EUROPÄISCHE
KOMMISSION

Brüssel, den 25.11.2021
COM(2021) 718 final

2021/0382 (NLE)

Vorschlag für einen

BESCHLUSS DES RATES

zur Ermächtigung der Mitgliedstaaten, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials zu unterzeichnen

BEGRÜNDUNG

1. GEGENSTAND DES VORSCHLAGS

Der vorliegende Vorschlag betrifft den Beschluss zur Ermächtigung der Mitgliedstaaten, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials (im Folgenden „Protokoll“) zu unterzeichnen.[1] Ziel des Protokolls ist es, auf internationaler Ebene gemeinsame Vorschriften zur Verstärkung der Zusammenarbeit im Bereich der Computerkriminalität und bei der Sammlung von Beweismitteln in elektronischer Form für strafrechtliche Ermittlungen oder Verfahren festzulegen.

Die Kommission wird auch einen Vorschlag für einen Beschluss des Rates der Europäischen Union (im Folgenden „Rat“) vorlegen, mit dem die Mitgliedstaaten ermächtigt werden, das Protokoll im Interesse der Europäischen Union zu ratifizieren.

Computerkriminalität stellt nach wie vor eine erhebliche Herausforderung für unsere Gesellschaft dar. Trotz der Bemühungen der Strafverfolgungs- und Justizbehörden nehmen Cyberangriffe, die auch Ransomware-Angriffe umfassen, zu und werden immer komplexer.[2] Gerade weil es im Internet keine Grenzen gibt, sind Ermittlungen im Zusammenhang mit Computerkriminalität fast immer grenzübergreifend, was eine enge Zusammenarbeit zwischen den Behörden verschiedener Länder erforderlich macht.

Elektronische Beweismittel gewinnen für strafrechtliche Ermittlungen zunehmend an Bedeutung. Die Kommission schätzt, dass die Strafverfolgungs- und Justizbehörden heutzutage bei 85 % der strafrechtlichen Ermittlungen, auch in Bezug auf Computerkriminalität, Zugang zu elektronischen Beweismitteln benötigen.[3] Beweise für Straftaten werden zunehmend in elektronischer Form von Diensteanbietern in anderen Ländern aufbewahrt. Für eine wirksame strafrechtliche Verfolgung sind geeignete Maßnahmen erforderlich, um an diese Beweismittel zu gelangen, damit die Rechtsstaatlichkeit gewahrt wird.

Weltweit werden auf nationaler, EU-[4] und internationaler Ebene Bemühungen zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln für strafrechtliche Ermittlungen unternommen, unter anderem durch das Protokoll. Es ist wichtig, für kompatible Vorschriften auf internationaler Ebene zu sorgen, um bei den Bemühungen um grenzüberschreitenden Zugang zu elektronischen Beweismitteln Rechtskollisionen zu vermeiden.

2. KONTEXT DES VORSCHLAGS

2.1. Hintergrund

Mit dem Budapester Übereinkommen des Europarats über Computerkriminalität (SEV Nr. 185) (im Folgenden „Übereinkommen“) wird das Ziel verfolgt, die Bekämpfung von

[1] Der Wortlaut des Protokolls wird dem Vorschlag für einen Beschluss des Rates zur Ermächtigung der Mitgliedstaaten, im Interesse der Union das Protokoll zu ratifizieren, als Anhang beigefügt.

[2] Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität in der Europäischen Union 2021 (EU SOCTA 2021).

[3] SWD(2018) 118 final.

[4] COM(2018) 225 final und COM(2018) 226 final.

Straftaten, die mittels Nutzung von Rechnernetzen begangen werden, zu erleichtern. Erstens enthält es Bestimmungen zur Harmonisierung von Tatbestandsmerkmalen im innerstaatlichen materiellen Strafrecht und damit zusammenhängenden Bestimmungen auf dem Gebiet der Computerkriminalität, zweitens sieht es im innerstaatlichen Strafprozessrecht die erforderlichen Befugnisse für die Untersuchung und Verfolgung solcher Straftaten sowie anderer Straftaten, die mithilfe eines Computersystems begangen werden oder bei denen die Beweismittel in elektronischer Form vorliegen, vor, und drittens strebt es die Einführung einer schnellen und wirksamen Regelung für die internationale Zusammenarbeit an.

Das Übereinkommen steht den Mitgliedstaaten des Europarats sowie auf Einladung Nichtmitgliedern offen. Derzeit sind 66 Länder Vertragsparteien des Übereinkommens, darunter 26 Mitgliedstaaten der Europäischen Union[5]. Im Übereinkommen ist ein möglicher Beitritt der Europäischen Union zu dem Übereinkommen nicht vorgesehen. Die Europäische Union ist jedoch als Beobachterorganisation im Ausschuss für das Übereinkommen über Computerkriminalität (T-CY) anerkannt.[6]

Ungeachtet der Bemühungen, auf Ebene der Vereinten Nationen ein neues Übereinkommen über Computerkriminalität auszuhandeln[7], bleibt das Budapester Übereinkommen die wichtigste multilaterale Übereinkunft zur Bekämpfung der Computerkriminalität. Von der Union wird das Übereinkommen konsequent unterstützt[8], auch im Rahmen der Finanzierung von Programmen zum Kapazitätsaufbau[9].

Auf Vorschlag der Arbeitsgruppe Cloud-Beweismittel[10] hat der Ausschuss für das Übereinkommen über Computerkriminalität mehrere Empfehlungen abgegeben, um u. a. durch die Aushandlung eines Zweiten Zusatzprotokolls zum Übereinkommen über Computerkriminalität über eine verstärkte internationale Zusammenarbeit der Herausforderung zu begegnen, dass elektronische Beweismittel im Zusammenhang mit Computerkriminalität und anderen Straftaten zunehmend von Diensteanbietern in anderen Ländern aufbewahrt werden, während die Befugnisse der Strafverfolgungsbehörden durch territoriale Grenzen beschränkt sind. Im Juni 2017 genehmigte der Ausschuss für das Übereinkommen über Computerkriminalität das Mandat für die Ausarbeitung des Zweiten Zusatzprotokolls im Zeitraum September 2017 bis Dezember 2019.[11] Da für den Abschluss der Gespräche mehr Zeit benötigt wurde und die COVID-19-Pandemie in den Jahren 2020 und 2021 zu Beschränkungen führte, verlängerte der Ausschuss für das Übereinkommen über Computerkriminalität das Mandat anschließend zwei Mal: zunächst bis Dezember 2020 und dann bis Mai 2021.

---

5 Alle Mitgliedstaaten außer Irland, das das Übereinkommen unterzeichnet, aber nicht ratifiziert hat, den Beitritt jedoch weiter anstrebt.

6 Geschäftsordnung des Ausschusses für das Übereinkommen über Computerkriminalität (T-CY (2013)25 rev), abrufbar unter www.coe.int/cybercrime.

7 Resolution 74/247 der Generalversammlung der Vereinten Nationen von Dezember 2019 „Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken“.

8 JOIN(2020) 81 final.

9 Siehe beispielsweise das Projekt „Global Action on Cybercrime Extended (GLACY)+“, abrufbar unter https://www.coe.int/en/web/cybercrime/glacyplus.

10 Abschlussbericht der Arbeitsgruppe Cloud-Beweismittel des Ausschusses für das Übereinkommen über Computerkriminalität: „Zugang der Strafjustiz zu elektronischen Beweismitteln in der Cloud: Empfehlungen für die Beratungen des T-CY“ vom 16. September 2016.

11 https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690

Nachdem der Europäische Rat sie in seinen Schlussfolgerungen vom 18. Oktober 2018[12] dazu aufgefordert hatte, nahm die Kommission am 5. Februar 2019 eine Empfehlung für einen Beschluss des Rates an, mit dem die Kommission ermächtigt wird, im Namen der Europäischen Union an den Verhandlungen über ein Zweites Zusatzprotokoll zum Übereinkommen des Europarats über Computerkriminalität teilzunehmen.[13] Der Europäische Datenschutzbeauftragte gab am 2. April 2019 eine Stellungnahme zu der Empfehlung ab.[14] Mit Beschluss vom 6. Juni 2019 ermächtigte der Rat der Europäischen Union die Kommission, im Namen der Europäischen Union an den Verhandlungen über das Zweite Zusatzprotokoll teilzunehmen.[15]

Wie in der EU-Strategie für eine Sicherheitsunion aus dem Jahr 2020[16], der EU-Cybersicherheitsstrategie für die digitale Dekade aus dem Jahr 2020[17] und der EU-Strategie zur Bekämpfung der organisierten Kriminalität aus dem Jahr 2021[18] dargelegt, setzt sich die Kommission für einen zügigen und erfolgreichen Abschluss der Verhandlungen über das Protokoll ein. Auch das Europäische Parlament hat 2021 in einer Entschließung zur EU-Cybersicherheitsstrategie für die digitale Dekade[19] anerkannt, dass die Arbeiten an dem Protokoll abgeschlossen werden müssen.

Im Einklang mit dem Beschluss des Rates der Europäischen Union hat die Kommission im Namen der Europäischen Union an den Verhandlungen über das Protokoll teilgenommen. Die Kommission hat konsequent den Sonderausschuss des Rates für die Verhandlungen zum Standpunkt der Union konsultiert.

Nach der Rahmenvereinbarung über die Beziehungen zwischen dem Europäischen Parlament und der Europäischen Kommission[20] hat die Kommission auch das Europäische Parlament in schriftlichen Berichten und mündlichen Ausführungen über die Verhandlungen informiert.

In der Plenarsitzung des Ausschusses für das Übereinkommen über Computerkriminalität vom 28. Mai 2021 hat der Ausschuss für das Übereinkommen über Computerkriminalität den Entwurf des Protokolls auf seiner Ebene genehmigt und ihn zur Annahme durch das Ministerkomitee des Europarats weitergeleitet.[21] Am 17. November 2021 hat das Ministerkomitee des Europarats das Protokoll angenommen.

2.2. Das Zweite Zusatzprotokoll

Ziel des Protokolls ist die Verstärkung der Zusammenarbeit im Bereich der Computerkriminalität und bei der Sammlung von Beweismitteln in elektronischer Form für spezifische strafrechtliche Ermittlungen oder Verfahren. Mit dem Protokoll wird die

---

12 https://www.consilium.europa.eu/de/press/press-releases/2018/10/18/20181018-european-council-conslusions/

13 COM(2019) 71 final.

14 Stellungnahme des EDSB zu der Teilnahme an den Verhandlungen über ein Zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität vom 2. April 2019, Stellungnahme 3/2019.

15 Beschluss des Rates, Referenz 9116/19.

16 COM(2020) 605 final.

17 JOIN(2020) 81 final.

18 COM(2021) 170 final.

19 Entschließung des Europäischen Parlaments vom 10. Juni 2021 zu der Cybersicherheitsstrategie der EU für die digitale Dekade.

20 ABl. L 304 vom 20.11.2010, S. 47.

21 https://rm.coe.int/0900001680a2aa42

Notwendigkeit einer verstärkten und effizienteren Zusammenarbeit zwischen Staaten und mit dem Privatsektor anerkannt, wie auch der Bedarf an mehr Klarheit und Rechtssicherheit für Diensteanbieter und andere Stellen in Bezug auf die Umstände, unter denen sie Ersuchen von Strafverfolgungsbehörden anderer Vertragsparteien um Weitergabe elektronischer Beweismittel nachkommen dürfen.

Ferner wird mit dem Protokoll anerkannt, dass eine wirksame grenzüberschreitende Zusammenarbeit für die Zwecke der Strafjustiz – auch zwischen Behörden des öffentlichen Sektors und Stellen des privaten Sektors – wirksame Voraussetzungen und solide Garantien für den Schutz der Grundrechte erfordert. Zu diesem Zweck verfolgt das Protokoll einen rechtebasierten Ansatz und sieht Voraussetzungen und Garantien vor, die mit den internationalen Menschenrechtsinstrumenten, unter anderem der Konvention des Europarats von 1950 zum Schutze der Menschenrechte und Grundfreiheiten, im Einklang stehen. Da elektronische Beweismittel häufig personenbezogene Daten betreffen, enthält das Protokoll auch solide Garantien für den Schutz der Privatsphäre und personenbezogener Daten.

Die in den folgenden Abschnitten genannten Bestimmungen sind für das Protokoll von besonderer Bedeutung. Dem Protokoll ist ein ausführlicher erläuternder Bericht beigefügt. Der erläuternde Bericht stellt kein Instrument dar, das eine verbindliche Auslegung des Protokolls bietet, sondern soll die Vertragsparteien bei der Anwendung des Protokolls „anleiten und unterstützen“[22].

2.2.1. Allgemeine Bestimmungen

Kapitel I des Protokolls enthält allgemeine Bestimmungen. In Artikel 2 ist der Geltungsbereich des Protokolls entsprechend dem Geltungsbereich des Übereinkommens festgelegt: Es gilt für spezifische strafrechtliche Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten sowie für die Erhebung von Beweismaterial in elektronischer Form für eine Straftat.

Artikel 3 enthält die Begriffsbestimmungen für „zentrale Behörde“, „zuständige Behörde“, „Notfall“, „personenbezogene Daten“ und „übermittelnde Vertragspartei“. Diese Begriffsbestimmungen gelten, zusammen mit den Begriffsbestimmungen des Übereinkommens, für das Protokoll.

In Artikel 4 sind die Sprachen festgelegt, in denen die Vertragsparteien Anordnungen, Ersuchen oder Notifikationen nach dem Protokoll übermitteln sollten.

2.2.2. Maßnahmen für die Zusammenarbeit

Kapitel II des Protokolls enthält Maßnahmen für eine verstärkte Zusammenarbeit. Zunächst ist in Artikel 5 Absatz 1 festgelegt, dass die Vertragsparteien auf der Grundlage des Protokolls im größtmöglichen Umfang zusammenarbeiten. In Artikel 5 Absätze 2 bis 5 ist geregelt, wie die Maßnahmen des Protokolls im Verhältnis zu bestehenden Rechtshilfeverträgen oder Übereinkünften anzuwenden sind. In Artikel 5 Absatz 7 ist festgelegt, dass die Zusammenarbeit zwischen Vertragsparteien oder zwischen Vertragsparteien und Diensteanbietern oder Stellen nach anderen anwendbaren Übereinkünften, Vereinbarungen, Verfahrensweisen oder nach anwendbarem innerstaatlichem Recht durch die in Kapitel II genannten Maßnahmen nicht beschränkt wird.

[22] Siehe Absatz 2 des erläuternden Berichts zu dem Protokoll.

Artikel 6 bildet eine Grundlage für die direkte Zusammenarbeit zwischen zuständigen Behörden in einer Vertragspartei und Stellen, die in einer anderen Vertragspartei Domänennamenregistrierungsdienste erbringen, bei der Weitergabe von Domainnamenregistrierungsdaten.

Artikel 7 bildet eine Grundlage für die direkte Zusammenarbeit zwischen zuständigen Behörden in einer Vertragspartei und Diensteanbietern in einer anderen Vertragspartei bei der Weitergabe von Bestandsdaten.

Artikel 8 bildet eine Grundlage für eine verstärkte Zusammenarbeit zwischen Behörden bei der Weitergabe von Computerdaten.

Artikel 9 bildet eine Grundlage für die Zusammenarbeit zwischen Behörden bei der Weitergabe von Computerdaten in Notfällen.

Artikel 10 bildet eine Grundlage für die Rechtshilfe in Notfällen.

Artikel 11 bildet eine Grundlage für eine Zusammenarbeit per Videokonferenz.

Artikel 12 bildet eine Grundlage für gemeinsame Ermittlungen und gemeinsame Ermittlungsgruppen.

2.2.3. Garantien

Das Protokoll verfolgt einen rechtebasierten Ansatz mit spezifischen Voraussetzungen und Garantien, von denen einige in die spezifischen Kooperationsmaßnahmen sowie in Kapitel III des Protokolls einbezogen wurden. Nach Artikel 13 des Protokolls müssen die Vertragsparteien sicherstellen, dass die Befugnisse und Verfahren einen angemessenen Schutz der Grundrechte vorsehen, wodurch, im Einklang mit Artikel 15 des Übereinkommens, die Anwendung des Grundsatzes der Verhältnismäßigkeit sichergestellt wird.

In Artikel 14 des Protokolls ist der Schutz personenbezogener Daten im Sinne des Artikels 3 des Protokolls im Einklang mit dem Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 223) (Übereinkommen 108+) und dem Unionsrecht vorgesehen.

Auf dieser Grundlage sind in Artikel 14 Absätze 2 bis 15 grundlegende Datenschutzgrundsätze festgelegt, darunter Zweckbindung, Rechtsgrundlage, Datenqualität sowie Vorschriften für die Verarbeitung besonderer Datenkategorien und Pflichten der für die Verarbeitung Verantwortlichen (u. a. in Bezug auf die Speicherung, das Führen von Aufzeichnungen, die Sicherheit und die Weiterübermittlung), durchsetzbare Rechte des Einzelnen (u. a. in Bezug auf Notifikation, Zugang, Berichtigung und automatisierte Entscheidungen), eine unabhängige und wirksame Aufsicht durch eine oder mehrere Behörden sowie verwaltungsrechtliche und gerichtliche Rechtsbehelfe. Die Garantien gelten für alle Formen der Zusammenarbeit, die im Protokoll festgelegt sind, wobei erforderlichenfalls Anpassungen vorgenommen werden, um den Besonderheiten der direkten Zusammenarbeit Rechnung zu tragen (z. B. im Zusammenhang mit der Meldung von Verstößen). Die Ausübung bestimmter Rechte des Einzelnen kann aufgeschoben, beschränkt oder versagt werden, wenn dies für die Verfolgung wichtiger Ziele des Allgemeininteresses erforderlich und angemessen ist, insbesondere, um eine Gefährdung laufender Ermittlungen der Strafverfolgungsbehörden zu verhindern. Dies steht auch im Einklang mit dem Unionsrecht.

Artikel 14 des Protokolls sollte auch in Verbindung mit Artikel 23 des Protokolls ausgelegt werden. Artikel 23 stärkt die Wirksamkeit der im Protokoll enthaltenen Garantien, indem er vorsieht, dass der Ausschuss für das Übereinkommen über Computerkriminalität die Umsetzung und Anwendung der Maßnahmen bewertet, die in den nationalen Rechtsvorschriften zur Durchführung der Bestimmungen des Protokolls getroffen wurden. Insbesondere wird in Artikel 23 Absatz 3 ausdrücklich anerkannt, dass die Durchführung des Artikels 14 durch die Vertragsparteien bewertet wird, sobald zehn Vertragsparteien des Übereinkommens ihre Zustimmung ausgedrückt haben, durch das Protokoll gebunden zu sein.

Als weitere Garantie nach Artikel 14 Absatz 15 kann eine Vertragspartei, wenn ihr stichhaltige Beweise dafür vorliegen, dass eine andere Vertragspartei systematisch oder schwerwiegend gegen die im Protokoll festgelegten Garantien verstößt, die Übermittlung personenbezogener Daten an diese Vertragspartei nach einer Konsultation (die in dringenden Fällen nicht erforderlich ist) aussetzen. Vor der Aussetzung übermittelte personenbezogene Daten müssen weiterhin im Einklang mit dem Protokoll verarbeitet werden.

Außerdem gestattet Artikel 14 Absatz 1 Buchstaben b und c des Protokolls es den Vertragsparteien angesichts des multilateralen Charakters des Protokolls, in ihren bilateralen Beziehungen unter bestimmten Voraussetzungen alternative Möglichkeiten zur Gewährleistung des Schutzes personenbezogener Daten, die im Rahmen des Protokolls übermittelt werden, zu vereinbaren. Die Garantien nach Artikel 14 Absätze 2 bis 15 gelten zwar standardmäßig für Vertragsparteien, die personenbezogene Daten empfangen, jedoch können sich Vertragsparteien, die wechselseitig durch eine völkerrechtliche Übereinkunft gebunden sind, die einen umfassenden Rahmen für den Schutz personenbezogener Daten im Einklang mit den geltenden Anforderungen der Rechtsvorschriften der betreffenden Vertragsparteien schafft, auf der Grundlage des Artikels 14 Absatz 1 Buchstabe b ebenfalls auf diesen Rahmen stützen. Dies gilt beispielsweise für das Übereinkommen 108+ (in Bezug auf die Vertragsparteien, die Datenübermittlungen an andere Vertragsparteien nach diesem Übereinkommen gestatten) oder das Rahmenabkommen zwischen der EU und den USA (innerhalb seines Anwendungsbereichs, d. h. für die Übermittlung personenbezogener Daten zwischen Behörden und – in Verbindung mit einer spezifischen Übermittlungsvereinbarung zwischen den USA und der EU – für die direkte Zusammenarbeit zwischen Behörden und Diensteanbietern). Darüber hinaus können die Vertragsparteien auf der Grundlage des Artikels 14 Absatz 1 Buchstabe c auch einvernehmlich bestimmen, dass die Übermittlung personenbezogener Daten auf der Grundlage anderer Übereinkünfte oder Vereinbarungen zwischen den betreffenden Vertragsparteien erfolgt. Die EU-Mitgliedstaaten können sich bei Datenübermittlungen nach dem Protokoll nur dann auf eine solche alternative Übereinkunft oder Vereinbarung stützen, wenn diese Übermittlungen den Anforderungen des Datenschutzrechts der Union entsprechen, nämlich Kapitel V der Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei der Strafverfolgung) und (für die direkte Zusammenarbeit zwischen Behörden und Diensteanbietern nach den Artikeln 6 und 7 des Protokolls) Kapitel V der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung).

2.2.4. Schlussbestimmungen

Kapitel IV des Protokolls enthält Schlussbestimmungen. Unter anderem wird mit Artikel 15 Absatz 1 Buchstabe a sichergestellt, dass die Vertragsparteien ihre Beziehungen in Bezug auf die von dem Protokoll erfassten Fragen im Einklang mit Artikel 39 Absatz 2 des Übereinkommens auf andere Weise regeln können. Artikel 15 Absatz 1 Buchstabe b gewährleistet, dass EU-Mitgliedstaaten, die Vertragspartei des Protokolls sind, in ihren Beziehungen untereinander weiterhin Unionsrecht anwenden können. Ferner bestimmt

Artikel 15 Absatz 2, dass Artikel 39 Absatz 3 des Übereinkommens auf das Protokoll Anwendung findet.

Nach Artikel 16 Absatz 3 tritt das Protokoll in Kraft, sobald fünf Vertragsparteien des Übereinkommens ihre Zustimmung ausgedrückt haben, durch das Protokoll gebunden zu sein.

In Artikel 19 Absatz 1 ist vorgesehen, dass die Vertragsparteien von den Vorbehalten nach Artikel 7 Absatz 9 Buchstaben a und b, Artikel 8 Absatz 13 und Artikel 17 Gebrauch machen können. In Artikel 19 Absatz 2 ist vorgesehen, dass die Vertragsparteien Erklärungen nach Artikel 7 Absatz 2 Buchstabe b und Absatz 8, Artikel 8 Absatz 11, Artikel 9 Absatz 1 Buchstabe b und Absatz 5, Artikel 10 Absatz 9, Artikel 12 Absatz 3 und Artikel 18 Absatz 2 abgeben können. Artikel 19 Absatz 3 bestimmt, dass eine Vertragspartei Erklärungen, Notifikationen oder Mitteilungen nach Artikel 7 Absatz 5 Buchstaben a und e, Artikel 8 Absatz 4 und Absatz 10 Buchstaben a und b, Artikel 14 Absatz 7 Buchstabe c und Absatz 10 Buchstabe b sowie Artikel 17 Absatz 2 abzugeben hat.

Artikel 23 Absatz 1 bildet im Einklang mit Artikel 46 des Übereinkommens eine Grundlage für Konsultationen zwischen Vertragsparteien, die auch im Ausschuss für das Übereinkommen über Computerkriminalität stattfinden können. Ferner bildet Artikel 23 Absatz 2 eine Grundlage für die Bewertung der Anwendung und Durchführung der Bestimmungen des Protokolls. Mit Artikel 23 Absatz 3 wird sichergestellt, dass die Bewertung der Anwendung und Umsetzung des Artikels 14 (Datenschutz) beginnt, sobald zehn Vertragsparteien ihre Zustimmung ausgedrückt haben, durch das Protokoll gebunden zu sein.

2.3. Rechtsvorschriften und Strategien der Union in diesem Bereich

Der durch das Protokoll geregelte Bereich ist weitgehend Gegenstand gemeinsamer Vorschriften auf der Grundlage des Artikels 82 Absatz 1 und des Artikels 16 AEUV. Der derzeitige Rechtsrahmen der Europäischen Union umfasst insbesondere Instrumente zur Strafverfolgung und justiziellen Zusammenarbeit in Strafsachen wie beispielsweise die Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen, das Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union und den Rahmenbeschluss 2002/465/JI des Rates über gemeinsame Ermittlungsgruppen. Extern hat die Europäische Union eine Reihe bilateraler Abkommen zwischen der Union und Drittländern geschlossen, wie etwa die Rechtshilfeabkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika, zwischen der Europäischen Union und Japan sowie zwischen der Europäischen Union und Norwegen und Island. Der derzeitige Rechtsrahmen der Europäischen Union umfasst auch die Verordnung (EU) 2017/1939 zur Durchführung einer Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft (EUStA). Die Mitgliedstaaten, die sich an der Verstärkten Zusammenarbeit beteiligen, sollten sicherstellen, dass die EUStA bei der Ausübung ihrer Zuständigkeiten nach den Artikeln 22, 23 und 25 der Verordnung (EU) 2017/1939 in gleicher Weise um eine Zusammenarbeit nach dem Protokoll ersuchen kann wie die nationalen Staatsanwälte dieser Mitgliedstaaten. Diese Instrumente und Abkommen stehen insbesondere mit den Artikeln 8, 9, 10, 11 und 12 des Protokolls in Zusammenhang.

Darüber hinaus hat die Union mehrere Richtlinien erlassen, mit denen die Verfahrensrechte von Verdächtigen und Beschuldigten gestärkt werden.[23] Diese Rechtsakte stehen

[23] 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);

insbesondere mit den Artikeln 6, 7, 8, 9, 10, 11, 12 und 13 des Protokolls in Zusammenhang. Besondere Garantien gelten für den Schutz personenbezogener Daten, der ein in den EU-Verträgen und in der Charta der Grundrechte der Europäischen Union verankertes Grundrecht ist. Personenbezogene Daten dürfen nur im Einklang mit der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) und der Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei der Strafverfolgung) verarbeitet werden. Das Grundrecht aller Menschen auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Kommunikation schließt als wesentliches Element auch die Achtung der Privatsphäre in der Kommunikation ein. Elektronische Kommunikationsdaten dürfen nur im Einklang mit der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) verarbeitet werden. Diese Rechtsakte stehen insbesondere mit Artikel 14 des Protokolls in Zusammenhang.

In Artikel 14 Absätze 2 bis 15 des Protokolls sind geeignete Datenschutzgarantien im Sinne der Datenschutzvorschriften der Union, insbesondere des Artikels 46 der Datenschutz-Grundverordnung und des Artikels 37 der Richtlinie zum Datenschutz bei der Strafverfolgung, sowie im Sinne der einschlägigen Rechtsprechung des Europäischen Gerichtshofs vorgesehen. Im Einklang mit den Anforderungen des Unionsrechts[24] und um die Wirksamkeit der in Artikel 14 des Protokolls vorgesehenen Garantien zu gewährleisten, sollten die Mitgliedstaaten – vorbehaltlich bestimmter Einschränkungen, z. B. um laufende Ermittlungen nicht zu gefährden – die Benachrichtigung der Personen, deren Daten übermittelt wurden, sicherstellen. Artikel 14 Absatz 11 Buchstabe c des Protokolls bietet den Mitgliedstaaten eine Grundlage für die Erfüllung dieser Anforderung.

Damit Artikel 14 Absatz 1 des Protokolls mit den Datenschutzvorschriften der Union vereinbar ist, ist ferner erforderlich, dass die Mitgliedstaaten im Hinblick auf mögliche Alternativen zur Gewährleistung eines angemessenen Schutzes der nach dem Protokoll übermittelten personenbezogenen Daten Folgendes bedenken. Hinsichtlich anderer internationaler Übereinkünfte, die einen umfassenden Rahmen für den Schutz personenbezogener Daten im Einklang mit den geltenden Anforderungen der

---

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); 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); 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); 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); 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); Richtlinie 2012/13/EU des Europäischen Parlaments und des Rates vom 22. Mai 2012 über das Recht auf Belehrung und Unterrichtung in Strafverfahren.

[24] Siehe Gerichtshof (Große Kammer), Gutachten 1/15, ECLI:EU:C:2017:592, Rn. 220. Siehe auch den Beitrag des EDSA zur Konsultation zum Entwurf eines Zweiten Zusatzprotokolls zum Übereinkommen des Europarats über Computerkriminalität (Budapester Übereinkommen) vom 13. November 2019, S. 6 („Die zuständigen nationalen Behörden, denen Zugang zu den Daten gewährt wurde, müssen die betroffenen Personen nach den geltenden nationalen Verfahren benachrichtigen, sobald eine solche Benachrichtigung die von diesen Behörden durchgeführten Ermittlungen nicht mehr gefährdet. … Die Benachrichtigung ist erforderlich, damit die betroffenen Personen unter anderem ihr Recht auf Einlegung eines Rechtsbehelfs und ihre Datenschutzrechte im Zusammenhang mit der Verarbeitung ihrer Daten ausüben können.“).

Rechtsvorschriften der betreffenden Vertragsparteien schaffen, sollten die Mitgliedstaaten nach Artikel 14 Absatz 1 Buchstabe b berücksichtigen, dass das Rahmenabkommen zwischen der EU und den USA für eine direkte Zusammenarbeit durch zusätzliche Garantien ergänzt werden muss, die den besonderen Anforderungen an eine Übermittlung elektronischer Beweismittel, die direkt durch Diensteanbieter und nicht zwischen Behörden erfolgt, Rechnung trägt. Diese zusätzlichen Garantien sind in einer spezifischen Übermittlungsvereinbarung zwischen den USA und der EU bzw. ihren Mitgliedstaaten vorzusehen.[25]

Ferner sollten die Mitgliedstaaten nach Artikel 14 Absatz 1 Buchstabe b des Protokolls bedenken, dass für EU-Mitgliedstaaten, die Vertragspartei des Übereinkommens 108+ sind, dieses Übereinkommen allein keine geeignete Grundlage für grenzüberschreitende Datenübermittlungen nach dem Protokoll an andere Vertragsparteien des genannten Übereinkommens darstellt. In diesem Zusammenhang sollten sie Artikel 14 Absatz 1 letzter Satz des Übereinkommens 108+ berücksichtigen.[26]

In Bezug auf andere Übereinkünfte oder Vereinbarungen nach Artikel 14 Absatz 1 Buchstabe c sollten die Mitgliedstaaten schließlich noch bedenken, dass sie sich nur dann auf solche anderen Übereinkünfte oder Vereinbarungen stützen dürfen, wenn entweder die Europäische Kommission einen Angemessenheitsbeschluss nach Artikel 45 der Datenschutz-Grundverordnung (EU) 2016/679 oder Artikel 36 der Richtlinie (EU) 2016/680 zum Datenschutz bei der Strafverfolgung für das betreffende Drittland erlassen hat, der für die jeweiligen Datenübermittlungen gilt, oder wenn die Übereinkunft oder Vereinbarung selbst geeignete Datenschutzgarantien nach Artikel 46 der Datenschutz-Grundverordnung oder Artikel 37 Absatz 1 Buchstabe a der Richtlinie zum Datenschutz bei der Strafverfolgung bietet.

Dabei ist nicht nur das Unionsrecht in seiner derzeitigen Form in dem betreffenden Bereich zu berücksichtigen, sondern auch seine künftige Entwicklung, soweit diese zum Zeitpunkt der Analyse absehbar ist. Der Bereich, um den es im Protokoll geht, ist für die absehbare künftige Entwicklung des Unionsrechts von unmittelbarer Bedeutung. In diesem Zusammenhang sind die Vorschläge der Kommission zum grenzüberschreitenden Zugang zu elektronischen Beweismitteln von April 2018[27] zu beachten. Diese Instrumente stehen insbesondere mit den Artikeln 6 und 7 des Protokolls in Zusammenhang.

Während die Kommission im Namen der Union an den Verhandlungen teilnahm, stellte sie sicher, dass das Protokoll in jeder Hinsicht mit dem Unionsrecht und den sich daraus ergebenden Verpflichtungen der Mitgliedstaaten vereinbar ist. Insbesondere stellte die

---

[25] Aus diesem Grund enthält der Beschluss des Rates vom 21. Mai 2019 über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen (9114/19) in seinen Verhandlungsrichtlinien eine Reihe zusätzlicher Datenschutzgarantien. Insbesondere heißt es in den Verhandlungsrichtlinien: „Das Abkommen sollte das Rahmenabkommen durch zusätzliche Garantien ergänzen, die der Sensibilität der betroffenen Datenkategorien und den besonderen Anforderungen an die direkte Übermittlung elektronischer Beweismittel durch Diensteanbieter statt zwischen Behörden und an die direkte Übermittlung von zuständigen Behörden an Diensteanbieter Rechnung tragen."

[26] Siehe auch den Erläuternden Bericht zum Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 10. Oktober 2018, Ziffern 106 bis 107.

[27] COM(2018) 225 final und COM(2018) 226 final.

Kommission sicher, dass die Bestimmungen des Protokolls es den Mitgliedstaaten ermöglichen, die in den EU-Verträgen und in der Charta der Grundrechte der Europäischen Union verankerten Grundrechte, Grundfreiheiten und allgemeinen Grundsätze des Unionsrechts zu achten, einschließlich der Verhältnismäßigkeit, der Verfahrensrechte, der Unschuldsvermutung und der Verteidigungsrechte von Personen, gegen die ein Strafverfahren anhängig ist, sowie der Achtung der Privatsphäre und des Schutzes personenbezogener Daten und elektronischer Kommunikationsdaten, wenn diese Daten verarbeitet werden, einschließlich der Übermittlung von Daten an Strafverfolgungsbehörden in Ländern außerhalb der Europäischen Union, sowie diesbezügliche Verpflichtungen der Strafverfolgungs- und Justizbehörden. Die Kommission berücksichtigte auch die Stellungnahmen des Europäischen Datenschutzbeauftragten[28] und des Europäischen Datenschutzausschusses[29].

Ferner stellte die Kommission sicher, dass die Bestimmungen des Protokolls und die Vorschläge der Kommission zu elektronischen Beweismitteln miteinander vereinbar sind – auch insofern, als der Entwurf der Gesetzgebungsakte in den Beratungen mit den beiden gesetzgebenden Organen weiterentwickelt wurde – und dass das Protokoll nicht zu Rechtskollisionen führt. Die Kommission stellte vor allem sicher, dass das Protokoll geeignete Garantien für den Datenschutz und den Schutz der Privatsphäre enthält, die es Diensteanbietern in der EU insofern ermöglichen, ihre Verpflichtungen aus den EU-Rechtsvorschriften zum Datenschutz und zum Schutz der Privatsphäre zu erfüllen, als das Protokoll eine Rechtsgrundlage für Datenübermittlungen aufgrund von Anordnungen oder Ersuchen einer Behörde einer nicht der EU angehörenden Vertragspartei des Protokolls bietet, durch die ein für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter in der EU zur Weitergabe personenbezogener Daten oder elektronischer Kommunikationsdaten verpflichtet wird.

2.4. Vorbehalte, Erklärungen, Notifikationen und Mitteilungen sowie sonstige Erwägungen

Im Protokoll ist die Möglichkeit vorgesehen, dass die Vertragsparteien bestimmte Vorbehalte geltend machen und Erklärungen, Notifikationen oder Mitteilungen zu bestimmten Artikeln abgeben. Bei bestimmten Vorbehalten und Erklärungen, Notifikationen und Mitteilungen sollten die Mitgliedstaaten einen einheitlichen Ansatz verfolgen, der im Anhang dieses Beschlusses dargelegt ist. Damit die Vereinbarkeit der Durchführung des Protokolls mit dem Unionsrecht gewährleistet wird, sollten die EU-Mitgliedstaaten bei ihren Vorbehalten und Erklärungen den im Folgenden dargelegten Standpunkt vertreten. In den Fällen, in denen das Protokoll eine Grundlage für andere Vorbehalte, Erklärungen, Notifikationen oder Mitteilungen bietet, ermächtigt dieser Vorschlag die Mitgliedstaaten, ihre eigenen Vorbehalte, Erklärungen, Notifikationen oder Mitteilungen zu erwägen und abzugeben.

---

[28] Stellungnahme des EDSB zu der Teilnahme an den Verhandlungen über ein Zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität vom 2. April 2019, Stellungnahme 3/2019.

[29] Unter anderem „EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)“ (Beitrag des EDSA zur Konsultation zum Entwurf eines Zweiten Zusatzprotokolls zum Übereinkommen des Europarats über Computerkriminalität (Budapester Übereinkommen)) vom 13. November 2019; „Stellungnahme 02/2021 zum neuen Entwurf von Bestimmungen des Zweiten Zusatzprotokolls zum Übereinkommen des Europarats über Computerkriminalität (Budapester Übereinkommen)“ in der am 2. Februar 2021 angenommenen Fassung; „EDPB Contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime of 4 May 2021“ (Beitrag des EDSA zur 6. Konsultationsrunde zum Entwurf des Zweiten Zusatzprotokolls zum Budapester Übereinkommen des Europarats über Computerkriminalität vom 4. Mai 2021).

Damit die Vereinbarkeit der Bestimmungen des Protokolls mit den einschlägigen Rechtsvorschriften und Strategien der Union gewährleistet ist, sollten die Mitgliedstaaten von den Vorbehalten nach Artikel 7 Absatz 9 Buchstaben a[30] und b[31] keinen Gebrauch machen. Außerdem sollten die Mitgliedstaaten die Erklärung nach Artikel 7 Absatz 2 Buchstabe b[32] und die Notifikation nach Artikel 7 Absatz 5 Buchstabe a[33] abgeben. Die Nichtinanspruchnahme dieser Vorbehalte und die Vorlage der Erklärung und der Notifikation sind wichtig, um die Vereinbarkeit des Protokolls mit den Legislativvorschlägen der Kommission zu elektronischen Beweismitteln zu gewährleisten, auch insofern, als der Entwurf der Gesetzgebungsakte in den Beratungen mit den beiden gesetzgebenden Organen weiterentwickelt wird.

Um eine einheitliche Anwendung des Protokolls in der Zusammenarbeit der EU-Mitgliedstaaten mit Vertragsparteien, die keine EU-Mitgliedstaaten sind, zu gewährleisten, werden die Mitgliedstaaten außerdem aufgefordert, von dem Vorbehalt nach Artikel 8 Absatz 13[34] keinen Gebrauch zu machen, auch weil ein solcher Vorbehalt eine Wechselwirkung haben würde[35]. Die Mitgliedstaaten sollten die Erklärung nach Artikel 8 Absatz 4 abgeben, damit den Anordnungen nachgekommen werden kann, falls zusätzliche begleitende Angaben erforderlich sind, z. B. über die Umstände des vorliegenden Falls, um Erforderlichkeit und Angemessenheit beurteilen zu können.[36]

Die Mitgliedstaaten werden ferner aufgefordert, von der Abgabe der Erklärung nach Artikel 9 Absatz 1 Buchstabe b[37] abzusehen, um eine wirksame Anwendung des Protokolls zu gewährleisten.

Die Mitgliedstaaten sollten die Mitteilungen nach Artikel 7 Absatz 5 Buchstabe e[38], Artikel 8 Absatz 10 Buchstaben a und b[39], Artikel 14 Absatz 7 Buchstabe c und Absatz 10 Buchstabe b vornehmen, um eine insgesamt wirksame Anwendung des Protokolls zu gewährleisten[40].

---

30 Die Vertragsparteien können sich das Recht vorbehalten, Artikel 7 (Weitergabe von Bestandsdaten) nicht anzuwenden.

31 Die Vertragsparteien können sich das Recht vorbehalten, Artikel 7 (Weitergabe von Bestandsdaten) auf bestimmte Arten von Zugangsnummern nicht anzuwenden, wenn dies mit den Grundprinzipien ihrer innerstaatlichen Rechtsordnung unvereinbar wäre.

32 Die Vertragsparteien können erklären, dass die Anordnung nach Artikel 7 Absatz 1 (Weitergabe von Bestandsdaten) durch eine Staatsanwältin beziehungsweise durch einen Staatsanwalt oder eine andere Justizbehörde oder unter staatsanwaltlicher Aufsicht oder unter Aufsicht einer anderen Justizbehörde oder anderweitig unter unabhängiger Aufsicht erlassen werden muss.

33 Die Vertragsparteien können der Generalsekretärin beziehungsweise dem Generalsekretär des Europarats notifizieren, dass sie, wenn eine Anordnung nach Artikel 7 Absatz 1 (Weitergabe von Bestandsdaten) an einen Diensteanbieter in ihrem Hoheitsgebiet gerichtet wird, in jedem Fall oder unter bestimmten Umständen eine zeitgleiche Benachrichtigung über die Anordnung, die ergänzenden Angaben und eine Zusammenfassung des mit den Ermittlungen oder dem Verfahren in Zusammenhang stehenden Sachverhalts verlangt.

34 Die Vertragsparteien können sich das Recht vorbehalten, Artikel 8 (Durchführung von Anordnungen einer anderen Vertragspartei) auf Verkehrsdaten nicht anzuwenden.

35 Siehe Absatz 147 des erläuternden Berichts zu dem Protokoll, in dem es heißt: „Eine Vertragspartei, die von dem Vorbehalt zu diesem Artikel Gebrauch macht, darf anderen Vertragsparteien keine Anordnungen in Bezug auf Verkehrsdaten nach [Artikel 8] Absatz 1 übermitteln“.

36 Die Vertragsparteien können erklären, dass zur Erfüllung einer Anordnung nach Artikel 8 Absatz 1 (Durchführung von Anordnungen einer anderen Vertragspartei) zusätzliche begleitende Angaben erforderlich sind.

37 Die Vertragsparteien können erklären, dass sie keine Ersuchen nach Artikel 9 Absatz 1 Buchstabe a (Umgehende Weitergabe von Computerdaten im Notfall), die lediglich auf die Weitergabe von Bestandsdaten gerichtet sind, erledigen werden.

Die Mitgliedstaaten sollten schließlich auch die nach Artikel 14 Absatz 11 Buchstabe c erforderlichen Maßnahmen treffen. Damit wird die empfangende Vertragspartei zum Zeitpunkt der Übermittlung über die unionsrechtliche Pflicht zur Benachrichtigung der Person, deren Daten übermittelt wurden[41], informiert und erhält geeignete Kontaktdaten, die es ihr ermöglichen, die zuständige Behörde in dem EU-Mitgliedstaat zu informieren, sobald die Vertraulichkeitsbeschränkung nicht mehr gilt und die Benachrichtigung erfolgen kann.

2.5. Grund für den Vorschlag

Das Protokoll tritt nach Artikel 16 Absätze 1 und 2 in Kraft, sobald fünf Vertragsparteien ihre Zustimmung ausgedrückt haben, durch das Protokoll gebunden zu sein. Die feierliche Unterzeichnung des Protokolls ist für März 2022 vorgesehen.

Die EU-Mitgliedstaaten sollten die notwendigen Schritte für ein zeitnahes Inkrafttreten des Protokolls unternehmen, da dies aus mehreren Gründen von Belang ist.

Erstens wird mit dem Protokoll sichergestellt, dass die Strafverfolgungs- und Justizbehörden besser gerüstet sind, um die für strafrechtliche Ermittlungen erforderlichen elektronischen Beweismittel zu beschaffen. Angesichts der zunehmenden Bedeutung elektronischer Beweismittel für strafrechtliche Ermittlungen ist es dringend erforderlich, dass die Strafverfolgungs- und Justizbehörden über die richtigen Instrumente verfügen, um auf wirksame Weise Zugang zu elektronischen Beweismitteln zu erhalten, damit sie Kriminalität im Internet wirksam bekämpfen können.

Zweitens wird mit dem Protokoll sichergestellt, dass diese Maßnahmen zur Erlangung des Zugangs zu elektronischen Beweismitteln so angewendet werden, dass die Mitgliedstaaten die Grundrechte, einschließlich der Verfahrensrechte in Strafverfahren, des Rechts auf Privatsphäre und des Rechts auf Schutz personenbezogener Daten, achten können. Ohne klare Vorschriften auf internationaler Ebene könnten die bestehenden Vorgehensweisen mit Blick auf Rechtssicherheit, Transparenz, Rechenschaftspflicht und Achtung der Grundrechte und der Verfahrensgarantien für Verdächtige bei strafrechtlichen Ermittlungen zu Herausforderungen führen.

Drittens werden mit dem Protokoll Rechtskollisionen, die sowohl Behörden als auch private Diensteanbieter und andere Stellen betreffen, gelöst und verhindert, indem auf internationaler Ebene kompatible Vorschriften für den grenzüberschreitenden Zugang zu elektronischen Beweismitteln festgelegt werden.

---

[38] Die Vertragsparteien können die Kontaktdaten der Behörde übermitteln, die für die Entgegennahme von Benachrichtigungen nach Artikel 7 Absatz 5 Buchstabe a und die Durchführung der in Artikel 7 Absatz 5 Buchstaben b, c und d bezeichneten Maßnahmen (Weitergabe von Bestandsdaten) bestimmt wurde.

[39] Die Vertragsparteien können die Kontaktdaten der Behörden übermitteln, die für die Vorlage und Entgegennahme von Anordnungen nach Artikel 8 (Durchführung von Anordnungen einer anderen Vertragspartei) bestimmt wurden. Nach der Verordnung (EU) 2017/1939 müssen die Mitgliedstaaten, die sich an der Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft (EUStA) beteiligen, die EUStA in die Mitteilung einbeziehen.

[40] Die Vertragsparteien können die Behörden mitteilen, die im Falle eines Sicherheitsvorfalls zu benachrichtigen sind oder die im Falle einer Weiterübermittlung an einen anderen Staat oder eine internationale Organisation zu kontaktieren sind, um eine vorherige Genehmigung einzuholen.

[41] Siehe Fußnote 24.

Viertens verdeutlicht das Protokoll den Stellenwert des Übereinkommens als nach wie vor wichtigster multilateraler Rahmen für die Bekämpfung der Computerkriminalität. Dies wird für den Prozess im Anschluss an die Resolution 74/247 der Generalversammlung der Vereinten Nationen vom Dezember 2019 „Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken“ von zentraler Bedeutung sein, mit der ein offener zwischenstaatlicher Ad-hoc-Sachverständigenausschuss eingerichtet wurde, der ein umfassendes internationales Übereinkommen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken ausarbeiten soll.

3. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

- *Rechtsgrundlage*

Die Zuständigkeit der Union für den Erlass von Rechtsvorschriften im Bereich der Erleichterung der Zusammenarbeit zwischen Justizbehörden oder entsprechenden Behörden im Rahmen der Strafverfolgung sowie des Vollzugs und der Vollstreckung von Entscheidungen beruht auf Artikel 82 Absatz 1 AEUV. Die Zuständigkeit der Union im Bereich des Schutzes personenbezogener Daten beruht auf Artikel 16 AEUV.

Nach Artikel 3 Absatz 2 AEUV hat die Union die ausschließliche Zuständigkeit für den Abschluss internationaler Übereinkünfte, soweit er gemeinsame Regeln der EU beeinträchtigen oder deren Tragweite verändern könnte. Die Bestimmungen des Protokolls gehören zu einem Bereich, der weitgehend Gegenstand gemeinsamer Vorschriften ist, wie oben in Abschnitt 2.3 dargelegt wurde.

Das Protokoll fällt daher in die ausschließliche Außenkompetenz der Union. Die Unterzeichnung des Protokolls durch die Mitgliedstaaten im Interesse der Union kann daher auf der Grundlage des Artikels 16, des Artikels 82 Absatz 1 und des Artikels 218 Absatz 5 AEUV erfolgen.

- *Subsidiarität (bei nicht ausschließlicher Zuständigkeit)*

Entfällt.

- *Verhältnismäßigkeit*

Die von der Union mit diesem Vorschlag verfolgten Ziele, die in Abschnitt 2.5 dargelegt wurden, können nur erreicht werden, wenn ein verbindliches internationales Übereinkommen geschlossen wird, das die notwendigen Kooperationsmaßnahmen vorsieht und gleichzeitig einen angemessenen Schutz der Grundrechte gewährleistet. Mit dem Protokoll wird dieses Ziel erreicht. Die Bestimmungen des Protokolls beschränken sich auf das zur Verwirklichung seiner wichtigsten Ziele erforderliche Maß. Einseitige Maßnahmen stellen keine Alternative dar, da sie keine ausreichende Grundlage für die Zusammenarbeit mit Drittländern bieten und den erforderlichen Schutz der Grundrechte nicht gewährleisten könnten. Zudem ist es effizienter, einer multilateralen Übereinkunft wie dem von der Union ausgehandelten Protokoll beizutreten, als auf bilateraler Ebene Verhandlungen mit einzelnen Drittländern aufzunehmen. Vorausgesetzt, dass alle 66 Vertragsparteien des Übereinkommens sowie künftige neue Vertragsparteien das Protokoll ratifizieren, wird das Protokoll einen gemeinsamen Rechtsrahmen für die Zusammenarbeit der EU-Mitgliedstaaten mit ihren wichtigsten internationalen Partnern bei der Verbrechensbekämpfung schaffen.

- ***Wahl des Instruments***

Entfällt.

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

- *Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften*

Entfällt.

- *Konsultation der Interessenträger*

Im Zusammenhang mit den Verhandlungen über das Protokoll organisierte der Europarat sechs öffentliche Konsultationsrunden: im Juli und November 2018, im Februar und November 2019, im Dezember 2020 und im Mai 2021.[42] Die im Rahmen dieser Konsultationen eingegangenen Beiträge wurden von den Vertragsparteien berücksichtigt.

In ihrer Rolle als Verhandlungsführerin im Namen der Union tauschte sich die Kommission auch mit Datenschutzbehörden aus und organisierte in den Jahren 2019 und 2021 gezielte Konsultationssitzungen mit Organisationen der Zivilgesellschaft, Diensteanbietern und Berufsverbänden. Die im Rahmen dieses Austauschs eingegangenen Beiträge wurden von der Kommission berücksichtigt.

- *Einholung und Nutzung von Expertenwissen*

Im Einklang mit dem Beschluss des Rates der Europäischen Union vom 6. Juni 2019, mit dem die Kommission ermächtigt wurde, im Namen der Union an den Verhandlungen teilzunehmen, hat die Kommission während der Verhandlungen konsequent den Sonderausschuss des Rates für die Verhandlungen konsultiert und damit Sachverständigen der Mitgliedstaaten Gelegenheit gegeben, zur Formulierung des Standpunkts der Union beizutragen. Eine Reihe von Sachverständigen der Mitgliedstaaten nahm auch an den Verhandlungen teil, parallel zur Kommission, die im Namen der Union teilnahm. Ferner wurden die Interessenträger konsultiert (siehe oben).

- *Folgenabschätzung*

Zu den Vorschlägen der Kommission zu elektronischen Beweismitteln wurde im Zeitraum 2017/2018 eine Folgenabschätzung vorgenommen.[43] In diesem Zusammenhang war die Herbeiführung einer Einigung über ein Zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität Teil der bevorzugten Option. Darüber hinaus sind die wichtigsten Auswirkungen in der vorliegenden Begründung dargelegt.

- *Effizienz der Rechtsetzung und Vereinfachung*

Das Protokoll kann Auswirkungen auf bestimmte Kategorien von Diensteanbietern haben, darunter kleine und mittlere Unternehmen (KMU), da nach dem Protokoll Ersuchen und Anordnungen für elektronische Beweismittel an sie gerichtet werden können. Solche Ersuchen werden jedoch häufig bereits heute an diese Diensteanbieter gerichtet – über andere bestehende Kanäle, manchmal über verschiedene Behörden und auch auf der Grundlage des Übereinkommens[44], anderer Verträge über gegenseitige Rechtshilfe oder anderer Rahmenregelungen, darunter Multi-Stakeholder-Strategien im Bereich der Internet-

[42] https://www.coe.int/en/web/cybercrime/protocol-consultations

[43] SWD(2018) 118 final.

[44] Siehe z. B. Leitfaden 10 des Ausschusses für das Übereinkommen über Computerkriminalität vom 1. März 2017 zu Herausgabeanordnungen in Bezug auf Bestandsdaten (Artikel 18 des Budapester Übereinkommens).

Governance[45]. Auch die Diensteanbieter – einschließlich KMU – werden von einem klaren Rechtsrahmen auf internationaler Ebene und einem gemeinsamen Ansatz aller Vertragsparteien des Protokolls profitieren.

- *Grundrechte*

Die im Protokoll vorgesehenen Instrumente für die Zusammenarbeit können sich auf die Grundrechte auswirken, wenn Daten einer Person im Rahmen eines Strafverfahrens beschaffen werden können, unter anderem auf das Recht auf ein faires Verfahren, das Recht auf Privatsphäre und das Recht auf Schutz personenbezogener Daten. Das Protokoll verfolgt einen rechtebasierten Ansatz und sieht Voraussetzungen und Garantien vor, die mit den internationalen Menschenrechtsinstrumenten, unter anderem der Konvention des Europarats von 1950 zum Schutze der Menschenrechte und Grundfreiheiten, im Einklang stehen. Insbesondere sieht das Protokoll spezifische Datenschutzgarantien vor. Wo erforderlich, bietet das Protokoll den Vertragsparteien auch eine Grundlage für bestimmte Vorbehalte, Erklärungen oder Notifikationen und enthält Gründe, die es ermöglichen, eine Zusammenarbeit, um die ersucht wird, in bestimmten Situationen abzulehnen. Dadurch wird die Vereinbarkeit des Protokolls mit der Charta der Grundrechte der Europäischen Union gewährleistet.

5. AUSWIRKUNGEN AUF DEN HAUSHALT

Es ergeben sich keine Auswirkungen auf den Unionshaushalt. Für die Mitgliedstaaten können einmalige Kosten für die Durchführung des Protokolls anfallen, und den Behörden der Mitgliedstaaten könnten aufgrund des erwarteten Anstiegs der Zahl der Fälle höhere Kosten entstehen.

6. WEITERE ANGABEN

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

Es gibt keinen Durchführungsplan, da die Mitgliedstaaten nach der Unterzeichnung und Ratifizierung des Protokolls verpflichtet sind, das Protokoll durchzuführen.

Was das Monitoring anbelangt, so nimmt die Kommission an den Sitzungen des Ausschusses für das Übereinkommen über Computerkriminalität teil, in dem die Europäische Union als Beobachterorganisation anerkannt ist.

[45] Siehe z. B. die Entschließung des Vorstands der Zentralstelle für die Vergabe von Internet-Namen und -Adressen (ICANN) vom 15. Mai 2019 zu den Empfehlungen für eine Temporäre Spezifikation für gTLD-Registrierungsdaten, abrufbar unter www.icann.org.

2021/0382 (NLE)

Vorschlag für einen

BESCHLUSS DES RATES

zur Ermächtigung der Mitgliedstaaten, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials zu unterzeichnen

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16, Artikel 82 Absatz 1 und Artikel 218 Absatz 5,

auf Vorschlag der Europäischen Kommission,

in Erwägung nachstehender Gründe:

(1) Am 9. Juni 2019 ermächtigte der Rat die Kommission, im Namen der Union an den Verhandlungen über das Zweite Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität teilzunehmen.

(2) Der Wortlaut des Zweiten Zusatzprotokolls zum Übereinkommen über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials (im Folgenden „Protokoll“) wurde vom Ministerkomitee des Europarats am 17. November 2021 angenommen und soll im März 2022 zur Unterzeichnung aufgelegt werden.

(3) Die Bestimmungen des Protokolls gehören zu einem Bereich, der weitgehend Gegenstand gemeinsamer Vorschriften im Sinne des Artikels 3 Absatz 2 AEUV ist, darunter Instrumente zur Erleichterung der justiziellen Zusammenarbeit in Strafsachen, die Mindeststandards für Verfahrensrechte gewährleisten, sowie Garantien für den Datenschutz und den Schutz der Privatsphäre.

(4) Die Kommission hat auch Legislativvorschläge für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM(2018) 225 final) und für eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren (COM(2018) 226 final) vorgelegt, mit denen verbindliche europäische Herausgabe- und Sicherungsanordnungen eingeführt werden, die unmittelbar an einen Vertreter eines Diensteanbieters in einem anderen Mitgliedstaat zu richten sind.

(5) Mit ihrer Teilnahme an den Verhandlungen im Namen der Union hat die Kommission sichergestellt, dass das Zweite Zusatzprotokoll mit den einschlägigen gemeinsamen Vorschriften der Europäischen Union vereinbar ist.

(6) Damit die Vereinbarkeit des Protokolls mit den Rechtsvorschriften und Strategien der Union sowie die einheitliche Anwendung des Protokolls durch die EU-Mitgliedstaaten in ihren Beziehungen zu nicht der EU angehörenden Vertragsparteien und die wirksame Anwendung des Protokolls gewährleistet sind, ist eine Reihe von Vorbehalten, Erklärungen, Notifikationen und Mitteilungen von Belang.

(7) Da das Protokoll zügige Verfahren zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln und ein hohes Maß an Garantien vorsieht, wird sein Inkrafttreten zur Bekämpfung der Computerkriminalität und anderer Formen der Kriminalität auf globaler Ebene beitragen, indem es die Zusammenarbeit zwischen den Vertragsparteien des Protokolls, die EU-Mitgliedstaaten sind, und denen, die keine EU-Mitgliedstaaten sind, erleichtert, ein hohes Schutzniveau für den Einzelnen gewährleisten und möglichen Rechtskollisionen begegnen.

(8) Da das Protokoll geeignete Garantien vorsieht, die den Anforderungen für internationale Übermittlungen personenbezogener Daten nach der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 entsprechen, wird sein Inkrafttreten zur weltweiten Verbreitung der Datenschutzstandards der Union beitragen, den Datenverkehr zwischen den Vertragsparteien des Protokolls, die EU-Mitgliedstaaten sind, und denen, die keine EU-Mitgliedstaaten sind, erleichtern, und die Erfüllung der Verpflichtungen der EU-Mitgliedstaaten aus den Datenschutzvorschriften der Union gewährleisten.

(9) Durch ein zeitnahes Inkrafttreten wird auch der Stellenwert des Budapester Übereinkommens des Europarats als wichtigster multilateraler Rahmen für die Bekämpfung der Computerkriminalität bestätigt.

(10) Die Europäische Union kann nicht Vertragspartei des Protokolls werden, da sowohl das Protokoll als auch das Übereinkommen des Europarats über Computerkriminalität nur Staaten offensteht.

(11) Die Mitgliedstaaten sollten daher ermächtigt werden, das Protokoll im Interesse der Europäischen Union gemeinsam zu unterzeichnen.

(12) Die Mitgliedstaaten werden aufgefordert, das Protokoll während der feierlichen Unterzeichnung oder so bald wie möglich danach zu unterzeichnen.

(13) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates angehört und hat am … eine Stellungnahme abgegeben.

(14) [Nach den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts und unbeschadet des Artikels 4 dieses Protokolls beteiligt sich Irland nicht an der Annahme dieses Beschlusses, der daher weder für Irland bindend noch Irland gegenüber anwendbar ist.]

[ODER]

[Nach den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts und unbeschadet des Artikels 4 dieses Protokolls hat Irland [mit Schreiben vom …] mitgeteilt, dass es sich an der Annahme und Anwendung dieses Beschlusses beteiligen möchte.]

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

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Die Mitgliedstaaten werden ermächtigt, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials (im Folgenden „Protokoll“) zu unterzeichnen.

Artikel 2

Bei der Unterzeichnung des Protokolls legen die Mitgliedstaaten die Vorbehalte, Erklärungen, Notifikationen und Mitteilungen vor, die im Anhang aufgeführt sind.

Artikel 3

Dieser Beschluss tritt am Tag seiner Annahme in Kraft.

Artikel 4

Dieser Beschluss wird im Amtsblatt der Europäischen Union veröffentlicht.

Artikel 5

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am […]

Im Namen des Rates
Der Präsident/die Präsidentin