass keine relevante Kollision mit Verpflichtungen im Sinne der Absätze 1 und 4 vorliegt, so erhält es die Europäische Herausgabeanordnung aufrecht.

(6) Stellt das zuständige Gericht auf der Grundlage der Beurteilung gemäß Absatz 4 Buchstabe b fest, dass die Rechtsvorschriften des Drittlands die Offenlegung der betreffenden Daten verbieten, so entscheidet es, ob die Europäische Herausgabeanordnung aufrechtzuerhalten oder aufzuheben ist. Diese Beurteilung stützt sich insbesondere auf folgende Faktoren, wobei den in den Buchstaben a und b genannten Faktoren besondere Bedeutung beizumessen ist:

a) das nach den einschlägigen Rechtsvorschriften des Drittlands geschützte Interesse, einschließlich der Grundrechte und sonstiger grundlegender Interessen, die eine Offenlegung der Daten verhindern, insbesondere die nationalen Sicherheitsinteressen des Drittlands;

b) den Grad der Verbindung zwischen der Strafsache, derentwegen die Europäische Herausgabeanordnung erlassen wurde, und einem der beiden Rechtssysteme; hierfür maßgeblich sind unter anderem:

   i) der Aufenthaltsort, die Staatsangehörigkeit und der Wohnsitz der Person, deren Daten angefordert werden, oder des Opfers bzw. der Opfer der betreffenden Straftat,

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

c) den Grad der Verbindung zwischen dem Diensteanbieter und dem betreffenden Drittstaat; in diesem Zusammenhang genügt der Datenspeicherort allein nicht zur Feststellung eines wesentlichen Verbindungsgrads;

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

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

(7) Das zuständige Gericht kann bei der zuständigen Behörde des Drittlands unter Berücksichtigung der Richtlinie (EU) 2016/680, insbesondere des Kapitels V, Informationen anfordern, soweit das betreffende Strafverfahren dadurch nicht behindert wird. Der Anordnungsstaat fordert bei der zuständigen Behörde des Drittlands insbesondere dann Informationen an, wenn der Konflikt der Verpflichtungen die Grundrechte oder sonstige grundlegende Interessen des Drittlands im Zusammenhang mit der nationalen Sicherheit und Verteidigung betrifft.

(8) Beschließt das zuständige Gericht, die Europäische Herausgabeanordnung aufzuheben, so teilt es dies der Anordnungsbehörde und dem Adressaten mit. Stellt das zuständige Gericht fest, dass die Europäische Herausgabeanordnung aufrechtzuerhalten ist, so teilt es dies der Anordnungsbehörde und dem Adressaten mit, und der Adressat hat die Europäische Herausgabeanordnung auszuführen.

(9) Für die Zwecke der Verfahren nach diesem Artikel werden die Fristen gemäß dem nationalen Recht der Anordnungsbehörde berechnet.

(10) Die Anordnungsbehörde unterrichtet die Vollstreckungsbehörde über das Ergebnis des Überprüfungsverfahrens.

Artikel 18

Wirksame Rechtsbehelfe

(1) Unbeschadet weiterer Rechtsbehelfe, die nach dem nationalen Recht zur Verfügung stehen, haben Personen, deren Daten im Wege einer Europäischen Herausgabeanordnung angefordert wurden, das Recht, wirksame Rechtsbehelfe gegen diese Anordnung einzulegen. Handelt es sich bei der betreffenden Person um einen Verdächtigen oder Beschuldigten, so hat die betreffende Person das Recht, während des Strafverfahrens, in dem die Daten verwendet wurden, wirksame Rechtsbehelfe einzulegen. Das im vorliegenden Absatz vorgesehene Recht auf wirksame Rechtsbehelfe lässt das Recht auf Einlegung von Rechtsbehelfen gemäß der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 unberührt.

(2) Das Recht auf Einlegung wirksamer Rechtsbehelfe wird vor einem Gericht des Anordnungsstaats nach dessen nationalem Recht ausgeübt und umfasst die Möglichkeit, die Rechtmäßigkeit der Maßnahme, einschließlich ihrer Notwendigkeit und Verhältnismäßigkeit, anzufechten; die Grundrechtsgarantien im Vollstreckungsstaat bleiben hiervon unberührt.

(3) Für die Zwecke von Artikel 13 Absatz 1 werden rechtzeitig Informationen über die nach nationalem Recht bestehenden Möglichkeiten zur Einlegung von Rechtsbehelfen bereitgestellt und wird sichergestellt, dass die Rechtsbehelfe effektiv wahrgenommen werden können.

(4) Für die Zwecke dieser Verordnung entsprechen die Fristen oder sonstigen Voraussetzungen für die Einlegung von Rechtsbehelfen denen, die in vergleichbaren nationalen Fällen gelten, und werden in einer Weise angewendet, die gewährleistet, dass die betroffenen Personen diese Rechtsbehelfe wirksam ausüben können.

(5) Unbeschadet der nationalen Verfahrensvorschriften stellen der Anordnungsstaat und jeder andere Mitgliedstaat, dem gemäß dieser Verordnung elektronische Beweismittel übermittelt worden sind, sicher, dass bei der Bewertung der mittels einer Europäischen Herausgabeanordnung eingeholten Beweismittel die Verteidigungsrechte gewahrt werden und ein faires Verfahren gewährleistet wird.

KAPITEL V

DEZENTRALES IT-SYSTEM

Artikel 19

Sichere digitale Kommunikation und sicherer Datenaustausch zwischen zuständigen Behörden und Diensteanbietern sowie zwischen zuständigen Behörden

(1) Die schriftliche Kommunikation zwischen zuständigen Behörden und benannten Niederlassungen oder Vertretern im Rahmen dieser Verordnung, einschließlich des Austauschs der in dieser Verordnung vorgesehenen Formulare und der im Wege einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung angeforderten Daten, erfolgt über ein sicheres und zuverlässiges dezentrales IT-System (im Folgenden „dezentrales IT-System").

(2) Jeder Mitgliedstaat stellt sicher, dass die benannten Niederlassungen oder Vertreter der Diensteanbieter, die in dem jeweiligen Mitgliedstaat ansässig sind, über ihr jeweiliges nationales IT-System Zugang zum dezentralen IT-System erhalten.

(3) Die Diensteanbieter stellen sicher, dass ihre benannten Niederlassungen oder Vertreter das dezentrale IT-System über das jeweilige nationale IT-System nutzen können, um EPOC und EPOC-PR zu empfangen, die angeforderten Daten der Anordnungsbehörde zu übermitteln und auf jede andere in dieser Verordnung vorgesehenen Weise mit der Anordnungsbehörde und der Vollstreckungsbehörde zu kommunizieren.

(4) Die schriftliche Kommunikation zwischen den zuständigen Behörden im Rahmen dieser Verordnung, einschließlich des Austauschs der in dieser Verordnung vorgesehenen Formulare und des Austauschs der angeforderten Daten im Rahmen des in Artikel 16 vorgesehenen Vollstreckungsverfahrens, sowie die schriftliche Kommunikation mit den zuständigen Einrichtungen oder sonstigen Stellen der Union erfolgen über das dezentrale IT-System.

(5) Ist die Kommunikation über das dezentrale IT-System gemäß den Absätzen 1 oder 4 nicht möglich – beispielsweise aufgrund einer Störung des dezentralen IT-Systems, aufgrund der Art des übermittelten Materials, aufgrund technischer Einschränkungen, etwa in Bezug auf die Größe der Daten, aufgrund rechtlicher Einschränkungen in Bezug auf die Zulässigkeit der angeforderten Daten als Beweismittel oder in Bezug auf forensische Anforderungen an die angeforderten Daten oder aufgrund außergewöhnlicher Umstände –, so erfolgt die Übermittlung mit den am besten geeigneten alternativen Mitteln, wobei die Notwendigkeit eines raschen, sicheren und zuverlässigen Informationsaustauschs, der dem Empfänger die Feststellung der Echtheit ermöglicht, zu berücksichtigen ist.

(6) Erfolgt eine Übermittlung mit alternativen Mitteln gemäß Absatz 5, so erfasst der Ersteller die Übermittlung unverzüglich im dezentralen IT-System, einschließlich – falls erfasst – des Datums und der Uhrzeit der Übermittlung, des Absenders und des Empfängers sowie des Namens und der Größe der Datei.

Artikel 20

Rechtswirkung elektronischer Dokumente

Dokumenten, die im Rahmen der elektronischen Kommunikation übermittelt werden, darf die Rechtswirkung oder die Zulässigkeit im Zusammenhang mit grenzüberschreitenden Gerichtsverfahren nach dieser Verordnung nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegen.

Artikel 21

Elektronische Signaturen und Siegel

(1) Für die elektronische Kommunikation nach dieser Verordnung gilt der mit der Verordnung (EU) Nr. 910/2014 geschaffene allgemeine Rechtsrahmen für die Verwendung von Vertrauensdiensten.

(2) Erfordert ein im Rahmen der elektronischen Kommunikation gemäß Artikel 19 Absatz 1 oder 4 dieser Verordnung übermitteltes Dokument gemäß dieser Verordnung ein Siegel oder eine Unterschrift, so muss das Dokument ein qualifiziertes elektronisches Siegel oder eine qualifizierte elektronische Signatur im Sinne der Verordnung (EU) Nr. 910/2014 enthalten.

Artikel 22

Referenzimplementierungssoftware

(1) Die Kommission ist verantwortlich für die Schaffung, Wartung und Weiterentwicklung einer Referenzimplementierungssoftware, für deren Einsatz sich die Mitgliedstaaten als ihr Back-End-System anstelle eines nationalen IT-Systems entscheiden können. Die Schaffung, Wartung und Weiterentwicklung der Referenzimplementierungssoftware werden aus dem Gesamthaushalt der Union finanziert.

(2) Die Kommission stellt die Referenzimplementierungssoftware sowie die entsprechende Wartung und Unterstützung kostenfrei bereit.

Artikel 23

Kosten des dezentralen IT-Systems

(1) Jeder Mitgliedstaat trägt die Kosten für die Einrichtung, den Betrieb und die Wartung der Zugangspunkte des dezentralen IT-Systems, für die dieser Mitgliedstaat zuständig ist.

(2) Jeder Mitgliedstaat trägt die Kosten für die Einrichtung und Anpassung seiner jeweiligen nationalen IT-Systeme zur Herstellung der Interoperabilität mit den Zugangspunkten sowie die Kosten für Verwaltung, Betrieb und Instandhaltung dieser Systeme.

(3) Die Einrichtungen und sonstigen Stellen der Union tragen die Kosten für die Einrichtung, den Betrieb und die Wartung der Komponenten des unter ihrer Verantwortung stehenden dezentralen IT-Systems.

(4) Die Einrichtungen und sonstigen Stellen der Union tragen die Kosten für die Einrichtung und Anpassung ihrer Fallbearbeitungssysteme zur Herstellung der Interoperabilität mit den Zugangspunkten sowie die Kosten für Verwaltung, Betrieb und Wartung dieser Systeme.

(5) Die Diensteanbieter tragen alle Kosten, die für die erfolgreiche Integration oder anderweitige Interaktion mit dem dezentralen IT-System erforderlich sind.

Artikel 24

Übergangszeitraum

Bevor die Verpflichtung zur schriftlichen Kommunikation über das dezentrale IT-System gemäß Artikel 19 anwendbar wird („Übergangszeitraum"), erfolgt die schriftliche Kommunikation zwischen den zuständigen Behörden und den benannten Niederlassungen oder Vertretern im Rahmen dieser Verordnung auf die am besten geeignete alternative Weise, wobei der Notwendigkeit Rechnung zu tragen ist, für einen raschen, sicheren und zuverlässigen Informationsaustausch zu sorgen. Wenn Diensteanbieter, Mitgliedstaaten oder Agenturen oder Einrichtungen der Union spezielle Plattformen oder andere sichere Kanäle für die Bearbeitung von Ersuchen um Daten von Strafverfolgungs- und Justizbehörden eingerichtet haben, können die Ausstellungsbehörden während dieses Übergangszeitraums auch beschließen, ein EPOC oder EPOC-PR über diese Kanäle an die benannten Niederlassungen oder Vertreter zu übermitteln.

Artikel 25

Durchführungsrechtsakte

(1) Zur Einrichtung und Verwendung des für die Zwecke dieser Verordnung zu nutzenden dezentralen IT-Systems erlässt die Kommission Durchführungsrechtsakte, durch die sie Folgendes festlegt:

a) die technischen Spezifikationen zur Festlegung der Methoden zur elektronischen Kommunikation für die Zwecke des dezentralen IT-Systems;

b) die technischen Spezifikationen für Kommunikationsprotokolle;

c) die Informationssicherheitsziele und entsprechenden technischen Maßnahmen zur Gewährleistung von Mindeststandards für die Informationssicherheit und eines hohen Cybersicherheitsniveaus bei der Verarbeitung und Übermittlung von Informationen im dezentralen IT-System;

d) die Mindestverfügbarkeitsziele und mögliche damit verbundene technische Anforderungen an die Leistungen des dezentralen IT-Systems.

(2) Die in Absatz 1 des vorliegenden Artikels genannten Durchführungsrechtsakte werden gemäß dem in Artikel 26 genannten Prüfverfahren erlassen.

(3) Die in Absatz 1 genannten Durchführungsrechtsakte werden bis zum 18. August 2025 erlassen.

Artikel 26

Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

KAPITEL VI

SCHLUSSBESTIMMUNGEN

Artikel 27

Sprachen

Jeder Mitgliedstaat kann jederzeit beschließen, dass er Übersetzungen von EPOC und EPOC-PR in eine oder mehrere Amtssprachen der Union neben seiner Amtssprache bzw. seinen Amtssprachen akzeptiert und er zeigt diesen Beschluss in einer schriftlichen Erklärung an, die der Kommission vorgelegt wird. Die Kommission stellt die Erklärungen allen Mitgliedstaaten und dem Europäischen Justiziellen Netz zur Verfügung.

Artikel 28

Überwachung und Berichterstattung

(1) Die Kommission stellt bis zum 18. August 2026 ein ausführliches Programm für die Überwachung der Leistungen, Ergebnisse und Auswirkungen dieser Verordnung auf. In dem Programm für die Überwachung werden die Instrumente benannt, mit denen Daten 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 zu ergreifen haben.

(2) In jedem Fall erheben die Mitgliedstaaten ab dem 18. August 2026 bei den zuständigen Behörden umfassende Statistiken und halten diese Statistiken vor. Die für das vorangegangene Kalenderjahr erhobenen Daten werden der Kommission jährlich bis zum 31. März übermittelt und umfassen:

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

b) die Zahl der EPOC, die im Rahmen von Ausnahmeregelungen für Notfälle ausgestellt wurden;

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

d) die Zahl der Mitteilungen an die Vollstreckungsbehörden gemäß Artikel 8 und die Zahl der EPOC, denen nicht Folge geleistet wurde, aufgeschlüsselt nach der Art der angeforderten Daten, den Adressaten, der jeweiligen Situation (Notfall oder nicht) und dem angeführten Ablehnungsgrund;

e) im Falle von EPOC, denen Folge geleistet wurde, die durchschnittliche Zeitspanne zwischen dem Zeitpunkt der Ausstellung eines EPOC und dem Zeitpunkt des Erhalts der angeforderten Daten, aufgeschlüsselt nach der Art der angeforderten Daten, den Adressaten und der jeweiligen Situation (Notfall oder nicht);

f) im Falle von EPOC-PR, denen Folge geleistet wurde, die durchschnittliche Zeitspanne zwischen dem Zeitpunkt der Ausstellung eines EPOC-PR und dem Zeitpunkt des entsprechenden Ersuchens um Herausgabe, aufgeschlüsselt nach der Art der angeforderten Daten und den Adressaten;

g) die Zahl der Europäischen Herstellungsanordnungen oder Europäischen Erhaltungsanordnungen, die einem Vollstreckungsstaat zwecks Vollstreckung übermittelt wurden und von diesem entgegengenommen wurden, aufgeschlüsselt nach der Art der angeforderten Daten, den Adressaten und der jeweiligen Situation (Notfall oder nicht) sowie die Zahl der jeweiligen Anordnungen, denen Folge geleistet wurde;

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

i) die Zahl der Fälle, in denen keine Ex-post-Validierung gemäß Artikel 4 Absatz 5 gewährt wurde;

j) eine Übersicht über die von Diensteanbietern im Zusammenhang mit der Ausführung von EPOC oder EPOC-PR geltend gemachten Kosten und die von den Anordnungsbehörden erstatteten Kosten.

(3) Ab dem 18. August 2026 können die in Absatz 2 des vorliegenden Artikels genannten Statistiken für den Datenaustausch über das dezentrale IT-System gemäß Artikel 19 Absatz 1 von nationalen Portalen programmatisch erhoben werden. Die in Artikel 22 genannte Referenzimplementierungssoftware muss technisch für diese Funktionalität ausgerüstet sein.

(4) Die Diensteanbieter können Statistiken im Einklang mit den bestehenden Datenschutzgrundsätzen erheben, vorhalten und veröffentlichen. Werden solche Statistiken für das vorangegangene Kalenderjahr erhoben, so können sie der Kommission bis zum 31. März übermittelt werden und können, soweit möglich, Folgendes umfassen:

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

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

c) im Falle von EPOC, denen Folge geleistet wurde, die durchschnittliche Zeitspanne, die für die Bereitstellung der angeforderten Daten vom Eingang von EPOC bis zur Bereitstellung benötigt wurde, aufgeschlüsselt nach der Art der angeforderten Daten, dem Anordnungsstaat und der jeweiligen Situation (Notfall oder nicht);

d) im Falle von EPOC-PR, denen Folge geleistet wurde, die durchschnittliche Zeitspanne zwischen dem Zeitpunkt der Ausstellung von EPOC-PR und dem Zeitpunkt, zu dem das anschließende Ersuchen um Herausgabe ausgestellt wurde, aufgeschlüsselt nach der Art der angeforderten Daten und dem Anordnungsstaat.

(5) Ab dem 18. August 2027 veröffentlicht die Kommission bis zum 30. Juni eines jeden Jahres einen Bericht, der die in den Absätzen 2 und 3 genannten Daten in zusammengefasster Form enthält, aufgeschlüsselt nach Mitgliedstaaten und Art des Diensteanbieters.

Artikel 29

Änderungen der Bescheinigungen und Formulare

Die Kommission erlässt gemäß Artikel 30 delegierte Rechtsakte zur Änderung der Anhänge I, II, III, V und VI, um einem etwaigen Verbesserungsbedarf hinsichtlich des Inhalts der EPOC- und der EPOC-PR-Formulare sowie der Formulare, die für die Übermittlung von Informationen über die Unmöglichkeit der Ausführung eines EPOC oder eines EPOC-PR, für die Bestätigung, dass ein Ersuchen um Herausgabe infolge einer Europäischen Sicherungsanordnung gestellt wurde, und für die Verlängerung der Sicherung elektronischer Beweismittel zu verwenden sind, wirksam zu entsprechen.

Artikel 30

Ausübung der Befugnisübertragung

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

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 29 wird der Kommission auf unbestimmte Zeit ab dem 18. August 2026 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 29 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 im Einklang mit den Grundsätzen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung niedergelegt wurden, die von den einzelnen Mitgliedstaaten benannten Sachverständigen.

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

Artikel 31

Mitteilung an die Kommission

(1) Jeder Mitgliedstaat teilt der Kommission bis spätestens 18. August 2025 Folgendes mit:

a) die Behörde bzw. die Behörden, die im Einklang mit dem nationalen Recht gemäß Artikel 4 befugt sind, Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen oder diesbezügliche Mitteilungen auszustellen, zu validieren oder zu übermitteln;

b) die Behörde bzw. die Behörden, die befugt sind, Mitteilungen gemäß Artikel 8 entgegenzunehmen und Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen im Namen eines anderen Mitgliedstaats gemäß Artikel 16 zu vollstrecken;

c) die Behörde bzw. die Behörden, die befugt sind, sich mit begründeten Einwänden von Adressaten gemäß Artikel 17 zu befassen;

d) die Sprachen, die für Mitteilungen über und Übermittlungen von EPOC, EPOC-PR, Europäischen Herausgabeanordnungen oder einer Europäischen Sicherungsanordnungen im Falle der Vollstreckung gemäß Artikel 27 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 für Strafsachen, auf die Artikel 9 des Beschlusses 2008/976/JI des Rates ([33]) Bezug nimmt, öffentlich zugänglich.

Artikel 32

Bezug zu anderen Instrumenten, Abkommen und Vereinbarungen

(1) Die vorliegende Verordnung lässt Unions- oder sonstige internationale Instrumente, Abkommen und Vereinbarungen über die Erhebung von in den Anwendungsbereich der vorliegenden Verordnung fallenden Beweismitteln unberührt.

(2) Die Mitgliedstaaten teilen der Kommission bis zum 18. August 2026 alle bestehenden Instrumente, Abkommen und Vereinbarungen im Sinne von Absatz 1, die sie weiterhin anwenden. Die Mitgliedstaaten unterrichten die Kommission ferner über alle neuen Abkommen oder Vereinbarungen im Sinne des Absatzes 1 binnen drei Monaten nach deren Unterzeichnung.

Artikel 33

Bewertung

Die Kommission nimmt bis zum 18. August 2029 eine Bewertung der vorliegenden Verordnung vor. Die Kommission übermittelt dem Europäischen Parlament, dem Rat, dem Europäischen Datenschutzbeauftragten und der Agentur der Europäischen Union für Grundrechte einen Bewertungsbericht. Dieser Bewertungsbericht enthält eine Bewertung der Anwendung der vorliegenden Verordnung und der im Hinblick auf ihre Ziele erzielten Ergebnisse sowie eine Bewertung der Auswirkungen der vorliegenden Verordnung auf die Grundrechte. Die Bewertung wird gemäß den Leitlinien der Kommission für bessere Rechtsetzung durchgeführt. Die Mitgliedstaaten übermitteln der Kommission die für die Ausarbeitung des Bewertungsberichts erforderlichen Informationen.

Artikel 34

Inkrafttreten und Anwendung

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

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

(2) Sie gilt ab dem 18. August 2026.

Die Verpflichtung der zuständigen Behörden und Diensteanbieter, das in Artikel 19 festgelegte dezentrale IT-System für die schriftliche Kommunikation im Rahmen dieser Verordnung zu nutzen, gilt jedoch ab einem Jahr nach dem Erlass der in Artikel 25 genannten Durchführungsrechtsakte.

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

Geschehen zu Straßburg am 12. Juli 2023.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
R. METSOLA	P. NAVARRO RÍOS

ANHANG I

BESCHEINIGUNG ÜBER EINE EUROPÄISCHE HERAUSGABEANORDNUNG (EPOC) ZUR HERAUSGABE ELEKTRONISCHER BEWEISMITTEL

Gemäß der Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates ([1]) muss der Adressat dieser Bescheinigung über eine Europäische Herausgabeanordnung (EPOC) dieses EPOC ausführen und der unter Abschnitt L Buchstabe a dieses EPOC genannten zuständigen Behörde die angeforderten Daten binnen der in Abschnitt C dieses EPOC genannten Frist(en) übermitteln.

In allen Fällen ist der Adressat nach Erhalt des EPOC verpflichtet, umgehend tätig zu werden, um die angeforderten Daten zu sichern, es sei denn, er kann diese Daten nicht anhand der Angaben im EPOC identifizieren. Die Daten müssen bis zur Herausgabe weiterhin gesichert werden, oder bis die Anordnungsbehörde oder gegebenenfalls die Vollstreckungsbehörde mitteilt, dass die Sicherung und Herausgabe der Daten nicht mehr erforderlich ist.

Der Adressat trifft die erforderlichen Maßnahmen, um die Vertraulichkeit, Geheimhaltung und Integrität des EPOC sowie der herausgegebenen oder gesicherten Daten sicherzustellen.

ABSCHNITT A: Anordnungsbehörde/Validierende Behörde

Anordnungsstaat: .....

Anordnungsbehörde: .....

(Ggf.) Validierende Behörde: .....

Hinweis: Nähere Informationen zur Anordnungsbehörde und zur validierenden Behörde sind am Ende anzugeben (Abschnitte I und J). .....

Aktenzeichen der Anordnungsbehörde: .....

Aktenzeichen der validierenden Behörde: .....

ABSCHNITT B: Adressat

Adressat: .....

☐ Benannte Niederlassung

☐ Vertreter

☐ Diese Anordnung ergeht in einem Notfall an den genannten Adressaten, weil die benannte Niederlassung oder der Vertreter eines Diensteanbieters nicht innerhalb der Fristen gemäß Artikel 10 der Verordnung (EU) 2023/1543 auf ein EPOC reagiert hat oder nicht innerhalb der Fristen gemäß der Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates ([2]) benannt oder bestellt worden ist.

Anschrift: .....

Tel./Fax/E-Mail (soweit bekannt): .....

Kontaktperson (soweit bekannt): .....

Aktenzeichen des Adressaten (soweit bekannt): .....

Betroffener Diensteanbieter (falls nicht identisch mit dem Adressaten): .....

Sonstige sachdienliche Angaben: .....

([1]) Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl. L 191 vom 28.7.2023, S. 118).

([2]) Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren (ABl. L 191 vom 28.7.2023, S. 181).

ABSCHNITT C: Fristen (Zutreffendes bitte ankreuzen und ggf. erläutern)

Nach Erhalt des EPOC sind die angeforderten Daten binnen folgender Fristen herauszugeben:

☐ so bald wie möglich und spätestens binnen zehn Tagen (ohne Mitteilung an die Vollstreckungsbehörde)

☐ bei einer Mitteilung an die Vollstreckungsbehörde: nach Ablauf der zehn Tage, wenn die Vollstreckungsbehörde innerhalb dieses Zeitraums keinen Ablehnungsgrund geltend gemacht hat, oder nach der Bestätigung der Vollstreckungsbehörde vor Ablauf der zehn Tage, dass sie keinen Ablehnungsgrund geltend machen wird, so bald wie möglich, spätestens jedoch nach Ablauf der zehn Tage

☐ unverzüglich, spätestens jedoch binnen acht Stunden in einem Notfall aufgrund:

☐ einer unmittelbaren Gefahr für das Leben, die körperliche Unversehrtheit oder die Sicherheit einer Person

☐ einer unmittelbaren Gefahr für eine kritische Infrastruktur im Sinne des Artikels 2 Buchstabe a der Richtlinie 2008/114/EG des Rates ([3]), wobei die Störung oder Zerstörung einer kritischen Infrastruktur zu einer unmittelbaren Gefahr für das Leben, die körperliche Unversehrtheit oder die Sicherheit einer Person führen würde, auch durch die schwere Beeinträchtigung der Bereitstellung der Grundversorgung für die Bevölkerung oder der Wahrnehmung der Kernfunktionen des Staates.

Bitte geben Sie an, ob es Verfahrens- oder sonstige Fristen gibt, die bei der Ausführung dieses EPOC zu berücksichtigen sind: ....

Machen Sie ggf. bitte zusätzliche Angaben: ....

ABSCHNITT D: Zusammenhang mit einem früheren Ersuchen um Herausgabe/Sicherung (bitte ankreuzen und ausfüllen, sofern zutreffend und verfügbar)

☐ Die angeforderten Daten wurden aufgrund eines früheren Ersuchens um Datensicherung folgender Behörde

....(bitte die Behörde und das Aktenzeichen angeben)

vom ..... (bitte das Datum des Ersuchens angeben) vollständig/teilweise gespeichert.

Diese Daten wurden am ..... (bitte das Datum der Übermittlung des Ersuchens angeben)

übermittelt an: ..... (bitte den Diensteanbieter/den Vertreter/die benannte Niederlassung/die zuständige Behörde, an den/die das Ersuchen übermittelt wurde, und – falls bekannt – das vom Adressaten angegebene Aktenzeichen angeben).

☐ Die angeforderten Daten beziehen sich auf ein früheres Ersuchen um Herausgabe folgender Behörde

....(bitte die Behörde und das Aktenzeichen angeben)

vom ....(bitte das Datum des Ersuchens angeben).

Diese Daten wurden am ..... (bitte das Datum der Übermittlung des Ersuchens angeben)

übermittelt an: ..... (bitte den Diensteanbieter/den Vertreter/die benannte Niederlassung/die zuständige Behörde, an den/die das Ersuchen übermittelt wurde, und – falls bekannt – das vom Adressaten angegebene Aktenzeichen angeben).

Sonstige sachdienliche Angaben: ....

([3]) 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).

ABSCHNITT E: Angaben zur Unterstützung der Identifizierung der angeforderten Daten (auszufüllen, soweit bekannt und zur Identifizierung der Daten erforderlich)

IP Adresse(en) und Zeitstempel (einschl. Datum und Zeitzone): ....

Tel.: ....

E-Mail-Adresse(en): ....

IMEI-Nummer(n): ....

MAC-Adresse(en): ....

Nutzer oder andere eindeutige Kennung(en) wie Nutzername(n), Login-ID(s) oder Kontobezeichnung(en): .....

Name(n) des bzw. der relevanten Dienste(s): ....

Sonstiges: ....

Erforderlichenfalls die Zeitspanne der Daten, für die deren Herausgabe angefordert wird:

....

☐ Zusätzliche Angaben, falls erforderlich: ....

ABSCHNITT F: Herauszugebende elektronische Beweismittel

Dieses EPOC betrifft (Zutreffendes bitte ankreuzen):

a) ☐ Teilnehmerdaten:

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

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

☐ Art und Dauer des Dienstes, einschließlich Identifikator(en), der/die von einem Teilnehmer zum Zeitpunkt der erstmaligen Registrierung/Anmeldung oder Aktivierung verwendet oder dem Teilnehmer zur Verfügung gestellt wird/werden (z. B. Telefonnummer, SIM-Kartennummer, MAC-Adresse) und zugehörige(s) Gerät/Geräte

☐ Angaben zum Profil (z. B. Nutzername, Screen name, Profilbild)

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

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

☐ PUK-Codes

☐ Sonstiges: .....

b) ☐ Ausschließlich zum Zweck der Identifizierung des Nutzers angeforderte Daten im Sinne des Artikels 3 Nummer 10 der Verordnung (EU) 2023/1543:

☐ IP-Verbindungsdaten wie IP-Adressen/IP-Protokolle/Zugangsnummern zusammen mit anderen technischen Identifikatoren wie Quellports und Zeitstempel oder Gleichwertiges, Nutzerkennung und im Zusammenhang mit der Nutzung des Dienstes verwendete Schnittstelle; bitte machen Sie erforderlichenfalls nähere Angaben: ....

☐ die Zeitspanne der Daten, für die deren Herausgabe angefordert wird (falls abweichend von Abschnitt E): ...

☐ Sonstiges: .....

c) ☐ Verkehrsdaten:

i) für (Mobil-)Telefonie:

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

☐ Verbindungszeit und -dauer

☐ Anrufversuche

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

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

☐ Sonstiges: .....

ii) für Internet:

☐ Routing-Informationen (Quell-IP-Adresse, Ziel-IP-Adresse(n), Port-Nummer(n), Browser, E-Mail-Header-Informationen, Message-ID)

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

☐ Datenvolumen

☐ Datum und Uhrzeit der Verbindung

☐ Dauer der Verbindung oder der Zugangssitzung(en)

☐ Sonstiges: .....

iii) für Hosting:

☐ Protokolldateien

☐ Tickets

☐ Sonstiges: .....

iv) Sonstiges:

☐ Kaufhistorie

☐ Historie über Prepaid-Aufladevorgänge

☐ Sonstiges: .....

d) ☐ Inhaltsdaten:

☐ (Web-)Mailbox-Dump

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

☐ Page-Dump

☐ Message log/Backup

☐ Voicemail-Dump

☐ Server-Inhalte

☐ Geräte-Backup

☐ Kontaktliste

☐ Sonstiges: .....

☐ Zusätzliche Angaben, falls erforderlich, um den Umfang der angeforderten Daten näher zu präzisieren oder zu begrenzen: .....

ABSCHNITT G: Angaben zu den zugrunde liegenden Bedingungen

a) Dieses EPOC betrifft (Zutreffendes bitte ankreuzen):

☐ (ein) Strafverfahren aufgrund einer/mehrerer Straftat(en)

☐ die Vollstreckung einer mindestens viermonatigen Freiheitsstrafe oder freiheitsentziehenden Maßregel der Sicherung im Anschluss an ein Strafverfahren, sofern diese in dem Fall, dass sich der Verurteilte der Justiz entzogen hat, nicht in Abwesenheit ergangen ist

b) Art und rechtliche Würdigung der Straftat(en), die dem EPOC zugrunde liegen, und anwendbare Rechtsnorm ([4]):

....

c) Dieses EPOC betrifft Verkehrsdaten, die nicht ausschließlich zum Zweck der Identifizierung des Nutzers angefordert werden, und/oder Inhaltsdaten im Zusammenhang mit (sofern zutreffend, bitte ankreuzen):

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

([4]) Zur Vollstreckung einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung für Verkehrsdaten, die nicht ausschließlich zum Zweck der Identifizierung des Nutzers erforderlich sind, oder für Inhaltsdaten unter Buchstaben b und c bitte die Straftat angeben, für die die Verurteilung erfolgt ist.

☐ einer oder mehreren der folgenden Straftaten, wenn diese ganz oder teilweise mittels eines Informationssystems begangen wurden:

☐ Straftat(en) im Sinne der Artikel 3 bis 8 der Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates ([5])

☐ Straftat(en) im Sinne der Artikel 3 bis 7 der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates ([6])

☐ Straftat(en) im Sinne der Artikel 3 bis 8 der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates ([7])

☐ Straftaten im Sinne der Artikel 3 bis 12 und 14 der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates ([8]).

d) Verantwortlicher/Auftragsverarbeiter:

Europäische Herausgabeanordnungen sind an Diensteanbieter zu richten, die als Verantwortliche fungieren. In Ausnahmefällen kann die Europäische Herausgabeanordnung unmittelbar an den Diensteanbieter gerichtet werden, der die Daten im Auftrag des Verantwortlichen verarbeitet.

Zutreffendes bitte ankreuzen:

☐ Dieses EPOC ist an den Diensteanbieter gerichtet, der als Verantwortlicher fungiert.

☐ Dieses EPOC ist an den Diensteanbieter gerichtet, der die Daten im Auftrag des Verantwortlichen verarbeitet oder – in Fällen, in denen der Verantwortliche nicht ermittelt werden kann – möglicherweise verarbeitet, weil

☐ der Verantwortliche trotz angemessener Bemühungen der Anordnungsbehörde nicht ermittelt werden kann

☐ es den Ermittlungen abträglich sein könnte, wenn es an den Verantwortlichen gerichtet würde

Wenn dieses EPOC an den Diensteanbieter gerichtet ist, der im Auftrag des Verantwortlichen die Daten verarbeitet,

☐ unterrichtet der Auftragsverarbeiter den Verantwortlichen über die Herausgabe der Daten

☐ unterrichtet der Auftragsverarbeiter den Verantwortlichen bis auf Weiteres nicht über die Herausgabe der Daten, da dies den Ermittlungen abträglich wäre. Bitte geben Sie eine kurze Begründung an ([9]): .....

e) Sonstige sachdienliche Angaben: ....

ABSCHNITT H: Informationen für den Nutzer

Der Adressat darf die Person, deren Daten angefordert werden, hiervon auf keinen Fall in Kenntnis setzen. Es obliegt der Anordnungsbehörde, diese Person unverzüglich über die Herausgabe der Daten zu unterrichten.

([5]) Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates (ABl. L 123 vom 10.5.2019, S. 18).

([6]) 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).

([7]) 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).

([8]) 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).

([9]) Die Anordnungsbehörde muss die Gründe für die Aufschiebung in der Verfahrensakte angeben, im EPOC braucht nur eine kurze Begründung angefügt zu werden.

Bitte beachten Sie, dass (Zutreffendes bitte ankreuzen):

☐ die Anordnungsbehörde die Information der Person, deren Daten angefordert werden, so lange aufschieben wird, bis eine oder mehrere der folgenden Bedingungen erfüllt sind:

☐ sie ist erforderlich, um zu gewährleisten, dass behördliche oder gerichtliche Ermittlungen, Untersuchungen oder Verfahren nicht behindert werden;

☐ sie ist erforderlich, um zu gewährleisten, dass die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden;

☐ sie ist zum Schutz der öffentlichen Sicherheit erforderlich;

☐ sie ist zum Schutz der nationalen Sicherheit erforderlich;

☐ sie ist zum Schutz der Rechte und Freiheiten anderer erforderlich.

ABSCHNITT I: Angaben zur Anordnungsbehörde

Art der Anordnungsbehörde (Zutreffendes bitte ankreuzen):

☐ Richter, Gericht oder Ermittlungsrichter

☐ Staatsanwalt

☐ andere vom Anordnungsstaat bezeichnete zuständige Behörde

Falls eine Validierung erforderlich ist, bitte auch Abschnitt J ausfüllen.

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

☐ Dieses EPOC wurde für Teilnehmerdaten und/oder für Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers angefordert werden, in einem hinreichend begründeten Notfall ohne vorherige Validierung erlassen, da eine Validierung nicht rechtzeitig hätte eingeholt werden können. Die Anordnungsbehörde bestätigt, dass sie in einem vergleichbaren nationalen Fall eine Anordnung ohne Validierung erlassen könnte und dass sie sich unverzüglich, spätestens innerhalb von 48 Stunden, um eine Ex-post-Validierung bemühen wird (bitte beachten Sie, dass der Adressat nicht informiert wird).

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

Bezeichnung der Behörde: ....

Name ihres Vertreters: ....

Funktion (Titel/Amtsbezeichnung): ....

Aktenzeichen: ....

Anschrift: ....

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

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

E-Mail: ....

Sprache(n): ....

Falls abweichend von oben, Behörde/Ansprechpartner (z. B. zentrale Behörde) für Rückfragen im Zusammenhang mit der Ausführung des EPOC:

Bezeichnung der Behörde/Name: ....

Anschrift: ....

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

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

E-Mail: ....

Unterschrift der Anordnungsbehörde oder ihres Vertreters zur Bestätigung der inhaltlichen Richtigkeit des EPOC:

Datum: ....

Unterschrift ([10]): ....

ABSCHNITT J: Angaben zur validierenden Behörde (auszufüllen, sofern zutreffend)

Art der validierenden Behörde

☐ Richter, Gericht oder Ermittlungsrichter

☐ Staatsanwalt

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

Bezeichnung der Behörde: ....

Name ihres Vertreters: ....

Funktion (Titel/Amtsbezeichnung): ....

Aktenzeichen: ....

Anschrift: ....

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

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

E-Mail: ....

Sprache(n): ....

([10]) Wird das dezentrale IT-System nicht genutzt, fügen Sie bitte auch einen amtlichen Stempel, ein elektronisches Siegel oder eine gleichwertige Authentifizierung bei.

Datum: ....

Unterschrift ([11]): ....

ABSCHNITT K: Unterrichtung und Angaben zur unterrichteten Vollstreckungsbehörde (falls zutreffend)

☐ Die folgende Vollstreckungsbehörde wird von diesem EPOC unterrichtet:
....

Bitte geben Sie für die unterrichtete Vollstreckungsbehörde Kontaktdaten an (falls vorhanden):

Bezeichnung der Vollstreckungsbehörde: ....

Anschrift: ....

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

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

E-Mail: ....

ABSCHNITT L: Übermittlung von Daten

a) Behörde, an die die Daten zu übermitteln sind

☐ Anordnungsbehörde

☐ validierende Behörde

☐ andere zuständige Behörde (z. B. zentrale Behörde)

Bezeichnung und Kontaktangaben: ....

b) Bevorzugtes Format, in dem oder mit dem die Daten übermittelt werden müssen (falls zutreffend): .....

ABSCHNITT M: Weitere Angaben, die aufzunehmen sind (nicht an den Adressaten senden – Übermittlung an die Vollstreckungsbehörde, falls eine Mitteilung an die Vollstreckungsbehörde erforderlich ist)

Die Gründe für die Feststellung, dass die Europäische Herausgabeanordnung die Voraussetzungen der Notwendigkeit und Verhältnismäßigkeit erfüllt:

....

Zusammenfassende Beschreibung des Falls:

....

([11]) Wird das dezentrale IT-System nicht genutzt, fügen Sie bitte auch einen amtlichen Stempel, ein elektronisches Siegel oder eine gleichwertige Authentifizierung bei.

Ist die Straftat, aufgrund deren die Europäische Herausgabeanordnung erlassen wird, im Anordnungsstaat mit einer Freiheitsstrafe oder freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht und in der nachstehenden Auflistung von Straftaten enthalten? (Zutreffendes bitte ankreuzen)

☐ Beteiligung an einer kriminellen Vereinigung

☐ Terrorismus

☐ Menschenhandel

☐ sexuelle Ausbeutung von Kindern und Kinderpornografie

☐ illegaler Handel mit Drogen und psychotropen Stoffen

☐ illegaler Handel mit Waffen, Munition und Sprengstoffen

☐ Bestechung

☐ Betrugsdelikte, einschließlich Betrug und anderer Straftaten zum Nachteil der finanziellen Interessen der Union im Sinne der Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates ([12])

☐ Wäsche von Erträgen aus Straftaten

☐ Geldfälschung einschließlich Euro-Fälschung

☐ Cyberkriminalität

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

☐ Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt

☐ vorsätzliche Tötung oder schwere Körperverletzung

☐ illegaler Handel mit menschlichen Organen und menschlichem Gewebe

☐ Entführung, Freiheitsberaubung oder Geiselnahme

☐ Rassismus und Fremdenfeindlichkeit

☐ Diebstahl in organisierter Form oder mit Waffen

☐ illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenständen

☐ Betrug

☐ Erpressung und Schutzgelderpressung

☐ Produktfälschung und Produktpiraterie

☐ Fälschung von amtlichen Dokumenten und Handel damit

☐ Fälschung von Zahlungsmitteln

☐ illegaler Handel mit Hormonen und anderen Wachstumsförderern

([12]) Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates vom 5. Juli 2017 über die strafrechtliche Bekämpfung von gegen die finanziellen Interessen der Union gerichtetem Betrug (ABl. L 198 vom 28.7.2017, S. 29).

☐ illegaler Handel mit nuklearen und radioaktiven Substanzen

☐ Handel mit gestohlenen Kraftfahrzeugen

☐ Vergewaltigung

☐ vorsätzliche Brandstiftung

☐ Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen

☐ Flugzeug- und Schiffsentführung

☐ Sabotage

Bitte machen Sie gegebenenfalls weitere Angaben, die die Vollstreckungsbehörde möglicherweise benötigt, um zu beurteilen, ob Ablehnungsgründe geltend gemacht werden können:

… ....

ANHANG II

BESCHEINIGUNG ÜBER EINE EUROPÄISCHE SICHERUNGSANORDNUNG (EPOC-PR) ZUR SICHERUNG ELEKTRONISCHER BEWEISMITTEL

Gemäß der Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates [1] muss der Empfänger der Bescheinigung über eine Europäische Sicherungsanordnung (EPOC-PR) unverzüglich nach Erhalt des EPOC-PR die angeforderten Daten sichern. Die Sicherung muss nach 60 Tagen enden, es sei denn, die Anordnungsbehörde verlängert sie um weitere 30 Tage oder die Anordnungsbehörde bestätigt, dass ein entsprechendes Ersuchen um Herausgabe gestellt wurde. Wenn die Anordnungsbehörde innerhalb dieser Zeiträume bestätigt, dass ein entsprechendes Ersuchen um Herausgabe gestellt wurde, muss der Empfänger die Daten so lange sichern, wie dies erforderlich ist, um die Daten nach Eingang des entsprechenden Ersuchens um Herausgabe herauszugeben.

Der Empfänger trifft die erforderlichen Maßnahmen, um die Vertraulichkeit, Geheimhaltung und Integrität des EPOC-PR sowie der gesicherten Daten sicherzustellen.

ABSCHNITT A: Anordnungsbehörde/Validierende Behörde:

Anordnungsstaat:.....

Anordnungsbehörde: .....

(Ggf.) Validierende Behörde:.....

Hinweis: Nähere Informationen zur Anordnungsbehörde und zur validierenden Behörde sind am Ende anzugeben (Abschnitte F und G)

Aktenzeichen der Anordnungsbehörde: .....

Aktenzeichen der validierenden Behörde:.....

ABSCHNITT B: Adressat

Adressat: .....

☐ Benannte Niederlassung

☐ Vertreter

☐ Diese Anordnung ergeht in einem Notfall an den genannten Adressaten, weil die benannte Niederlassung oder der Vertreter eines Diensteanbieters nicht innerhalb der Fristen auf ein EPOC-PR reagiert hat oder nicht innerhalb der Fristen gemäß der Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates [2] benannt oder bestellt worden ist.

[1] Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl. L 191 vom 28.7.2023, S. 118).

[2] Verordnung (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl. L 191 vom 28.7.2023, S. 181).

Anschrift: .....

Tel./Fax/E-Mail (soweit bekannt): .....

Kontaktperson (soweit bekannt): .....

Aktenzeichen des Adressaten (soweit bekannt): .....

Betroffener Diensteanbieter (falls nicht identisch mit dem Adressaten): .....

Sonstige sachdienliche Angaben: .....

ABSCHNITT C: Angaben zur Unterstützung der Identifizierung der Daten, deren Sicherung angefordert wird (auszufüllen, soweit bekannt und zur Identifizierung der Daten erforderlich)

☐ IP-Adresse(n) und Zeitstempel (einschl. Datum und Zeitzone): .....

☐ Tel. Nr.: .....

☐ E-Mail-Adresse(en): .....

☐ IMEI-Nummer(n): .....

☐ MAC-Adresse(n): .....

☐ Nutzer des Dienstes oder andere eindeutige Kennung(en) wie Nutzername(n), Login-ID(s) oder Kontobezeichnung(en) .....

☐ Name(n) des bzw. der relevanten Dienste(s): .....

☐ Sonstiges: .....

Erforderlichenfalls die Zeitspanne der Daten, für die deren Sicherung angefordert wird: .....

☐ Zusätzliche Angaben, falls erforderlich: ..... .

ABSCHNITT D: Zu sichernde elektronische Beweismittel

Dieses EPOC-PR betrifft (Zutreffendes bitte ankreuzen):

a) ☐ Teilnehmerdaten:

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

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

☐ Art und Dauer des Dienstes, einschließlich Identifikator(en), der/die von einem Teilnehmer zum Zeitpunkt der erstmaligen Registrierung/Anmeldung oder Aktivierung verwendet oder dem Teilnehmer zur Verfügung gestellt wird/werden (z. B. Telefonnummer, SIM-Kartennummer, MAC-Adresse) und zugehörige(s) Gerät/Geräte

☐ Angaben zum Profil (z. B. Nutzername, Screen name, Profilbild)

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

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

☐ PUK-Codes

☐ Sonstiges:..... .....

b) ☐ Ausschließlich zum Zweck der Identifizierung des Nutzers angeforderte Daten im Sinne des Artikels 3 Nummer 10 der Verordnung (EU) 2023/1543:

☐ IP-Verbindungsdaten wie IP-Adressen/IP-Protokolle/Zugangsnummern zusammen mit anderen Identifikatoren wie Quellports und Zeitstempel oder Gleichwertiges, Nutzerkennung und im Zusammenhang mit der Nutzung des Dienstes verwendete Schnittstelle, die zu Identifizierungszwecken unbedingt erforderlich sind; bitte machen Sie erforderlichenfalls nähere Angaben:..... .....

☐ die Zeitspanne der Daten, für die deren Sicherung angefordert wird (falls abweichend von Abschnitt C):...

☐ Sonstiges:..... .....

c) ☐ Verkehrsdaten:

i) für (Mobil-)Telefonie:

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

☐ Verbindungszeit und -dauer

☐ Anrufversuche

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

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

☐ Sonstiges:..... .....

ii) für Internet:

☐ Routing-Informationen (Quell-IP-Adresse, Ziel-IP-Adresse(n), Port-Nummer(n), Browser, E-Mail-Header-Informationen, Message-ID)

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

☐ Datenvolumen

☐ Datum und Uhrzeit der Verbindung

☐ Dauer der Verbindung oder der Zugangssitzung(en)

☐ Sonstiges:..... .....

iii) für Hosting:

☐ Protokolldateien

☐ Tickets

☐ Sonstiges:..... .....

iv) Sonstiges:

☐ Kaufhistorie

☐ Historie über Prepaid-Aufladevorgänge

☐ Sonstiges:..... .....

d) ☐ Inhaltsdaten:

☐ (Web-)Mailbox-Dump

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

☐ Page-Dump

☐ Message log/Backup

☐ Voicemail-Dump

☐ Server-Inhalte

☐ Geräte-Backup

☐ Kontaktliste

☐ Sonstiges:..... .....

☐ Zusätzliche Angaben, falls erforderlich, um den Umfang der angeforderten Daten näher zu präzisieren oder zu begrenzen:..... .....

ABSCHNITT E: Angaben zu den zugrunde liegenden Bedingungen

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

☐ (ein) Strafverfahren aufgrund einer Straftat

☐ die Vollstreckung einer mindestens viermonatigen Freiheitsstrafe oder freiheitsentziehenden Maßregel der Sicherung im Anschluss an ein Strafverfahren, sofern diese in dem Fall, dass sich der Verurteilte der Justiz entzogen hat, nicht in Abwesenheit ergangen ist

b) Art und rechtliche Würdigung der Straftat(en), die dem EPOC-PR zugrunde liegen, und anwendbare Rechtsnorm ([3]).....

ABSCHNITT F: Angaben zur Anordnungsbehörde

Art der Anordnungsbehörde (Zutreffendes bitte ankreuzen):

☐ Richter, Gericht oder Ermittlungsrichter

☐ Staatsanwalt

☐ andere nach dem Recht des Anordnungsstaats zuständige Behörde

Falls eine Validierung erforderlich ist, bitte auch Abschnitt G ausfüllen.

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

☐ Dieses EPOC-PR wurde für Teilnehmerdaten und/oder für Daten, die ausschließlich zum Zweck der Identifizierung des Nutzers angefordert werden, in einem hinreichend begründeten Notfall ohne vorherige Validierung erlassen, da eine Validierung nicht rechtzeitig hätte eingeholt werden können. Die Anordnungsbehörde bestätigt, dass sie in einem vergleichbaren nationalen Fall eine Anordnung ohne Validierung erlassen könnte und dass sie sich unverzüglich, spätestens innerhalb von 48 Stunden, um eine Ex-post-Validierung bemühen wird (bitte beachten Sie, dass der Adressat nicht informiert wird).

Dieser Notfall bezieht sich auf eine unmittelbare Gefahr für das Leben, die körperliche Unversehrtheit oder die Sicherheit einer Person oder für eine kritische Infrastruktur im Sinne des Artikels 2 Buchstabe a der Richtlinie 2008/114/EG des Rates ([4]), wobei die Störung oder Zerstörung einer kritischen Infrastruktur zu einer unmittelbaren Gefahr für das Leben, die körperliche Unversehrtheit oder die Sicherheit einer Person führen würde, auch durch die schwere Beeinträchtigung der Bereitstellung der Grundversorgung für die Bevölkerung oder der Wahrnehmung der Kernfunktionen des Staates.

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

Bezeichnung der Behörde: .....

Name ihres Vertreters: .....

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

([3]) Zur Vollstreckung einer Freiheitsstrafe oder freiheitsentziehenden Maßregel der Sicherung, bitte die Straftat angeben, für die die Verurteilung erfolgt ist.

([4]) 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).

Aktenzeichen:.....

Anschrift:.....

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

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

E-Mail:.....

Sprache(n):.....

Falls abweichend von oben, Behörde/Ansprechpartner (z. B. zentrale Behörde) für Rückfragen im Zusammenhang mit der Ausführung des EPOC-PR:

Bezeichnung der Behörde/Name:.....

Anschrift:.....

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

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

E-Mail:.....

Unterschrift der Anordnungsbehörde oder ihres Vertreters zur Bestätigung der inhaltlichen Richtigkeit des EPOC-PR:

Datum:.....

Unterschrift ([5]):.....

ABSCHNITT G: Angaben zur validierenden Behörde (auszufüllen, sofern zutreffend)

Art der validierenden Behörde:

☐ Richter, Gericht oder Ermittlungsrichter

☐ Staatsanwalt

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

Bezeichnung der Behörde:.....

Name ihres Vertreters:.....

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

([5]) Wird das dezentrale IT-System nicht genutzt, fügen Sie bitte auch einen amtlichen Stempel, ein elektronisches Siegel oder eine gleichwertige Authentifizierung bei.

Aktenzeichen: .....

Anschrift: .....

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

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

E-Mail: .....

Sprache(n): .....

Datum: .....

Unterschrift ([6]): .....

([6]) Wird das dezentrale IT-System nicht genutzt, fügen Sie bitte auch einen amtlichen Stempel, ein elektronisches Siegel oder eine gleichwertige Authentifizierung bei.

ANHANG III

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

Falls der Adressat seiner Verpflichtung zur Sicherung der angeforderten Daten im Rahmen eines EPOC-PR oder zur Herausgabe im Rahmen eines EPOC nicht nachkommen kann, die genannte Frist nicht einhalten kann oder die Daten nicht vollständig übermittelt, sollte gemäß der Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates [1] dieses Formular von ihm ausgefüllt und unverzüglich an die Anordnungsbehörde und, falls eine Mitteilung ergangen ist sowie gegebenenfalls in anderen Fällen, an die im EPOC genannte Vollstreckungsbehörde zurückgesandt werden.

Sofern möglich sichert der Adressat die angeforderten Daten selbst dann, wenn noch zusätzliche Angaben erforderlich sind, um sie genau zu identifizieren, es sei denn die Angaben in dem EPOC/EPOC-PR sind zu diesem Zweck nicht ausreichend. Sind Klarstellungen seitens der Anordnungsbehörde erforderlich, so fordert der Adressat diese umgehend mit diesem Formular an.

ABSCHNITT A: Betreffende Bescheinigung

Die nachfolgenden Informationen betreffen:

☐ eine Bescheinigung über eine Europäische Herausgabeanordnung (EPOC)

☐ eine Bescheinigung über eine Europäische Sicherungsanordnung (EPOC-PR)

ABSCHNITT B: Zuständige Behörde(n)

Anordnungsbehörde: .....

Aktenzeichen der Anordnungsbehörde: .....

Gegebenenfalls die validierende Behörde: .....

Gegebenenfalls Aktenzeichen der validierenden Behörde: .....

Datum der Ausstellung des EPOC/EPOC-PR: .....

Datum der Entgegennahme des EPOC/EPOC-PR: .....

Gegebenenfalls die Vollstreckungsbehörde: .....

Gegebenenfalls Aktenzeichen der Vollstreckungsbehörde: .....

ABSCHNITT C: Adressat des EPOC/EPOC-PR

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

Aktenzeichen des Adressaten: .....

[1] Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl. L 191 vom 28.7.2023, S. 118).

ABSCHNITT D: Gründe für die Unmöglichkeit der Ausführung

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

☐ Es ist unvollständig.

☐ Es enthält offensichtliche Fehler.

☐ Es enthält keine ausreichenden Angaben.

☐ Es betrifft keine Daten, die zum Zeitpunkt der Entgegennahme des EPOC/EPOC-PR von einem Diensteanbieter oder in dessen Auftrag gespeichert wurden.

☐ Andere Gründe für eine faktische Unmöglichkeit aufgrund von Umständen, die nicht dem Adressaten oder dem Diensteanbieter angelastet werden können, zum Zeitpunkt der Entgegennahme des EPOC/EPOC-PR.

☐ Die Europäische Herausgabeanordnung/Europäische Sicherungsanordnung wurde nicht von einer Anordnungsbehörde nach Artikel 4 der Verordnung (EU) 2023/1543 erlassen oder validiert.

☐ die Europäische Herausgabeanordnung zur Erlangung von Verkehrsdaten, die nicht ausschließlich zum Zwecke der Identifizierung des Nutzers im Sinne von Artikel 3 Nummer 10 der Verordnung (EU) 2023/1543 oder zur Erlangung von Inhaltsdaten angefordert werden, wurde für eine Straftat erlassen, die nicht unter Artikel 5 Absatz 4 der Verordnung (EU) 2023/1543 fällt.

☐ die Dienstleistung fällt nicht unter die Verordnung (EU) 2023/1543.

☐ die angeforderten Daten sind durch Immunitäten oder Vorrechte geschützt, die nach dem Recht des Vollstreckungsstaats gewährt werden, oder die angeforderten Daten unterliegen Vorschriften über die Bestimmung oder Beschränkung der strafrechtlichen Verantwortlichkeit, die sich auf die Pressefreiheit oder die freie Meinungsäußerung in anderen Medien beziehen und die Vollstreckung der Europäischen Herausgabeanordnung/Europäischen Sicherungsanordnung verhindern.

☐ die Befolgung der Europäischen Herausgabeanordnung würde im Widerspruch zum anwendbaren Recht eines Drittlands stehen. Bitte auch Abschnitt E ausfüllen.

b) Bitte erläutern Sie, weshalb eine Ausführung nach Buchstabe a nicht möglich war, und nennen und erläutern Sie erforderlichenfalls alle weiteren Gründe, die nicht unter Buchstabe a aufgeführt sind:

… ....

ABSCHNITT E: Einander widersprechende Verpflichtungen, die sich aus dem Recht eines Drittlands ergeben

Im Falle einander widersprechender Verpflichtungen, die sich aus dem Recht eines Drittlands ergeben, bitte Folgendes angeben:

— Bezeichnung der Rechtsvorschrift(en) des Drittlands:

… ....

— anwendbare Gesetzesnorm(en) und Wortlaut der einschlägigen Bestimmung(en):

… ....

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

☐ Grundrechte natürlicher Personen (bitte angeben):

… ....

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

… ....

☐ andere Interessen (bitte angeben):

… ....

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

… ....

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

… ....

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

… ....

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

… ....

Bitte stellen Sie alle weiteren einschlägigen Informationen zur Verfügung: .....

ABSCHNITT F: Ersuchen um weitere Informationen/Klarstellungen (ggf. ausfüllen)

Zur Ausführung des EPOC/EPOC-PR bedarf es weiterer Informationen seitens der Anordnungsbehörde:

… ....

SECTION G: ABSCHNITT G: Datensicherung

Die angeforderten Daten (bitte Zutreffendes ankreuzen und ergänzen):

☐ werden gesichert, bis Daten herausgegeben werden oder bis die Anordnungsbehörde oder gegebenenfalls die Vollstreckungsbehörde mitteilt, dass die Sicherung und Herausgabe von Daten nicht mehr erforderlich ist, oder bis von der Anordnungsbehörde die erforderlichen Informationen geliefert werden, sodass die zu sichernden/herauszugebenden Daten präzisiert werden können

☐ wurden nicht gesichert (dies sollte nur ausnahmsweise der Fall sein, z. B. wenn der Diensteanbieter bei Eingang des Ersuchens nicht über die Daten verfügt oder die angeforderten Daten nicht hinreichend identifizieren kann)

ABSCHNITT H: Kontaktdaten der benannten Niederlassung/des Vertreters des Diensteanbieters

Name der benannten Niederlassung/des Vertreters des Diensteanbieters:
.....

Name der Kontaktperson: ....

Funktion: .....

Anschrift: .....

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

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

E-Mail: .....

Name der bevollmächtigten Person: .....

Datum: ....

Unterschrift ([2]): .....

([2]) Wird das dezentrale IT-System nicht genutzt, fügen Sie bitte auch einen amtlichen Stempel, ein elektronisches Siegel oder eine gleichwertige Authentifizierung bei.

ANHANG IV

KATEGORIEN VON STRAFTATEN GEMÄß ARTIKEL 12 ABSATZ 1 BUCHSTABE D

(1) Beteiligung an einer kriminellen Vereinigung;

(2) Terrorismus;

(3) Menschenhandel;

(4) sexuelle Ausbeutung von Kindern und Kinderpornografie;

(5) illegaler Handel mit Drogen und psychotropen Stoffen;

(6) illegaler Handel mit Waffen, Munition und Sprengstoffen;

(7) Bestechung;

(8) Betrugsdelikte, einschließlich Betrug und anderer Straftaten zum Nachteil der finanziellen Interessen der Union im Sinne der Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates ([1]);

(9) Wäsche von Erträgen aus Straftaten;

(10) Geldfälschung einschließlich Euro-Fälschung;

(11) Cyberkriminalität;

(12) Umweltkriminalität, einschließlich des illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten;

(13) Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt;

(14) vorsätzliche Tötung oder schwere Körperverletzung;

(15) illegaler Handel mit menschlichen Organen und menschlichem Gewebe;

(16) Entführung, Freiheitsberaubung oder Geiselnahme;

(17) Rassismus und Fremdenfeindlichkeit;

(18) Diebstahl in organisierter Form oder mit Waffen;

(19) illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenständen;

(20) Betrug;

(21) Erpressung und Schutzgelderpressung;

(22) Nachahmung und Produktpiraterie;

([1]) Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates vom 5. Juli 2017 über die strafrechtliche Bekämpfung von gegen die finanziellen Interessen der Union gerichtetem Betrug (ABl. L 198 vom 28.7.2017, S. 29).

(23) Fälschung von amtlichen Dokumenten und Handel damit;

(24) Fälschung von Zahlungsmitteln;

(25) illegaler Handel mit Hormonen und anderen Wachstumsförderern;

(26) illegaler Handel mit nuklearen und radioaktiven Substanzen;

(27) Handel mit gestohlenen Kraftfahrzeugen;

(28) Vergewaltigung;

(29) Brandstiftung;

(30) Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen;

(31) Flugzeug- und Schiffsentführung;

(32) Sabotage.

ANHANG V

BESTÄTIGUNG DER AUSSTELLUNG EINES ERSUCHENS UM HERAUSGABE IM ANSCHLUSS AN EINE EUROPÄISCHE SICHERUNGSANORDNUNG

Gemäß der Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates [1] muss der Adressat nach Entgegennahme der Bescheinigung über eine Europäische Sicherungsanordnung (EPOC-PR) die angeforderten Daten unverzüglich sichern. Die Sicherung muss nach 60 Tagen enden, es sei denn, die Anordnungsbehörde verlängert sie um weitere 30 Tage oder die Anordnungsbehörde bestätigt, dass ein entsprechendes Ersuchen um Herausgabe unter Verwendung des Formulars in diesem Anhang ausgestellt wurde.

Nach dieser Bestätigung muss der Adressat die Daten so lange sichern, wie dies erforderlich ist, um die Daten nach Entgegennahme des entsprechenden Ersuchens um Herausgabe herauszugeben.

ABSCHNITT A: Anordnungsbehörde für das EPOC-PR

Anordnungsstaat:..... .....

Anordnungsbehörde: ....

Falls abweichend von der im EPOC-PR angegebenen Kontaktstelle, Behörde/Ansprechpartner (z. B. zentrale Behörde) für Rückfragen im Zusammenhang mit der Ausführung:

Name und Kontaktangaben:..... .....

ABSCHNITT B: Adressat des EPOC-PR

Adressat:..... .....

Anschrift:..... .....

Telefon/Fax/E-Mail (soweit bekannt): ....

Kontaktperson (soweit bekannt): ....

Aktenzeichen des Adressaten (soweit bekannt):..... .....

Betroffener Diensteanbieter (falls nicht identisch mit dem Adressaten):.....

Sonstige sachdienliche Angaben: ....

[1] Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl. L 191 vom 28.7.2023, S. 118).

ABSCHNITT C: Informationen über das EPOC-PR

Die Daten werden in Übereinstimmung mit dem EPOC-PR vom ..... (Bitte das Datum der Ausstellung des Ersuchens angeben) gesichert und am ..... (Bitte das Datum der Übermittlung des Ersuchens angeben) mit dem Aktenzeichen ..... (Bitte das Aktenzeichen angeben) übermittelt.

☐ Sie wurde von der Anordnungsbehörde …, Aktenzeichen …, am … um 30 Tage verlängert. (Sofern zutreffend, bitte das Kästchen ankreuzen und ausfüllen.)

ABSCHNITT D: Bestätigung

Damit wird bestätigt, dass folgendes Ersuchen um Herausgabe gestellt wurde (Zutreffendes ankreuzen und ggf. ausfüllen):

☐ Bescheinigung über eine Europäische Herausgabeanordnung ausgestellt von..... (Bitte die Behörde angeben) am ..... (Bitte das Datum der Ausstellung des Ersuchens angeben) und übermittelt am ..... (Bitte das Datum der Übermittlung des Ersuchens angeben) mit dem Aktenzeichen..... (Bitte das Aktenzeichen angeben) an .... (Bitte den Diensteanbieter/die benannte Niederlassung/den Vertreter/die zuständige Behörde, an die es übermittelt wurde, und – falls bekannt – das vom Adressaten angegebene Aktenzeichen angeben).

☐ Europäische Ermittlungsanordnung ausgestellt von..... (Bitte die Behörde angeben) am..... (Bitte das Datum der Ausstellung des Ersuchens angeben) und übermittelt am ..... (Bitte das Datum der der Übermittlung des Ersuchens angeben) mit dem Aktenzeichen.... (Bitte das Aktenzeichen angeben) an..... (Bitte den Staat und die zuständige Behörde, an die es übermittelt wurde, und – falls bekannt – das von den ersuchten Behörden angegebene Aktenzeichen angeben).

☐ Rechtshilfeersuchen ausgestellt von ..... (Bitte die Behörde angeben) am ..... (Bitte das Datum der Ausstellung des Ersuchens angeben) und übermittelt am ..... (Bitte das Datum der Übermittlung des Ersuchens angeben) mit dem Aktenzeichen ..... (Bitte das Aktenzeichen angeben) an..... (Bitte den Staat und die zuständige Behörde, an die es übermittelt wurde, und – falls bekannt – das von den ersuchten Behörden angegebene Aktenzeichen angeben).

Unterschrift der Anordnungsbehörde und/oder ihres Vertreters:

Name:.....

Datum:.....

Unterschrift ([2]):.....

([2]) Wird das dezentrale IT-System nicht genutzt, fügen Sie bitte auch einen amtlichen Stempel, ein elektronisches Siegel oder eine gleichwertige Authentifizierung bei.

ANHANG VI

VERLÄNGERUNG DER SICHERUNG ELEKTRONISCHER BEWEISMITTEL

Gemäß der Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates [1] muss der Adressat nach Entgegennahme der Bescheinigung über eine Europäische Sicherungsanordnung (EPOC-PR) die angeforderten Daten unverzüglich sichern. Die Sicherung muss nach 60 Tagen enden, es sei denn, die Anordnungsbehörde bestätigt, dass ein entsprechendes Ersuchen um Herausgabe ausgestellt wurde. Innerhalb von 60 Tagen kann die Anordnungsbehörde die Dauer der Sicherung erforderlichenfalls um weitere 30 Tage verlängern, damit das anschließende Ersuchen.

ABSCHNITT A: Anordnungsbehörde für das EPOC-PR

Anordnungsstaat: … ....

Anordnungsbehörde: … .....

Aktenzeichen der Anordnungsbehörde: … ..... .

Falls abweichend von der im EPOC-PR angegebenen Kontaktstelle, Behörde/Ansprechpartner (z. B. zentrale Behörde) für Rückfragen im Zusammenhang mit der Ausführung des EPOC-PR:

Name und Kontaktangaben: … ....

ABSCHNITT B: Adressat des EPOC-PR

Adressat: … ....

Anschrift: … ....

Telefon/Fax/E-Mail (soweit bekannt): … ....

Kontaktperson (soweit bekannt): … ....

Aktenzeichen des Adressaten (soweit bekannt): … ....

Betroffener Diensteanbieter (falls nicht identisch mit dem Adressaten): … .....

Sonstige sachdienliche Angaben: … ....

ABSCHNITT C: Informationen über ein früheres EPOC-PR

Die Daten werden in Übereinstimmung mit dem EPOC-PR vom … ..... (Bitte das Datum der Ausstellung des Ersuchens angeben) gesichert und am … ..... (Bitte das Datum der Übermittlung des Ersuchens angeben) mit dem Aktenzeichen … ..... (Bitte das Aktenzeichen angeben) an … ..... übermittelt.

[1] Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl. L 191 vom 28.7.2023, S. 118).

ABSCHNITT D: Verlängerung einer früheren Sicherungsanordnung

Die Verpflichtung zur Sicherung von Daten im Rahmen des EPOC-PR gemäß Abschnitt C wird hiermit um weitere 30 Tage verlängert.

Unterschrift der Anordnungsbehörde und/oder ihres Vertreters

Name: ….....

Datum: ….....

Unterschrift ([2]): … ....

([2]) Wird das dezentrale IT-System nicht genutzt, fügen Sie bitte auch einen amtlichen Stempel, ein elektronisches Siegel oder eine gleichwertige Authentifizierung bei.