EUROPÄISCHE
KOMMISSION

Brüssel, den 25.11.2021
COM(2021) 719 final

2021/0383 (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 ratifizieren

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 ratifizieren.[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.

Dieser Vorschlag ergänzt einen gesonderten Vorschlag der Kommission für einen Beschluss des Rates der Europäischen Union (im Folgenden „Rat“), mit dem die Mitgliedstaaten ermächtigt werden, das Protokoll im Interesse der Europäischen Union zu unterzeichnen.

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 Straftaten, die mittels Nutzung von Rechnernetzen begangen werden, zu erleichtern. Erstens

[1] Der Wortlaut des Protokolls ist diesem Vorschlag 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.

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 und eine zeitnahe Ratifikation 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 Ratifikation 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 6 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 Ratifikation 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.

2021/0383 (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 ratifizieren

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 6,

auf Vorschlag der Europäischen Kommission,

nach Zustimmung des Europäischen Parlaments,

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 ratifizieren.

(12) 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.

(13) [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.]

(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. 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 ratifizieren.

Artikel 2

Bei der Ratifikation 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

EUROPÄISCHE
KOMMISSION

Brüssel, den 25.11.2021
COM(2021) 719 final

ANNEX 1

ANHANG

des

Vorschlags 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 ratifizieren

ANHANG

Bei der Ratifikation des Protokolls legen die Mitgliedstaaten im Interesse der Union die folgenden Vorbehalte, Erklärungen, Notifikationen, Mitteilungen und sonstigen Erwägungen vor.

1. VORBEHALTE

Das Zweite Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials (im Folgenden „Protokoll“) gestattet einer Vertragspartei, nach Artikel 19 Absatz 1 zu erklären, dass sie von Vorbehalten Gebrauch macht, die in Bezug auf eine Reihe von Artikeln des Protokolls vorgesehen sind.

Die Mitgliedstaaten sehen davon ab, sich das Recht vorzubehalten, Artikel 7 (Weitergabe von Bestandsdaten) nach Artikel 7 Absatz 9 Buchstabe a nicht anzuwenden.

Die Mitgliedstaaten sehen davon ab, sich das Recht vorzubehalten, Artikel 7 (Weitergabe von Bestandsdaten) nach Artikel 7 Absatz 9 Buchstabe b nicht auf bestimmte Arten von Zugangsnummern anzuwenden.

Die Mitgliedstaaten werden aufgefordert, davon abzusehen, sich das Recht vorzubehalten, Artikel 8 (Durchführung von Anordnungen einer anderen Vertragspartei) nach Artikel 8 Absatz 13 nicht auf Verkehrsdaten anzuwenden.

In den Fällen, in denen Artikel 19 Absatz 1 eine Grundlage für andere Vorbehalte bietet, sind die Mitgliedstaaten ermächtigt, eigene Vorbehalte zu prüfen und anzubringen.

2. ERKLÄRUNGEN

Das Protokoll gestattet einer Vertragspartei ferner, nach Artikel 19 Absatz 2 eine Erklärung in Bezug auf eine Reihe von Artikeln des Protokolls abzugeben.

Die Mitgliedstaaten geben die Erklärung nach Artikel 7 Absatz 2 Buchstabe b ab, dass gegenüber Diensteanbietern in ihrem Hoheitsgebiet erlassene Anordnungen 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 müssen. Die Mitgliedstaaten geben daher bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde die folgende Erklärung ab:

> *„Die Anordnung nach Artikel 7 Absatz 1 muss 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.“*

Die Mitgliedstaaten werden aufgefordert, davon abzusehen, nach Artikel 9 Absatz 1 Buchstabe b zu 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.

In den Fällen, in denen Artikel 19 Absatz 2 eine Grundlage für andere Erklärungen bietet, sind die Mitgliedstaaten ermächtigt, eigene Erklärungen zu prüfen und abzugeben.

3. ERKLÄRUNGEN, NOTIFIKATIONEN ODER MITTEILUNGEN

Zudem schreibt das Protokoll vor, dass eine Vertragspartei nach Artikel 19 Absatz 3 Erklärungen, Notifikationen oder Mitteilungen in Bezug auf eine Reihe von Artikeln des Protokolls abgibt.

Die Mitgliedstaaten notifizieren, dass die Vertragspartei, wenn eine Anordnung nach Artikel 7 Absatz 1 an einen Diensteanbieter in ihrem Hoheitsgebiet gerichtet wird, eine zeitgleiche Benachrichtigung über die Anordnung, die ergänzenden Angaben und eine Zusammenfassung des mit den Ermittlungen oder dem Verfahren in Zusammenhang stehenden Sachverhalts nach Artikel 7 Absatz 5 Buchstabe a verlangt. Die Mitgliedstaaten übermitteln daher der Generalsekretärin beziehungsweise dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde die folgende Notifikation:

> *„Wenn eine Anordnung nach Artikel 7 Absatz 1 an einen Diensteanbieter im Hoheitsgebiet [des Mitgliedstaats] gerichtet wird, verlangen wir in jedem Fall eine zeitgleiche Benachrichtigung über die Anordnung, die ergänzenden Angaben und eine Zusammenfassung des mit den Ermittlungen oder dem Verfahren in Zusammenhang stehenden Sachverhalts.“*

Nach Artikel 7 Absatz 5 Buchstabe e bestimmen die Mitgliedstaaten für die Entgegennahme von Benachrichtigungen nach Artikel 7 Absatz 5 Buchstabe a und die Durchführung der in Absatz 5 Buchstaben b, c und d bezeichneten Maßnahmen eine einzige Behörde und teilen die Kontaktdaten dieser Behörde mit.

Die Mitgliedstaaten erklären nach Artikel 8 Absatz 4, dass für die Erfüllung einer Anordnung nach Artikel 8 Absatz 1 zusätzliche begleitende Angaben erforderlich sind. Die Mitgliedstaaten geben daher bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde die folgende Erklärung ab:

> *„Für die Erfüllung einer Anordnung nach Artikel 8 Absatz 1 sind zusätzliche begleitende Angaben erforderlich. Welche zusätzlichen begleitenden Informationen erforderlich sind, hängt von den Umständen der Anordnung und der damit in Zusammenhang stehenden Ermittlungen oder Verfahren ab.“*

Die Mitgliedstaaten teilen die Kontaktdaten der nach Artikel 8 Absatz 10 Buchstabe a für die Vorlage einer Anordnung nach Artikel 8 benannten Behörden und der nach Artikel 8 Absatz 10 Buchstabe b für die Entgegennahme einer Anordnung nach Artikel 8 benannten Behörden mit und aktualisieren sie laufend. Die Mitgliedstaaten, die sich an der Verstärkten Zusammenarbeit nach der Verordnung (EU) 2017/1939 zur Durchführung einer Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft (EUStA) beteiligen, nehmen die EUStA bei der Ausübung ihrer Zuständigkeiten nach den Artikeln 22, 23 und 25 der Verordnung (EU) 2017/1939 in die Liste der Behörden auf, die nach Artikel 8 Absatz 10 Buchstaben a und b mitgeteilt werden.

Die Mitgliedstaaten teilen mit, welche Behörden nach Artikel 14 Absatz 7 Buchstabe c im Zusammenhang mit einem Sicherheitsvorfall zu benachrichtigen sind.

Die Mitgliedstaaten teilen die Behörden mit, die die Genehmigung für die Zwecke des Artikels 14 Absatz 10 Buchstabe b in Bezug auf die Weiterübermittlung von nach dem Protokoll empfangenen Daten an einen anderen Staat oder eine internationale Organisation erteilen können.

In den Fällen, in denen Artikel 19 Absatz 3 eine Grundlage für andere Erklärungen, Notifikationen oder Mitteilungen bietet, sind die Mitgliedstaaten ermächtigt, eigene Erklärungen, Notifikationen oder Mitteilungen zu prüfen und abzugeben.

4. SONSTIGE ERWÄGUNGEN

Die Mitgliedstaaten, die sich an der Verstärkten Zusammenarbeit nach der Verordnung (EU) 2017/1939 zur Durchführung einer Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft (EUStA) beteiligen, stellen sicher, 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.

Die Mitgliedstaaten stellen sicher, dass die empfangende Vertragspartei bei der Übermittlung von Daten für die Zwecke des Protokolls darüber unterrichtet wird, dass ihr innerstaatliches Recht eine persönliche Information der Person, deren Daten zur Verfügung gestellt wurden, nach Artikel 14 Absatz 11 Buchstabe c des Protokolls erfordert.

In Bezug auf internationale Übermittlungen auf der Grundlage des Rahmenabkommens zwischen der EU und den USA teilen die Mitgliedstaaten den zuständigen Behörden der Vereinigten Staaten für die Zwecke des Artikels 14 Absatz 1 Buchstabe b des Protokolls mit, dass das Abkommen für die gegenseitigen Übermittlungen personenbezogener Daten nach dem Protokoll zwischen zuständigen Behörden gilt. Die Mitgliedstaaten berücksichtigen jedoch, dass das Abkommen 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 tragen. Die Mitgliedstaaten übermitteln daher den zuständigen Behörden der Vereinigten Staaten bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde die folgende Mitteilung:

> *„Für die Zwecke des Artikels 14 Absatz 1 Buchstabe b des Zweiten Zusatzprotokolls zum Übereinkommen des Europarats über Computerkriminalität sind wir der Auffassung, dass das Rahmenabkommen zwischen der EU und den USA für die gegenseitigen Übermittlungen personenbezogener Daten nach dem Protokoll zwischen zuständigen Behörden gilt. Für Übermittlungen nach dem Protokoll zwischen Diensteanbietern in unserem Hoheitsgebiet und Behörden in den Vereinigten Staaten gilt das Abkommen nur in Verbindung mit einer weiteren, spezifischen Übermittlungsvereinbarung, die den besonderen Anforderungen an eine Übermittlung elektronischer Beweismittel, die direkt durch Diensteanbieter und nicht zwischen Behörden erfolgt, Rechnung trägt.“*

Die Mitgliedstaaten stellen sicher, dass sie sich für die Zwecke des Artikels 14 Absatz 1 Buchstabe c des Protokolls nur dann auf andere Übereinkünfte oder Vereinbarungen stützen, 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 geeignete Datenschutzgarantien nach Artikel 46 der Datenschutz-Grundverordnung oder Artikel 37 Absatz 1 Buchstabe a der Richtlinie zum Datenschutz bei der Strafverfolgung bietet.

EUROPÄISCHE
KOMMISSION

Brüssel, den 25.11.2021
COM(2021) 719 final

ANNEX 2

ANHANG

des

Vorschlags 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

ANHANG

ZWEITES ZUSATZPROTOKOLL ZUM ÜBEREINKOMMEN ÜBER COMPUTERKRIMINALITÄT ÜBER EINE VERSTÄRKTE ZUSAMMENARBEIT UND DIE WEITERGABE ELEKTRONISCHEN BEWEISMATERIALS

PRÄAMBEL

Die Mitgliedstaaten des Europarats und die anderen Vertragsstaaten des am 23. November 2001 in Budapest zur Unterzeichnung aufgelegten Übereinkommens über Computerkriminalität (SEV Nr. 185, im Folgenden „Übereinkommen“), die dieses Protokoll unterzeichnen –

eingedenk der Reichweite und Wirkung des Übereinkommens weltweit,

im Hinblick darauf, dass das Übereinkommen für die Vertragsparteien des entsprechenden Protokolls bereits durch das am 28. Januar 2003 in Straßburg zur Unterzeichnung aufgelegte Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art (SEV Nr. 189, im Folgenden „Erstes Zusatzprotokoll“) ergänzt wurde,

unter Berücksichtigung bestehender Verträge des Europarats über die Zusammenarbeit in Strafsachen sowie sonstiger Übereinkünfte und Vereinbarungen über die Zusammenarbeit in Strafsachen zwischen den Vertragsparteien des Übereinkommens,

im Hinblick auch auf das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) in der durch das am 10. Oktober 2018 in Straßburg zur Unterzeichnung aufgelegte Änderungsprotokoll (SEV Nr. 223) geänderten Fassung, zu dessen Beitritt jeder Staat eingeladen werden kann,

angesichts der zunehmenden Nutzung von Informations- und Kommunikationstechnik einschließlich Internetdiensten sowie wachsender Computerkriminalität, die eine Bedrohung für Demokratie und Rechtsstaatlichkeit und nach Auffassung vieler Staaten auch eine Bedrohung für die Menschenrechte darstellt,

auch angesichts der steigenden Zahl an Opfern von Computerkriminalität und der Wichtigkeit, ihnen zu ihrem Recht zu verhelfen,

im Hinblick darauf, dass Regierungen in der Verantwortung stehen, die Gesellschaft und den einzelnen Menschen nicht nur offline, sondern auch online vor Straftaten zu schützen, auch mithilfe wirksamer strafrechtlicher Ermittlungen und Strafverfolgungsmaßnahmen,

in dem Bewusstsein, dass Beweismaterial zu Straftaten zunehmend in elektronischer Form auf Computersystemen in ausländischen, mehreren oder unbekannten Rechtsordnungen gespeichert ist, und in der Überzeugung, dass zusätzliche Maßnahmen erforderlich sind, um solches Beweismaterial rechtmäßig zu erlangen, damit eine wirksame Strafverfolgung ermöglicht wird und die Rechtsstaatlichkeit gewahrt bleibt,

in der Erkenntnis, dass eine verstärkte und effizientere Zusammenarbeit zwischen Staaten und dem Privatsektor und in diesem Zusammenhang mehr Klarheit beziehungsweise Rechtssicherheit für Diensteanbieter und sonstige Stellen hinsichtlich der Umstände, unter denen sie Ersuchen um Weitergabe elektronischer Daten vonseiten der Strafverfolgungsbehörden aus anderen Vertragsstaaten unmittelbar nachkommen dürfen, erforderlich ist,

dementsprechend mit dem Ziel einer weiteren Verstärkung der Zusammenarbeit auf dem Gebiet der Computerkriminalität und bei der Erhebung von Beweismaterial in elektronischer Form zu allen Arten von Straftaten für die Zwecke spezifischer strafrechtlicher Ermittlungen oder Verfahren durch zusätzliche Instrumente mit Bezug auf eine effizientere Rechtshilfe und sonstige Formen der Zusammenarbeit zwischen den zuständigen Behörden, durch Zusammenarbeit in Notfällen und durch direkte Zusammenarbeit zwischen den zuständigen Behörden und den Diensteanbietern sowie sonstigen Stellen, in deren Besitz oder unter deren Kontrolle sich relevante Informationen befinden,

in der Überzeugung, dass wirksame Bedingungen und Garantien für den Schutz der Menschenrechte und Grundfreiheiten eine wirksame grenzüberschreitende Zusammenarbeit im strafrechtlichen Bereich, auch zwischen dem öffentlichen und dem privaten Sektor, begünstigen,

in der Erkenntnis, dass bei der Erhebung elektronischen Beweismaterials für strafrechtliche Ermittlungen häufig personenbezogene Daten betroffen sind und dass viele Vertragsstaaten den Schutz von Privatsphäre und personenbezogenen Daten gewährleisten müssen, um ihren verfassungsrechtlichen und internationalen Verpflichtungen nachzukommen, und

mit Rücksicht darauf, dass für wirksame Strafverfolgungsmaßnahmen in Bezug auf Computerkriminalität und für die Erhebung von Beweismaterial in elektronischer Form Bedingungen und Garantien gelten müssen, die einen angemessenen Schutz der Menschenrechte und Grundfreiheiten vorsehen, einschließlich der Rechte, die sich aus den Verpflichtungen der Staaten nach geltenden internationalen Menschenrechtsinstrumenten ergeben, wie der Konvention des Europarats zum Schutz der Menschenrechte und Grundfreiheiten von 1950 (SEV Nr. 5), des Internationalen Pakts der Vereinten Nationen über bürgerliche und politische Rechte von 1966, der Afrikanischen Charta der Menschenrechte und Rechte der Völker von 1981, der Amerikanischen Menschenrechtskonvention von 1969 und weiterer völkerrechtlicher Verträge auf dem Gebiet der Menschenrechte –

sind wie folgt übereingekommen:

KAPITEL I – ALLGEMEINE BESTIMMUNGEN

Artikel 1 – Zweck

Dieses Protokoll hat zum Zweck,

a) das Übereinkommen für die Vertragsparteien dieses Protokolls zu ergänzen, und

b) das Erste Zusatzprotokoll für die Vertragsparteien des vorliegenden Protokolls, die auch Vertragsparteien des Ersten Zusatzprotokolls sind, zu ergänzen.

Artikel 2 – Geltungsbereich

(1) Soweit in diesem Protokoll nichts anderes bestimmt ist, werden die hierin bezeichneten Maßnahmen

a) zwischen den Vertragsparteien des Übereinkommens, die Vertragsparteien dieses Protokolls sind, auf spezifische strafrechtliche Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten und auf die Erhebung von Beweismaterial in elektronischer Form für eine Straftat angewandt, und

b) zwischen den Vertragsparteien des Ersten Zusatzprotokolls, die Vertragsparteien des vorliegenden Protokolls sind, auf spezifische strafrechtliche Ermittlungen oder Verfahren in Bezug auf Straftaten nach dem Ersten Zusatzprotokoll angewandt.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den in diesem Protokoll bezeichneten Verpflichtungen nachzukommen.

Artikel 3 – Begriffsbestimmungen

(1) Die Begriffsbestimmungen in Artikel 1 und Artikel 18 Absatz 3 des Übereinkommens gelten für dieses Protokoll.

(2) Im Sinne dieses Protokolls gelten die folgenden zusätzlichen Begriffsbestimmungen:

a) „zentrale Behörde“ bezeichnet die im Rahmen eines zwischen den betreffenden Vertragsparteien geltenden Rechtshilfevertrags oder einer zwischen den betreffenden Vertragsparteien geltenden, auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffenen Übereinkunft bestimmte Behörde beziehungsweise bestimmten Behörden, oder in Ermangelung dessen die von einer Vertragspartei nach Artikel 27 Absatz 2 Buchstabe a des Übereinkommens bestimmte Behörden beziehungsweise bestimmten Behörden;

b) „zuständige Behörde“ bezeichnet eine Justiz-, Verwaltungs- oder sonstige Strafverfolgungsbehörde, die nach innerstaatlichem Recht ermächtigt ist, Maßnahmen im Sinne dieses Protokolls für Zwecke der Erhebung oder Herausgabe von Beweismaterial in Bezug auf spezifische strafrechtliche Ermittlungen oder Verfahren anzuordnen, zu bewilligen oder durchzuführen;

c) „Notfall“ bezeichnet eine Lage, in der eine erhebliche und unmittelbare Gefahr für das Leben oder die Sicherheit einer natürlichen Person besteht;

d) „personenbezogene Daten“ bezeichnet Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen;

e) „übermittelnde Vertragspartei“ bezeichnet die Vertragspartei, die die Daten im Rahmen der Erledigung eines Ersuchens oder einer gemeinsamen Ermittlungsgruppe übermittelt, oder, für die Zwecke von Kapitel II Abschnitt 2, eine Vertragspartei, in deren Hoheitsgebiet sich ein übermittelnder Diensteanbieter oder eine Stelle, die Domänennamenregistrierungsdienste bereitstellt, befindet.

Artikel 4 – Sprache

(1) Ersuchen, Anordnungen und begleitende Angaben sind einer ersuchten Vertragspartei oder einer nach Artikel 7 Absatz 5 benachrichtigten Vertragspartei in einer für sie annehmbaren Sprache vorzulegen oder ihnen ist eine Übersetzung in eine solche Sprache beizufügen.

(2) Anordnungen nach Artikel 7 und Ersuchen nach Artikel 6 sowie begleitende Angaben müssen

a) in einer Sprache der anderen Vertragspartei, in der der Diensteanbieter oder die Stelle vergleichbare innerstaatliche Abläufe entgegennimmt, vorgelegt werden,

b) in einer anderen für den Diensteanbieter oder die Stelle annehmbaren Sprache vorgelegt werden, oder

c) ihnen ist eine Übersetzung in eine der Sprachen nach Buchstabe a oder b beizufügen.

KAPITEL II – MAßNAHMEN FÜR EINE VERSTÄRKTE ZUSAMMENARBEIT

Abschnitt 1 – Allgemeine Grundsätze für Kapitel II

Artikel 5 – Allgemeine Grundsätze für Kapitel II

(1) Die Vertragsparteien arbeiten nach Maßgabe dieses Kapitels im größtmöglichen Umfang zusammen.

(2) Abschnitt 2 dieses Kapitels besteht aus den Artikeln 6 und 7. Er sieht Verfahren zur Verstärkung der unmittelbaren Zusammenarbeit mit Anbietern und Stellen im Hoheitsgebiet einer anderen Vertragspartei vor. Abschnitt 2 findet unabhängig davon Anwendung, ob zwischen den betreffenden Vertragsparteien ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, in Kraft ist.

(3) Abschnitt 3 dieses Kapitels besteht aus den Artikeln 8 und 9. Er sieht Verfahren zur Verstärkung der internationalen Zusammenarbeit zwischen Behörden zur Weitergabe gespeicherter Computerdaten vor. Abschnitt 3 findet unabhängig davon Anwendung, ob zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, in Kraft ist.

(4) Abschnitt 4 dieses Kapitels besteht aus Artikel 10. Er sieht Verfahren für Rechtshilfe in Notfällen vor. Abschnitt 4 findet unabhängig davon Anwendung, ob zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, in Kraft ist.

(5) Abschnitt 5 dieses Kapitels besteht aus den Artikeln 11 und 12. Abschnitt 5 findet Anwendung, sofern zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, nicht in Kraft ist. Vorbehaltlich des Artikels 12 Absatz 7 findet Abschnitt 5 keine Anwendung, wenn ein solcher Vertrag oder eine solche Übereinkunft besteht. Die betreffenden Vertragsparteien können jedoch einvernehmlich bestimmen, dass stattdessen Abschnitt 5 anzuwenden ist, sofern dies nach dem Vertrag oder der Übereinkunft nicht untersagt ist.

(6) Darf die ersuchte Vertragspartei nach diesem Protokoll die Zusammenarbeit von der Bedingung abhängig machen, dass die beiderseitige Strafbarkeit gegeben ist, so gilt, gleichviel, ob die Straftat nach ihrem Recht in dieselbe Kategorie von Straftaten fällt oder mit dem gleichen Begriff benannt ist wie nach dem Recht der ersuchenden Vertragspartei, diese Bedingung als erfüllt, wenn die Handlung, die der Straftat, derentwegen um Rechtshilfe ersucht wird, zugrunde liegt, nach ihrem Recht eine Straftat darstellt.

(7) Die Zusammenarbeit zwischen Vertragsparteien oder zwischen Vertragsparteien und Diensteanbietern oder sonstigen Stellen nach anderen anwendbaren Übereinkünften,

Vereinbarungen, Verfahrensweisen oder nach anwendbarem innerstaatlichem Recht wird durch dieses Kapitel nicht beschränkt.

Abschnitt 2 – Verfahren zur Verstärkung der unmittelbaren Zusammenarbeit mit Anbietern und Stellen in anderen Vertragsstaaten

Artikel 6 – Ersuchen um Registrierungsinformationen zu Domänennamen

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen, für die Zwecke spezifischer strafrechtlicher Ermittlungen oder Verfahren an eine Stelle, die Domänennamenregistrierungsdienste im Hoheitsgebiet einer anderen Vertragspartei bereitstellt, ein Ersuchen um Informationen, die sich im Besitz oder unter der Kontrolle der Stelle befinden, zu richten, um den Domäneninhaber zu identifizieren oder zu kontaktieren.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um einer Stelle in ihrem Hoheitsgebiet zu gestatten, unter Beachtung der nach innerstaatlichem Recht vorgesehenen angemessenen Bedingungen derlei Informationen zur Erledigung eines Ersuchens nach Absatz 1 weiterzugeben.

(3) Das Ersuchen nach Absatz 1 umfasst:

a) das Datum, an dem das Ersuchen gestellt wurde, und die Identität und Kontaktdaten der zuständigen Behörde, die das Ersuchen stellt,

b) den Domänennamen, zu dem Informationen angefordert werden, und eine genaue Auflistung der erbetenen Informationen einschließlich der einzelnen Datenelemente,

c) eine Erklärung, dass das Ersuchen nach Maßgabe dieses Protokolls gestellt wird, dass die Informationen aufgrund ihrer Relevanz für spezifische strafrechtliche Ermittlungen oder Verfahren benötigt werden und dass die Informationen nur für diese spezifischen strafrechtlichen Ermittlungen oder Verfahren verwendet werden, und

d) den vorgesehenen zeitlichen Rahmen und die vorgesehene Art und Weise der Weitergabe der Informationen sowie sonstige besondere Verfahrensanweisungen.

(4) Sofern dies für die Stelle annehmbar ist, kann eine Vertragspartei ein Ersuchen nach Absatz 1 in elektronischer Form vorlegen. Die Einhaltung angemessener Sicherheits- und Authentifizierungsstandards kann verlangt werden.

(5) Lehnt eine in Absatz 1 bezeichnete Stelle die Zusammenarbeit ab, kann eine ersuchende Vertragspartei die Stelle darum ersuchen zu begründen, warum sie die angeforderten Informationen nicht weitergibt. Die ersuchende Vertragspartei kann sich um Konsultation mit dem Vertragsstaat, in dem sich die Stelle befindet, bemühen, um verfügbare Maßnahmen zur Erlangung der Informationen zu bestimmen.

(6) Jede Vertragspartei teilt der Generalsekretärin beziehungsweise dem Generalsekretär des Europarats bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde oder zu jedem anderen Zeitpunkt die für Konsultationen nach Absatz 5 bestimmte Behörde mit.

(7) Die Generalsekretärin beziehungsweise der Generalsekretär des Europarats erstellt und aktualisiert ein Verzeichnis der von den Vertragsparteien nach Absatz 6 bestimmten Behörden. Jede Vertragspartei stellt sicher, dass die von ihr für das Verzeichnis bereitgestellten Angaben stets richtig sind.

Artikel 7 – Weitergabe von Bestandsdaten

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen, eine unmittelbar einem Diensteanbieter im Hoheitsgebiet einer anderen Vertragspartei vorzulegende Anordnung zu erlassen, um die Weitergabe bestimmter gespeicherter Bestandsdaten zu erwirken, die sich in seinem Besitz oder unter seiner Kontrolle befinden, sofern die Bestandsdaten für spezifische strafrechtliche Ermittlungen oder Verfahren der erlassenden Vertragspartei erforderlich sind.

(2) a) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, damit ein Diensteanbieter in ihrem Hoheitsgebiet zur Erledigung eines Ersuchens nach Absatz 1 Bestandsdaten weitergeben kann.

b) Bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde kann eine Vertragspartei – in Bezug auf gegenüber Diensteanbietern in ihrem Hoheitsgebiet erlassene Anordnungen – folgende Erklärung abgeben: „Die Anordnung nach Artikel 7 Absatz 1 muss 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.“

(3) In der Anordnung nach Absatz 1 sind anzugeben:

a) die erlassende Behörde und das Datum des Erlasses,

b) eine Erklärung, dass die Anordnung nach Maßgabe dieses Protokolls erlassen wird,

c) der Name und die Anschrift des Diensteanbieters beziehungsweise der Diensteanbieter, an den beziehungsweise die sich die Anordnung richtet,

d) die Straftat beziehungsweise die Straftaten, die Gegenstand der strafrechtlichen Ermittlungen oder des strafrechtlichen Verfahrens ist beziehungsweise sind,

e) die Behörde, die die spezifischen Bestandsdaten anfordert, sofern es sich dabei nicht um die erlassende Behörde handelt, und

f) eine genaue Beschreibung der angeforderten spezifischen Bestandsdaten.

(4) Der Anordnung nach Absatz 1 sind folgende ergänzende Angaben beizufügen:

a) die innerstaatliche Rechtsgrundlage, nach der die Behörde zum Erlass der Anordnung ermächtigt ist,

b) ein Verweis auf die Rechtsvorschriften und den geltenden Strafrahmen für die Tat, die Gegenstand der Ermittlung oder der Strafverfolgung ist,

c) die Kontaktdaten der Behörde, an welche die Bestandsdaten durch den Diensteanbieter zu übermitteln sind, an die Nachfragen gerichtet werden können oder welcher der Diensteanbieter anderweitig zu antworten hat,

d) der zeitliche Rahmen und die Art und Weise der Übermittlung der Bestandsdaten,

e) die Angabe, ob bereits die Sicherung der Daten angefordert wurde, einschließlich des Sicherungsdatums und gegebenenfalls der Vorgangsnummer oder Vorgangsnummern,

f) sonstige besondere Verfahrenshinweise,

g) gegebenenfalls eine Erklärung, dass eine zeitgleiche Benachrichtigung nach Absatz 5 erfolgt ist, und

h) sonstige Informationen, die im Hinblick auf die Weitergabe der Bestandsdaten hilfreich sein können.

(5) Eine Vertragspartei kann bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde oder zu jedem anderen Zeitpunkt der Generalsekretärin beziehungsweise dem Generalsekretär des Europarats notifizieren, dass sie, wenn eine Anordnung nach Absatz 1 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.

b) Unabhängig davon, ob eine Vertragspartei nach Buchstabe a zu benachrichtigen ist, kann sie von dem Diensteanbieter verlangen, dass er unter bestimmten Umständen vor der Weitergabe ihre Behörden konsultiert.

c) Die nach Buchstabe a benachrichtigten oder nach Buchstabe b konsultierten Behörden können den Diensteanbieter ohne ungebührliche Verzögerung anweisen, die Bestandsdaten nicht weiterzugeben,

i) wenn die Weitergabe strafrechtliche Ermittlungen oder Verfahren in dieser Vertragspartei beeinträchtigen kann oder

ii) wenn Bedingungen oder Gründe für die Ablehnung nach Artikel 25 Absatz 4 und Artikel 27 Absatz 4 des Übereinkommens vorliegen würden, wenn die Bestandsdaten im Wege der Rechtshilfe angefordert worden wären.

d) Die nach Buchstabe a benachrichtigten oder nach Buchstabe b konsultierten Behörden

i) können für die Zwecke der Anwendung von Buchstabe c um zusätzliche Informationen von der in Absatz 4 Buchstabe c genannten Behörde ersuchen und dürfen diese dem Diensteanbieter ohne die Zustimmung dieser Behörde nicht weitergeben und

ii) unterrichten unter Darlegung der Gründe umgehend die in Absatz 4 Buchstabe c genannte Behörde darüber, falls der Diensteanbieter angewiesen wurde, die Bestandsdaten nicht weiterzugeben.

e) Eine Vertragspartei bestimmt für die Entgegennahme von Benachrichtigungen nach Buchstabe a und die Durchführung der in den Buchstaben b, c und d bezeichneten Maßnahmen eine einzige Behörde. Zum Zeitpunkt der ersten Notifikation an die Generalsekretärin beziehungsweise den Generalsekretär des Europarats nach Buchstabe a teilt die Vertragspartei der Generalsekretärin beziehungsweise dem Generalsekretär die Kontaktdaten dieser Behörde mit.

f) Die Generalsekretärin beziehungsweise der Generalsekretär des Europarats erstellt und aktualisiert ein Verzeichnis der nach Buchstabe e von den Vertragsparteien bestimmten Behörden und erfasst darin, ob und unter welchen Umständen sie eine Benachrichtigung nach Buchstabe a verlangen. Jede Vertragspartei stellt sicher, dass die von ihr für das Verzeichnis bereitgestellten Angaben stets richtig sind.

(6) Sofern dies für den Diensteanbieter annehmbar ist, kann eine Vertragspartei eine Anordnung nach Absatz 1 und ergänzende Angaben nach Absatz 4 in elektronischer Form vorlegen. Eine Vertragspartei kann Benachrichtigungen und zusätzliche Angaben nach Absatz 5 in elektronischer Form übermitteln. Die Einhaltung angemessener Sicherheits- und Authentifizierungsstandards kann verlangt werden.

(7) Unterrichtet ein Diensteanbieter die in Absatz 4 Buchstabe c bezeichnete Behörde darüber, dass er die angeforderten Bestandsdaten nicht weitergeben wird, oder gibt er die Bestandsdaten zur Erledigung einer Anordnung nach Absatz 1 nicht innerhalb von dreißig Tagen nach Eingang der Anordnung oder innerhalb des nach Absatz 4 Buchstabe d vorgesehenen zeitlichen Rahmens weiter, wobei jeweils der längere Zeitraum gilt, so können die zuständigen Behörden der erlassenden Vertragspartei die Durchführung der Anordnung anschließend nur noch anhand von Artikel 8 oder im Wege sonstiger Formen der Rechtshilfe anstreben. Die Vertragsparteien können darum ersuchen, dass ein Diensteanbieter begründet, warum er die in der Anordnung angeforderten Bestandsdaten nicht weitergibt.

(8) Eine Vertragspartei kann bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde erklären, dass eine erlassende Vertragspartei die Weitergabe der Bestandsdaten zunächst bei dem Diensteanbieter anzufordern hat, bevor sie diese anhand von Artikel 8 anfordert, es sei denn, die erlassende Vertragspartei begründet hinreichend, warum sie abweichend vorgeht.

(9) Bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde kann eine Vertragspartei

a) sich das Recht vorbehalten, diesen Artikel nicht anzuwenden, oder

b) sofern die Weitergabe bestimmter Arten von Zugangsnummern nach diesem Artikel mit den Grundprinzipien ihrer innerstaatlichen Rechtsordnung unvereinbar sein sollte, sich das Recht vorbehalten, diesen Artikel nicht auf solche Nummern anzuwenden.

Abschnitt 3 – Verfahren zur Verstärkung der internationalen Zusammenarbeit zwischen Behörden zur Weitergabe gespeicherter Computerdaten

Artikel 8 – Durchführung von Anordnungen einer anderen Vertragspartei auf umgehende Herausgabe von Bestandsdaten und Verkehrsdaten

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen, eine Anordnung zu erlassen, die im Rahmen eines an eine andere Vertragspartei gerichteten Ersuchens vorzulegen ist, um einen Diensteanbieter im Hoheitsgebiet der ersuchten Vertragspartei zu verpflichten, spezifische gespeicherte

a) Bestandsdaten und

b) Verkehrsdaten

herauszugeben, die sich im Besitz dieses Diensteanbieters oder unter seiner Kontrolle befinden und die für die spezifischen strafrechtlichen Ermittlungen oder Verfahren der Vertragspartei erforderlich sind.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen zur Durchführung einer durch eine ersuchende Vertragspartei vorgelegten Anordnung nach Absatz 1.

(3) Im Rahmen ihres Ersuchens legt die ersuchende Vertragspartei der ersuchten Vertragspartei die Anordnung nach Absatz 1, begleitende Angaben und sonstige besondere Verfahrensanweisungen vor.

a) In der Anordnung sind anzugeben:

i) die erlassende Behörde und das Datum der Anordnung,

ii) eine Erklärung, dass die Anordnung nach Maßgabe dieses Protokolls vorgelegt wird,

iii) der Name und die Anschrift des Diensteanbieters beziehungsweise der Diensteanbieter, an den beziehungsweise die sich die Anordnung richtet,

iv) die Straftat beziehungsweise die Straftaten, die Gegenstand der strafrechtlichen Ermittlungen oder des strafrechtlichen Verfahrens ist beziehungsweise sind,

v) die Behörde, welche die Informationen oder Daten anfordert, sofern es sich dabei nicht um die erlassende Behörde handelt, und

vi) eine genaue Beschreibung der angeforderten spezifischen Informationen oder Daten.

b) In den begleitenden Angaben, die bereitgestellt werden, um die ersuchte Vertragspartei bei der Durchführung der Anordnung zu unterstützen, und die dem Diensteanbieter nicht ohne die Zustimmung der ersuchenden Vertragspartei weitergegeben werden dürfen, sind anzugeben:

i) die innerstaatliche Rechtsgrundlage, nach der die Behörde zum Erlass der Anordnung ermächtigt ist,

ii) die Rechtsvorschriften und der geltende Strafrahmen für die Tat beziehungsweise die Taten, die Gegenstand der Ermittlung oder der Strafverfolgung ist beziehungsweise sind,

iii) eine Begründung, weshalb die ersuchende Vertragspartei der Auffassung ist, dass sich die Daten im Besitz des Diensteanbieters oder unter seiner Kontrolle befinden,

iv) eine Zusammenfassung des mit den Ermittlungen oder dem Verfahren in Zusammenhang stehenden Sachverhalts,

v) die Relevanz der Informationen oder Daten für die Ermittlungen oder das Verfahren,

vi) die Kontaktdaten einer Behörde oder mehrerer Behörden, die weitere Informationen zur Verfügung stellen können,

vii) die Angabe, ob bereits die Sicherung der Informationen oder Daten angefordert wurde, einschließlich des Sicherungsdatums und gegebenenfalls der Vorgangsnummer beziehungsweise Vorgangsnummern, und

viii) die Angabe, ob die Informationen oder Daten bereits auf anderem Wege angefordert wurden, und wenn ja, auf welche Weise.

c) Die ersuchende Vertragspartei kann darum ersuchen, dass die ersuchte Vertragspartei besondere Verfahrensanweisungen befolgt.

(4) Eine Vertragspartei kann bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde oder zu jedem anderen Zeitpunkt erklären, dass für die Erfüllung einer Anordnung nach Absatz 1 zusätzliche begleitende Angaben erforderlich sind.

(5) Die ersuchte Vertragspartei nimmt Ersuchen in elektronischer Form entgegen. Sie kann angemessene Sicherheits- und Authentifizierungsstandards verlangen, bevor dem Ersuchen stattgegeben wird.

(6) a) Die ersuchte Vertragspartei unternimmt angemessene Anstrengungen, damit die Zustellung an den Diensteanbieter spätestens binnen fünfundvierzig Tagen nach Eingang aller in den Absätzen 3 und 4 bezeichneten Informationen erfolgt, und ordnet die Übermittlung der angeforderten Informationen oder Daten spätestens

i) innerhalb von zwanzig Tagen an, wenn es sich um Bestandsdaten handelt, und

ii) innerhalb von fünfundvierzig Tagen an, wenn es sich um Verkehrsdaten handelt.

b) Die ersuchte Vertragspartei sorgt dafür, dass die herausgegebenen Informationen oder Daten der ersuchenden Vertragspartei ohne ungebührliche Verzögerung übermittelt werden.

(7) Kann die ersuchte Vertragspartei die Anweisungen nach Absatz 3 Buchstabe c nicht wie verlangt befolgen, so unterrichtet sie umgehend die ersuchende Vertragspartei und gibt gegebenenfalls an, unter welchen Bedingungen sie die Anweisungen befolgen könnte, woraufhin die ersuchende Vertragspartei entscheidet, ob das Ersuchen dennoch erledigt werden soll.

(8) Die ersuchte Vertragspartei kann die Erledigung eines Ersuchens aus den in Artikel 25 Absatz 4 oder in Artikel 27 Absatz 4 des Übereinkommens festgelegten Gründen ablehnen oder Bedingungen stellen, die sie zur Genehmigung der Erledigung des Ersuchens für erforderlich hält. Die ersuchte Vertragspartei kann die Erledigung von Ersuchen aus den in Artikel 27 Absatz 5 des Übereinkommens festgelegten Gründen aufschieben. Die ersuchte Vertragspartei benachrichtigt die ersuchende Vertragspartei so bald wie möglich über die Ablehnung, die Bedingungen oder den Aufschub. Die ersuchte Vertragspartei benachrichtigt die ersuchende Vertragspartei auch bezüglich sonstiger Umstände, die zu einer erheblichen Verzögerung bei der Erledigung des Ersuchens führen könnten. Artikel 28 Absatz 2 Buchstabe b des Übereinkommens findet auf diesen Artikel Anwendung.

(9) a) Kann die ersuchende Vertragspartei einer durch die ersuchte Vertragspartei nach Absatz 8 gestellten Bedingung nicht entsprechen, so unterrichtet sie umgehend die ersuchte Vertragspartei. Die ersuchte Vertragspartei entscheidet sodann, ob die Informationen oder Unterlagen dennoch zur Verfügung gestellt werden sollen.

b) Nimmt die ersuchende Vertragspartei die Bedingung an, so ist sie daran gebunden. Die ersuchte Vertragspartei, die Informationen oder Unterlagen unter einer solchen Bedingung zur Verfügung stellt, kann von der ersuchenden Vertragspartei verlangen, dass sie in Zusammenhang mit dieser Bedingung Angaben über die Verwendung der Informationen oder Unterlagen macht.

(10) Jede Vertragspartei teilt der Generalsekretärin beziehungsweise dem Generalsekretär des Europarats bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde die Kontaktdaten der Behörden mit – und aktualisiert diese laufend – die dazu bestimmt wurden,

a) eine Anordnung nach diesem Artikel vorzulegen und

b) eine Anordnung nach diesem Artikel entgegenzunehmen.

(11) Eine Vertragspartei kann bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde erklären, dass ihr Ersuchen anderer Vertragsparteien nach diesem Artikel durch die zentrale Behörde der ersuchenden Vertragspartei oder eine andere einvernehmlich bestimmte Behörde vorzulegen sind.

(12) Die Generalsekretärin beziehungsweise der Generalsekretär des Europarats erstellt und aktualisiert ein Verzeichnis der von den Vertragsparteien nach Absatz 10 bestimmten Behörden. Jede Vertragspartei stellt sicher, dass die von ihr für das Verzeichnis bereitgestellten Angaben stets richtig sind.

(13) Bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde kann sich eine Vertragspartei das Recht vorbehalten, diesen Artikel nicht auf Verkehrsdaten anzuwenden.

Artikel 9 – Umgehende Weitergabe gespeicherter Computerdaten im Notfall

(1) a) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, damit ihre Kontaktstelle für das in Artikel 35 des Übereinkommens bezeichnete 24/7-Netzwerk („Kontaktstelle“) im Notfall ein Ersuchen an eine Kontaktstelle in einem anderen Vertragsstaat übermitteln und ein Ersuchen einer solchen Kontaktstelle entgegennehmen kann, mit dem Ziel der unverzüglichen Unterstützung bei den Bemühungen, von einem Diensteanbieter im Hoheitsgebiet dieser Vertragspartei die umgehende Weitergabe spezifischer gespeicherter Computerdaten, die sich in seinem Besitz oder unter seiner Kontrolle befinden, zu erwirken, ohne dass ein Rechtshilfeersuchen vorliegt.

b) Eine Vertragspartei kann bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde erklären, dass sie keine Ersuchen nach Buchstabe a, die lediglich auf die Weitergabe von Bestandsdaten gerichtet sind, erledigen wird.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um nach Absatz 1

a) ihren Behörden zu ermöglichen, infolge eines Ersuchens nach Absatz 1 Daten bei einem Diensteanbieter in ihrem Hoheitsgebiet anzufordern,

b) einem Diensteanbieter in ihrem Hoheitsgebiet zu ermöglichen, zur Erledigung eines Ersuchens nach Buchstabe a die angeforderten Daten an ihre Behörden weiterzugeben, und

c) ihren Behörden zu ermöglichen, die angeforderten Daten der ersuchenden Vertragspartei zur Verfügung zu stellen.

(3) Im Ersuchen nach Absatz 1 sind anzugeben:

a) die zuständige Behörde, die die Daten anfordert, sowie das Datum, an dem das Ersuchen gestellt wurde,

b) eine Erklärung, dass das Ersuchen nach Maßgabe dieses Protokolls gestellt wird,

c) der Name und die Anschrift des Dienstanbieters beziehungsweise der Diensteanbieter, in dessen beziehungsweise deren Besitz oder unter dessen beziehungsweise deren Kontrolle sich die angeforderten Daten befinden,

d) die Straftat beziehungsweise die Straftaten, die Gegenstand der strafrechtlichen Ermittlungen oder des strafrechtlichen Verfahrens ist beziehungsweise sind sowie ein Verweis auf die entsprechenden Rechtsvorschriften und den geltenden Strafrahmen,

e) die Tatsachen, aus denen das Vorliegen eines Notfalls und der Bezug der angeforderten Daten hierzu ausreichend hervorgehen,

f) eine genaue Beschreibung der angeforderten Daten,

g) sonstige besondere Verfahrenshinweise und

h) sonstige Informationen, die bei den Bemühungen um die Weitergabe der angeforderten Daten hilfreich sein können.

(4) Die ersuchte Vertragspartei nimmt Ersuchen in elektronischer Form entgegen. Eine Vertragspartei kann Ersuchen auch mündlich entgegennehmen und eine Bestätigung in elektronischer Form verlangen. Sie kann angemessene Sicherheits- und Authentifizierungsstandards verlangen, bevor dem Ersuchen stattgegeben wird.

(5) Eine Vertragspartei kann bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde erklären, dass die ersuchenden Vertragsparteien nach Erledigung eines Ersuchens dieses und alle begleitend übermittelten ergänzenden Angaben in einer von der ersuchten Vertragspartei bestimmten Form und auf einem von der ersuchten Vertragspartei bestimmten Weg, gegebenenfalls auch im Wege der Rechtshilfe, zu übermitteln haben.

(6) Die ersuchte Vertragspartei unterrichtet die ersuchende Vertragspartei in einem besonders beschleunigten Verfahren über ihre Entscheidung bezüglich des Ersuchens nach Absatz 1 und gibt gegebenenfalls an, unter welchen Bedingungen sie die Daten zur Verfügung stellen würde und welche sonstigen Formen der Zusammenarbeit möglich sind.

(7) a) Kann die ersuchende Vertragspartei einer durch die ersuchte Vertragspartei nach Absatz 6 gestellten Bedingung nicht entsprechen, so unterrichtet sie umgehend die ersuchte Vertragspartei. Die ersuchte Vertragspartei entscheidet sodann, ob die Informationen oder Unterlagen dennoch zur Verfügung gestellt werden sollen. Nimmt die ersuchende Vertragspartei die Bedingung an, so ist sie daran gebunden.

b) Die ersuchte Vertragspartei, die Informationen oder Unterlagen unter einer solchen Bedingung zur Verfügung stellt, kann von der ersuchenden Vertragspartei verlangen, dass sie in Zusammenhang mit dieser Bedingung Angaben über die Verwendung der Informationen oder Unterlagen macht.

Abschnitt 4 – Verfahren für Rechtshilfe in Notfällen

Artikel 10 – Rechtshilfe in Notfällen

(1) Jede Vertragspartei kann um besonders beschleunigte Rechtshilfe ersuchen, wenn sie der Auffassung ist, dass ein Notfall vorliegt. Ein Ersuchen nach diesem Artikel umfasst neben den übrigen erforderlichen Inhalten eine Beschreibung der Tatsachen, aus denen das Vorliegen eines Notfalls und der Bezug der angeforderten Rechtshilfe hierzu hervorgeht.

(2) Eine ersuchte Vertragspartei nimmt ein solches Ersuchen in elektronischer Form entgegen. Sie kann angemessene Sicherheits- und Authentifizierungsstandards verlangen, bevor dem Ersuchen stattgegeben wird.

(3) Die ersuchte Vertragspartei kann in einem besonders beschleunigten Verfahren ergänzende Angaben zur Beurteilung des Ersuchens anfordern. Die ersuchende Vertragspartei stellt solche ergänzenden Angaben in einem besonders beschleunigten Verfahren bereit.

(4) Hat sie sich davon überzeugt, dass ein Notfall vorliegt, und sind die übrigen Erfordernisse für Rechtshilfe erfüllt, erledigt die ersuchte Vertragspartei das Ersuchen in einem besonders beschleunigten Verfahren.

(5) Jede Vertragspartei stellt sicher, dass in ihrer zentralen Behörde oder sonstigen für die Erledigung von Rechtshilfeersuchen zuständigen Behörden an sieben Wochentagen 24 Stunden täglich eine Person zur Verfügung steht, um Ersuchen nach diesem Artikel zu erledigen.

(6) Die zentrale Behörde oder sonstige für die Rechtshilfe zuständige Behörden der ersuchenden und der ersuchten Vertragsparteien können einvernehmlich bestimmen, dass die Ergebnisse der Erledigung eines Ersuchens nach diesem Artikel oder eine Vorabkopie dieser Ergebnisse der ersuchenden Vertragspartei auf einem anderen als dem für das Ersuchen genutzten Weg übermittelt werden können.

(7) Ist zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, nicht in Kraft, so finden Artikel 27 Absatz 2 Buchstabe b und Absätze 3 bis 8 sowie Artikel 28 Absätze 2 bis 4 des Übereinkommens auf den vorliegenden Artikel Anwendung.

(8) Besteht ein solcher Vertrag oder eine solche Übereinkunft, so wird dieser Artikel durch einen solchen Vertrag oder eine solche Übereinkunft ergänzt, es sei denn, die betreffenden Vertragsparteien bestimmen einvernehmlich, stattdessen die in Absatz 7 genannten Bestimmungen des Übereinkommens ganz oder teilweise anzuwenden.

(9) Jede Vertragspartei kann bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde erklären, dass Ersuchen auch unmittelbar an ihre Justizbehörden oder über die Kanäle der Internationalen Kriminalpolizeilichen Organisation (Interpol) oder an ihre nach Artikel 35 des Übereinkommens eingerichtete 24/7-Kontaktstelle übermittelt werden können. In solchen Fällen ist gleichzeitig über die zentrale Behörde der ersuchenden Vertragspartei eine Kopie an die zentrale Behörde der ersuchten Vertragspartei zu übermitteln. Wird ein Ersuchen unmittelbar an eine Justizbehörde der ersuchten Vertragspartei übermittelt und ist diese Behörde für die Erledigung nicht zuständig, so leitet sie das Ersuchen an die zuständige Behörde ihres Landes weiter und setzt die ersuchende Vertragspartei unmittelbar davon in Kenntnis.

Abschnitt 5 – Verfahren für die internationale Zusammenarbeit ohne anwendbare völkerrechtliche Übereinkünfte

Artikel 11 – Videokonferenzen

(1) Eine ersuchende Vertragspartei kann darum ersuchen und die ersuchte Vertragspartei kann gestatten, dass Aussagen und Erklärungen von Zeuginnen beziehungsweise Zeugen und von Sachverständigen über Videokonferenzen entgegengenommen werden. Die ersuchende Vertragspartei und die ersuchte Vertragspartei konsultieren einander im Hinblick auf die Klärung von möglicherweise in Zusammenhang mit der Erledigung des Ersuchens auftretenden Fragen, darunter gegebenenfalls, welche Vertragspartei den Vorsitz führt, welche Behörden und Personen anwesend sind, ob durch eine oder beide Vertragsparteien bestimmte Eide der Zeuginnen beziehungsweise Zeugen oder der Sachverständigen abgenommen oder ihnen Belehrungen oder Anweisungen erteilt werden, wie die Zeuginnen beziehungsweise Zeugen oder Sachverständigen befragt werden, wie die Rechte der Zeuginnen beziehungsweise Zeugen oder Sachverständigen ordnungsgemäß gewahrt werden, wie die Geltendmachung von Vorrechten oder Immunitäten behandelt wird, wie Einwände gegen Fragen oder Antworten behandelt werden und ob von einer oder beiden Vertragsparteien Übersetzungs-, Dolmetsch- oder Transkriptionsdienste bereitgestellt werden.

(2) a) Für die Zwecke dieses Artikels kommunizieren die zentralen Behörden der ersuchten und der ersuchenden Vertragspartei auf direktem Wege miteinander. Eine ersuchte Vertragspartei kann ein Ersuchen in elektronischer Form entgegennehmen. Sie kann angemessene Sicherheits- und Authentifizierungsstandards verlangen, bevor dem Ersuchen stattgegeben wird.

b) Die ersuchte Vertragspartei unterrichtet die ersuchende Vertragspartei über die Gründe, aus denen sie das Ersuchen nicht erledigt oder die Erledigung verzögert. Artikel 27 Absatz 8 des Übereinkommens findet auf diesen Artikel Anwendung. Unbeschadet jeder

sonstigen Bedingung, die eine ersuchte Vertragspartei nach diesem Artikel stellen kann, findet Artikel 28 Absätze 2 bis 4 des Übereinkommens auf diesen Artikel Anwendung.

(3) Leistet eine ersuchte Vertragspartei Rechtshilfe nach diesem Artikel, so bemüht sie sich, die Anwesenheit der Person zu erwirken, deren Aussage oder Stellungnahme erbeten wird. Gegebenenfalls kann die ersuchte Vertragspartei, soweit dies nach ihrem Recht zulässig ist, die erforderlichen Maßnahmen treffen, um Zeuginnen beziehungsweise Zeugen oder Sachverständige zu zwingen, zu einem bestimmten Zeitpunkt an einem bestimmten Ort in der ersuchten Vertragspartei zu erscheinen.

(4) Die von der ersuchenden Vertragspartei bestimmten Verfahren zur Durchführung der Videokonferenz werden eingehalten, sofern sie nicht mit dem innerstaatlichen Recht der ersuchten Vertragspartei unvereinbar sind. Bei Unvereinbarkeit oder soweit das Verfahren von der ersuchenden Vertragspartei nicht bestimmt wurde, wendet die ersuchte Vertragspartei das nach ihrem innerstaatlichen Recht vorgesehene Verfahren an, sofern die ersuchende und die ersuchte Vertragspartei nicht einvernehmlich etwas anderes bestimmt haben.

(5) Unbeschadet der gerichtlichen Zuständigkeit nach dem innerstaatlichem Recht der ersuchenden Vertragspartei können Zeuginnen beziehungsweise Zeugen oder Sachverständige, die im Rahmen der Videokonferenz

a) vorsätzlich falsch aussagen, nachdem sie von der ersuchten Vertragspartei nach dem innerstaatlichen Recht der ersuchten Vertragspartei zur wahrheitsgemäßen Aussage verpflichtet worden sind,

b) die Aussage verweigern, nachdem sie von der ersuchten Vertragspartei nach dem innerstaatlichen Recht der ersuchten Vertragspartei zur Aussage verpflichtet worden sind, oder

c) eine sonstige Verfehlung begehen, die nach dem innerstaatlichen Recht der ersuchten Vertragspartei im Rahmen eines solchen Verfahrens untersagt ist,

in der ersuchten Vertragspartei in derselben Weise bestraft werden, als hätten sie diese Handlung in einem innerstaatlichen Verfahren begangen.

(6) a) Sofern die ersuchende und die ersuchte Vertragspartei nicht einvernehmlich etwas anderes bestimmt haben, trägt die ersuchte Vertragspartei sämtliche mit der Erledigung eines Ersuchens nach diesem Artikel verbundene Kosten außer

i) die Honorare der sachverständigen Zeuginnen beziehungsweise Zeugen,

ii) die Übersetzungs-, Dolmetsch- und Transkriptionskosten und

iii) außergewöhnliche Kosten.

b) Würde die Erledigung eines Ersuchens außergewöhnliche Kosten verursachen, konsultieren die ersuchende und die ersuchte Vertragspartei einander, um zu bestimmen, unter welchen Bedingungen das Ersuchen erledigt werden kann.

(7) Soweit von der ersuchenden und der ersuchten Vertragspartei einvernehmlich vereinbart,

a) kann dieser Artikel für die Zwecke der Durchführung von Audiokonferenzen Anwendung finden;

b) kann Videokonferenztechnik für andere als die in Absatz 1 bezeichneten Zwecke oder Anhörungen eingesetzt werden, einschließlich für Zwecke der Identifizierung von Personen oder Sachen.

(8) Gestattet eine ersuchte Vertragspartei die Anhörung einer verdächtigen oder beschuldigten Person, kann sie verlangen, dass bestimmte Bedingungen und Garantien hinsichtlich der Entgegennahme der Aussage oder Erklärung von dieser Person, der Zustellung an oder der Anwendung von verfahrensrechtlichen Maßnahmen auf diese Person eingehalten werden.

Artikel 12 – Gemeinsame Ermittlungsgruppen und gemeinsame Ermittlungen

(1) Wenn eine verstärkte Koordination besonders zweckmäßig erscheint, können die zuständigen Behörden von zwei oder mehr Vertragsparteien zur Erleichterung von strafrechtlichen Ermittlungen oder Verfahren in ihren Hoheitsgebieten einvernehmlich eine gemeinsame Ermittlungsgruppe einrichten und unterhalten. Die zuständigen Behörden werden jeweils von den betreffenden Vertragsparteien bestimmt.

(2) Die Verfahren und Bedingungen für den Einsatz gemeinsamer Ermittlungsgruppen, etwa ihre spezifischen Zielsetzungen, ihre Besetzung, ihre Aufgaben, ihre Dauer und eventuelle Verlängerungszeiträume, ihren Ort, ihre Struktur, Vorgaben hinsichtlich der Erhebung, Übermittlung und Verwendung von Informationen oder Beweismaterial, Vorgaben hinsichtlich der Vertraulichkeit und Vorgaben hinsichtlich der Mitwirkung der beteiligten Behörden einer Vertragspartei an Ermittlungsmaßnahmen im Hoheitsgebiet einer anderen Vertragspartei, werden von diesen zuständigen Behörden vereinbart.

(3) Eine Vertragspartei kann bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde erklären, dass ihre zentrale Behörde die Vereinbarung zur Einrichtung der Gruppe unterzeichnen oder dieser Vereinbarung auf andere Weise zustimmen muss.

(4) Diese zuständigen und beteiligten Behörden kommunizieren auf direktem Wege miteinander, jedoch können die Vertragsparteien einvernehmlich andere geeignete Kommunikationswege bestimmen, wenn außergewöhnliche Umstände eine zentralere Koordination erforderlich machen.

(5) Müssen Ermittlungsmaßnahmen im Hoheitsgebiet einer der betreffenden Vertragsparteien durchgeführt werden, so können die beteiligten Behörden dieser Vertragspartei ihre eigenen Behörden um Ergreifung dieser Maßnahmen ersuchen, ohne dass die anderen Vertragsparteien ein Rechtshilfeersuchen stellen müssen. Diese Maßnahmen werden von den Behörden dieser Vertragspartei in ihrem Hoheitsgebiet unter den Bedingungen vorgenommen, die nach innerstaatlichem Recht für eine nationale Ermittlung gelten.

(6) Die Verwendung von Informationen oder Beweismaterial, die beziehungsweise das die beteiligten Behörden einer Vertragspartei den beteiligten Behörden der anderen betreffenden Vertragsparteien zur Verfügung gestellt haben, kann auf die in der Vereinbarung nach den Absätzen 1 und 2 festgelegte Weise versagt oder beschränkt werden. Werden in dieser Vereinbarung keine Vorgaben hinsichtlich der Versagung oder Beschränkung der Verwendung gemacht, so können die Vertragsparteien die zur Verfügung gestellten Informationen oder das zur Verfügung gestellte Beweismaterial folgendermaßen nutzen:

a) für die Zwecke, für die die Vereinbarung geschlossen wurde,

b) für die Aufdeckung, Untersuchung und Verfolgung von anderen Straftaten als denen, hinsichtlich derer die Vereinbarung geschlossen wurde, vorbehaltlich der vorherigen Zustimmung der Behörden, welche die Informationen oder das Beweismaterial zur Verfügung gestellt haben. Eine Zustimmung ist jedoch nicht erforderlich, wenn wesentliche

Rechtsgrundsätze der Vertragspartei, welche die Informationen oder das Beweismaterial verwendet, es erforderlich machen, dass sie die Informationen oder das Beweismaterial zum Schutz der Rechte einer beschuldigten Person in einem strafrechtlichen Verfahren weitergibt. In diesem Fall benachrichtigen die entsprechenden Behörden ohne ungebührliche Verzögerung die Behörden, welche die Informationen oder das Beweismaterial zur Verfügung gestellt haben, oder

c) zur Verhinderung eines Notfalls. In diesem Fall benachrichtigen die beteiligten Behörden, welche die Informationen oder das Beweismaterial empfangen haben, ohne ungebührliche Verzögerung die beteiligten Behörden, welche die Informationen oder das Beweismaterial zur Verfügung gestellt haben, sofern nicht einvernehmlich etwas anderes bestimmt wurde.

(7) In Ermangelung einer Vereinbarung nach den Absätzen 1 und 2 können gemeinsame Ermittlungen im Einzelfall nach einvernehmlich bestimmten Vorgaben durchgeführt werden. Dieser Absatz findet unabhängig davon Anwendung, ob zwischen den betreffenden Vertragsparteien ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, in Kraft ist.

Kapitel III - Bedingungen und Garantien

Artikel 13 Bedingungen und Garantien

Im Einklang mit Artikel 15 des Übereinkommens stellt jede Vertragspartei sicher, dass für die Schaffung, Umsetzung und Anwendung der in diesem Protokoll vorgesehenen Befugnisse und Verfahren Bedingungen und Garantien ihres innerstaatlichen Rechts gelten, die einen angemessenen Schutz der Menschenrechte und Freiheiten vorsehen.

Artikel 14 – Schutz personenbezogener Daten

(1) Geltungsbereich

a) Sofern in den Buchstaben b und c nichts anderes vorgesehen ist, verarbeitet jede Vertragspartei die personenbezogenen Daten, die sie nach diesem Protokoll empfängt, nach Maßgabe der Absätze 2 bis 15.

b) Sind die übermittelnde Vertragspartei und die empfangende Vertragspartei zum Zeitpunkt des Empfangs personenbezogener Daten nach diesem Protokoll wechselseitig durch eine völkerrechtliche Übereinkunft gebunden, die zwischen diesen Vertragsparteien einen umfassenden Rahmen für den Schutz personenbezogener Daten schafft, der auf die Übermittlung personenbezogener Daten für den Zweck der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Straftaten Anwendung findet und der vorsieht, dass die Verarbeitung personenbezogener Daten nach dieser Übereinkunft den in den Datenschutzgesetzen der betreffenden Vertragsparteien niedergelegten Anforderungen entspricht, so finden bei Maßnahmen, die in den Geltungsbereich einer solchen Übereinkunft fallen, auf nach dem Protokoll empfangene personenbezogene Daten anstelle der Absätze 2 bis 15 die Vorgaben der Übereinkunft Anwendung, sofern die betreffenden Vertragsparteien nichts anderes vereinbart haben.

c) Sind die übermittelnde Vertragspartei und die empfangende Vertragspartei nicht durch eine unter Buchstabe b bezeichnete Übereinkunft wechselseitig gebunden, können sie

einvernehmlich bestimmen, dass die Übermittlung personenbezogener Daten nach diesem Protokoll statt auf der Grundlage der Absätze 2 bis 15 auf der Grundlage anderer Übereinkünfte oder Vereinbarungen zwischen den betreffenden Vertragsparteien erfolgen kann.

d) Jede Vertragspartei geht davon aus, dass die Verarbeitung personenbezogener Daten nach den Buchstaben a und b die Anforderungen ihres Rechtsrahmens im Bereich des Schutzes personenbezogener Daten für internationale Übermittlungen personenbezogener Daten erfüllt; einer weiteren Genehmigung der Übermittlung nach diesem Rechtsrahmen bedarf es nicht. Eine Vertragspartei darf die Übermittlung von Daten an eine andere Vertragspartei nach diesem Protokoll nur dann aus Gründen des Datenschutzes unter den in Absatz 15 festgelegten Bedingungen ablehnen oder untersagen, wenn Buchstabe a Anwendung findet, oder nach den Vorgaben einer in Buchstabe b oder c genannten Übereinkunft oder Vereinbarung, sofern einer dieser Buchstaben Anwendung findet.

e) Dieser Artikel hindert eine Vertragspartei nicht daran, auf die Verarbeitung von nach diesem Protokoll empfangenen personenbezogenen Daten durch ihre eigenen Behörden strengere Garantien anzuwenden.

(2) Zweck und Verwendung

a) Die Vertragspartei, die personenbezogene Daten empfangen hat, verarbeitet diese für die in Artikel 2 bezeichneten Zwecke. Sie darf die personenbezogenen Daten nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeiten und sie darf die Daten nicht weiterverarbeiten, wenn dies nach ihrem innerstaatlichen Recht nicht zulässig ist. Dieser Artikel berührt nicht die Möglichkeit der übermittelnden Vertragspartei, in einem bestimmten Fall zusätzliche Bedingungen nach diesem Protokoll vorzusehen, jedoch dürfen diese Bedingungen keine allgemeinen Datenschutzbedingungen einschließen.

b) Die empfangende Vertragspartei stellt in ihrem innerstaatlichen Recht sicher, dass angeforderte und verarbeitete personenbezogene Daten für den Verarbeitungszweck erheblich sind und nicht darüber hinausgehen.

(3) Qualität und Unversehrtheit

Jede Vertragspartei ergreift angemessene Maßnahmen, um sicherzustellen, dass personenbezogene Daten mit der für ihre rechtmäßige Verarbeitung notwendigen und angemessenen Richtigkeit, Vollständigkeit und Aktualität aufbewahrt werden, wobei die Zwecke, für die sie verarbeitet werden, Berücksichtigung finden.

(4) Sensible Daten

Die Verarbeitung von personenbezogenen Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder sonstige Überzeugungen oder eine Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, von biometrischen Daten, die angesichts der damit verbundenen Gefahren als sensibel angesehen werden, oder von die Gesundheit oder das Sexualleben betreffenden personenbezogenen Daten durch eine Vertragspartei darf nur unter Wahrung angemessener Garantien zum Schutz vor ungerechtfertigten nachteiligen Auswirkungen der Verwendung solcher Daten, insbesondere vor unrechtmäßiger Diskriminierung, durch eine Vertragspartei erfolgen.

(5) Speicherfristen

Jede Vertragspartei speichert die personenbezogenen Daten lediglich so lange, wie es für die Zwecke der Verarbeitung der Daten nach Absatz 2 notwendig und angemessen ist. Zur Erfüllung dieser Verpflichtung sieht sie in ihrem innerstaatlichen Recht konkrete

Speicherfristen oder regelmäßige Überprüfungen der Notwendigkeit einer weiteren Speicherung der Daten vor.

(6) Automatisierte Entscheidungen

Entscheidungen, die die rechtmäßigen Interessen der Person, auf die sich die personenbezogenen Daten beziehen, erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung von personenbezogenen Daten gestützt sein, es sei denn, dies ist nach innerstaatlichem Recht zulässig und es gibt geeignete Garantien einschließlich der Möglichkeit, das Eingreifen eines Menschen zu erwirken.

(7) Datensicherheit und Sicherheitsvorfälle

a) Jede Vertragspartei stellt sicher, dass sie über geeignete technische, physische und organisatorische Maßnahmen zum Schutz personenbezogener Daten verfügt, insbesondere vor Verlust, zufälligem oder unberechtigtem Zugang oder zufälliger oder unberechtigter Weitergabe, Änderung oder Zerstörung („Sicherheitsvorfall“).

b) Nach Feststellung eines Sicherheitsvorfalls, von dem eine erhebliche Gefahr eines körperlichen oder anderen Schadens für Personen oder die andere Vertragspartei ausgeht, prüft die empfangende Vertragspartei umgehend die Wahrscheinlichkeit und das Ausmaß dieses Schadens und ergreift umgehend geeignete Schadensbegrenzungsmaßnahmen. Diese Maßnahmen schließen die Benachrichtigung der übermittelnden Behörde oder, für die Zwecke von Kapitel II Abschnitt 2, der nach Absatz 7 Buchstabe c bestimmten Behörde beziehungsweise Behörden ein. Die Benachrichtigung kann jedoch geeignete Einschränkungen in Bezug auf die Weiterleitung der Benachrichtigung einschließen; sie kann aufgeschoben werden oder entfallen, falls durch sie die nationale Sicherheit gefährdet werden könnte, oder aufgeschoben werden, falls durch sie Maßnahmen zum Schutz der öffentlichen Sicherheit gefährdet werden könnten. Die Maßnahmen schließen ferner die Benachrichtigung der betroffenen Person ein, es sei denn, die Vertragspartei hat geeignete Maßnahmen ergriffen, sodass keine erhebliche Gefahr mehr besteht. Die Benachrichtigung der Person kann unter den in Absatz 12 Buchstabe a Ziffer i festgelegten Bedingungen aufgeschoben werden oder entfallen. Die benachrichtigte Vertragspartei kann bezüglich des Vorfalls und der Reaktion darauf um Konsultation und zusätzliche Informationen ersuchen.

c) Jede Vertragspartei teilt der Generalsekretärin beziehungsweise dem Generalsekretär des Europarats bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde die nach Absatz 7 Buchstabe b für die Zwecke von Kapitel II Abschnitt 2 zu benachrichtigende Behörde beziehungsweise zu benachrichtigenden Behörden mit; die gemachten Angaben können nachträglich geändert werden.

(8) Führung von Aufzeichnungen

Jede Vertragspartei führt Aufzeichnungen oder verfügt über andere geeignete Mittel, um nachzuweisen, wie in einem bestimmten Fall auf die personenbezogenen Daten einer Person zugegriffen wird, wie sie verwendet und wie sie weitergegeben werden.

(9) Weitergabe innerhalb einer Vertragspartei

a) Stellt eine Behörde einer Vertragspartei personenbezogene Daten, die sie ursprünglich nach diesem Protokoll empfangen hat, einer anderen Behörde derselben Vertragspartei zur Verfügung, so verarbeitet diese andere Behörde die Daten vorbehaltlich des Buchstabens b im Einklang mit diesem Artikel.

b) Ungeachtet des Buchstabens a kann eine Vertragspartei, die einen Vorbehalt nach Artikel 17 angebracht hat, personenbezogene Daten, die sie empfangen hat, ihren Gliedstaaten

oder anderen gleichartigen Gebietseinheiten zur Verfügung stellen, sofern die Vertragspartei über Maßnahmen verfügt, damit die empfangenden Behörden die Daten weiterhin wirksam schützen, indem sie für die Daten ein mit diesem Artikel vergleichbares Schutzniveau vorsehen.

c) Gibt es Anzeichen einer nicht ordnungsgemäßen Durchführung dieses Absatzes, kann die übermittelnde Vertragspartei um Konsultation und zusätzliche Informationen zu diesen Anzeichen ersuchen.

(10) Weiterübermittlung an einen anderen Staat oder eine internationale Organisation

a) Die empfangende Vertragspartei darf die personenbezogenen Daten nur mit vorheriger Genehmigung der übermittelnden Behörde oder, für die Zwecke von Kapitel II Abschnitt 2, der nach Absatz 10 Buchstabe b bestimmten Behörde beziehungsweise Behörden an einen anderen Staat oder eine internationale Organisation übermitteln.

b) Jede Vertragspartei teilt der Generalsekretärin beziehungsweise dem Generalsekretär des Europarats bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde die Behörde beziehungsweise Behörden mit, die für die Zwecke von Kapitel II Abschnitt 2 eine Genehmigung erteilen kann beziehungsweise können; die gemachten Angaben können nachträglich geändert werden.

(11) Transparenz und Information

a) Jede Vertragspartei informiert durch Veröffentlichung allgemeiner Informationen oder durch persönliche Information der Person, deren personenbezogene Daten erhoben wurden, über:

i) die Rechtsgrundlage und die Zwecke der Verarbeitung,

ii) etwaige Speicher- und Überprüfungsfristen nach Absatz 5, soweit einschlägig,

iii) die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und

iv) Zugangs-, Berichtigungs- und Rechtsbehelfsmöglichkeiten.

b) Eine Vertragspartei kann hinsichtlich der Pflicht zur persönlichen Information nach den in Absatz 12 Buchstabe a Ziffer i festgelegten Bedingungen angemessene Beschränkungen nach ihrem innerstaatlichen Recht vorsehen.

c) Verlangt das innerstaatliche Recht der übermittelnden Vertragspartei eine persönliche Information der Person, deren Daten einer anderen Vertragspartei zur Verfügung gestellt wurden, so trifft die übermittelnde Vertragspartei Maßnahmen, um die andere Vertragspartei zum Zeitpunkt der Übermittlung hinsichtlich dieses Erfordernisses und geeigneter Kontaktinformationen zu unterrichten. Eine persönliche Information erfolgt nicht, wenn die andere Vertragspartei darum ersucht hat, die Bereitstellung der Daten vertraulich zu behandeln, soweit die in Absatz 12 Buchstabe a Ziffer i genannten Bedingungen für Beschränkungen gelten. Sobald diese Beschränkungen nicht mehr gelten und die persönliche Information erfolgen kann, ergreift die andere Vertragspartei Maßnahmen zur Unterrichtung der übermittelnden Vertragspartei. Sofern noch keine Unterrichtung der übermittelnden Vertragspartei erfolgt ist, kann diese sich mit Ersuchen an die empfangende Vertragspartei wenden, die sodann die übermittelnde Vertragspartei darüber unterrichtet, ob die Beschränkung aufrechtzuerhalten ist.

(12) Zugang und Berichtigung

a) Jede Vertragspartei stellt sicher, dass jede Person, deren personenbezogene Daten nach diesem Protokoll empfangen wurden, in Übereinstimmung mit den im innerstaatlichen Recht der Vertragspartei festgelegten Verfahren ohne ungebührliche Verzögerung Folgendes beantragen und erhalten kann:

i) eine schriftliche oder elektronische Kopie der über die betroffene Person vorgehaltenen Unterlagen, die die personenbezogenen Daten der Person enthalten, sowie verfügbare Informationen über die Rechtsgrundlage und die Zwecke der Verarbeitung, die Speicherfristen und die Empfänger oder Kategorien von Empfängern der Daten („Zugang"), sowie Informationen über verfügbare Rechtsbehelfsmöglichkeiten, vorausgesetzt, dass in bestimmten Einzelfällen der Zugang verhältnismäßigen Beschränkungen unterworfen werden kann, die nach dem innerstaatlichen Recht zulässig und zum Zeitpunkt der Entscheidung zum Schutz der Rechte und Freiheiten anderer oder wichtiger Ziele des allgemeinen öffentlichen Interesses erforderlich sind und die die berechtigten Interessen der betroffenen Person angemessen berücksichtigen;

ii) eine Berichtigung, wenn die personenbezogenen Daten der Person unrichtig sind oder nicht ordnungsgemäß verarbeitet wurden; die Berichtigung umfasst – soweit dies unter Berücksichtigung der Gründe für die Berichtigung und der konkreten Umstände der Verarbeitung angemessen und vertretbar ist – die Korrektur, Ergänzung, Löschung oder Anonymisierung, Einschränkung der Verarbeitung oder Sperrung.

b) Wird der Zugang oder die Berichtigung versagt oder beschränkt, so übermittelt die Vertragspartei der betroffenen Person ohne ungebührliche Verzögerung eine schriftliche Antwort, die auch elektronisch übermittelt werden kann, mit der die Person über die Versagung oder Beschränkung unterrichtet wird. Die Vertragspartei begründet die Versagung oder Beschränkung und macht Angaben zu verfügbaren Rechtsbehelfsmöglichkeiten. Die Kosten für die Zugangsgewährung sollten auf ein angemessenes und nicht überzogenes Maß beschränkt werden.

(13) Gerichtliche und außergerichtliche Rechtsbehelfe

Jede Vertragspartei verfügt über wirksame gerichtliche und außergerichtliche Rechtsbehelfe, um Verstöße gegen diesen Artikel abzuhelfen.

(14) Beaufsichtigung

Jede Vertragspartei verfügt über eine oder mehrere Behörden, die, allein oder gemeinsam, unabhängige und wirksame Beaufsichtigungsfunktionen und -befugnisse in Bezug auf die in diesem Artikel festgelegten Maßnahmen ausüben. Die Funktionen und Befugnisse dieser allein oder gemeinsam tätig werdenden Behörden umfassen Untersuchungsbefugnisse, die Befugnis, auf Beschwerden hin tätig zu werden, und die Fähigkeit, Abhilfemaßnahmen durchzuführen.

(15) Konsultation und Aussetzung

Eine Vertragspartei kann die Übermittlung personenbezogener Daten an eine andere Vertragspartei aussetzen, wenn ihr stichhaltige Beweise dafür vorliegen, dass die andere Vertragspartei systematisch oder schwerwiegend gegen diesen Artikel verstößt oder dass ein schwerwiegender Verstoß unmittelbar bevorsteht. Sie setzt Übermittlungen nicht ohne angemessene Ankündigung aus, und auch erst, nachdem die betreffenden Vertragsparteien eine angemessene Zeitspanne für Konsultationen aufgebracht haben, ohne zu einer Lösung zu gelangen. Eine Vertragspartei kann Übermittlungen jedoch vorläufig aussetzen, wenn ein systematischer oder schwerwiegender Verstoß vorliegt, der eine erhebliche und unmittelbare

Gefahr für das Leben oder die Sicherheit oder eine erhebliche Schädigung des Ansehens oder Vermögens einer natürlichen Person darstellt; in diesem Fall benachrichtigt sie die andere Vertragspartei und nimmt im Anschluss daran sofort Konsultationen mit der anderen Vertragspartei auf. Hat die Konsultation nicht zu einer Lösung geführt, so kann die andere Vertragspartei die Übermittlungen ihrerseits aussetzen, wenn ihr stichhaltige Beweise dafür vorliegen, dass die Aussetzung durch die aussetzende Vertragspartei diesem Absatz zuwiderlief. Die aussetzende Vertragspartei hebt die Aussetzung auf, sobald der die Aussetzung rechtfertigende Verstoß behoben wurde; zu diesem Zeitpunkt wird auch eine etwaige gegenseitige Aussetzung aufgehoben. Alle vor der Aussetzung übermittelten personenbezogenen Daten werden weiterhin nach Maßgabe dieses Protokolls behandelt.

KAPITEL IV – SCHLUSSBESTIMMUNGEN

Artikel 15 – Wirkungen dieses Protokolls

(1) a) Artikel 39 Absatz 2 des Übereinkommens findet auf dieses Protokoll Anwendung.

b) Vertragsparteien, die Mitglied der Europäischen Union sind, können in ihren Beziehungen untereinander das Recht der Europäischen Union, das die von diesem Protokoll erfassten Fragen betrifft, anwenden.

c) Buchstabe b hat keine Auswirkungen auf die uneingeschränkte Anwendung dieses Protokolls zwischen Vertragsparteien, die Mitglied der Europäischen Union sind, und anderen Vertragsparteien.

(2) Artikel 39 Absatz 3 des Übereinkommens findet auf dieses Protokoll Anwendung.

Artikel 16 – Unterzeichnung und Inkrafttreten

(1) Dieses Protokoll liegt für die Vertragsparteien des Übereinkommens zur Unterzeichnung auf; sie können ihre Zustimmung, gebunden zu sein, ausdrücken,

a) indem sie es ohne Vorbehalt der Ratifikation, Annahme oder Genehmigung unterzeichnen oder

b) indem sie es vorbehaltlich der Ratifikation, Annahme oder Genehmigung unterzeichnen und später ratifizieren, annehmen oder genehmigen.

(2) Die Ratifikations-, Annahme- oder Genehmigungsurkunden werden bei der Generalsekretärin beziehungsweise dem Generalsekretär des Europarats hinterlegt.

(3) Dieses Protokoll tritt am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag folgt, an dem fünf Vertragsparteien des Übereinkommens nach den Absätzen 1 und 2 ihre Zustimmung ausgedrückt haben, durch dieses Protokoll gebunden zu sein.

(4) Für jede Vertragspartei des Übereinkommens, die später ihre Zustimmung ausdrückt, durch dieses Protokoll gebunden zu sein, tritt es am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag folgt, an dem die Vertragspartei nach den Absätzen 1 und 2 ihre Zustimmung ausgedrückt hat, durch dieses Protokoll gebunden zu sein.

Artikel 17 – Bundesstaatsklausel

(1) Ein Bundesstaat kann sich das Recht vorbehalten, Verpflichtungen nach diesem Protokoll so weit zu übernehmen, wie sie mit den Grundprinzipien vereinbar sind, welche die Beziehungen zwischen seiner Zentralregierung und seinen Gliedstaaten oder anderen gleichartigen Gebietseinheiten regeln, vorausgesetzt,

a) das Protokoll findet auf die Zentralregierung des Bundesstaats Anwendung,

b) ein solcher Vorbehalt wirkt sich nicht auf die Verpflichtungen zur Zusammenarbeit aus, um die andere Vertragsparteien nach Kapitel II ersuchen, und

c) Artikel 13 findet auf die Gliedstaaten oder andere gleichartigen Gebietseinheiten des Bundesstaats Anwendung.

(2) Eine andere Vertragspartei kann Behörden, Anbietern und Stellen in ihrem Hoheitsgebiet die Zusammenarbeit zur Erledigung von unmittelbar von einem Gliedstaat oder einer anderen gleichartigen Gebietseinheit eines Bundesstaats, der einen Vorbehalt nach Absatz 1 angebracht hat, gestellten Ersuchen oder Anordnungen, untersagen, es sei denn, der Bundesstaat notifiziert der Generalsekretärin beziehungsweise dem Generalsekretär des Europarats, dass ein Gliedstaat oder eine andere gleichartige Gebietseinheit die auf den Bundesstaat anwendbaren Verpflichtungen nach diesem Protokoll anwendet. Die Generalsekretärin beziehungsweise der Generalsekretär des Europarats erstellt und aktualisiert ein Verzeichnis solcher Notifikationen.

(3) Eine andere Vertragspartei wird den Behörden, Anbietern und Stellen in ihrem Hoheitsgebiet nicht auf der Grundlage eines Vorbehalts nach Absatz 1 die Zusammenarbeit mit einem Gliedstaat oder einer anderen gleichartigen Gebietseinheit untersagen, wenn eine Anordnung oder ein Ersuchen über die Zentralregierung vorgelegt wurde oder unter Beteiligung der Zentralregierung eine Vereinbarung über die Bildung einer gemeinsamen Ermittlungsgruppe nach Artikel 12 getroffen wird. In diesen Fällen sorgt die Zentralregierung für die Erfüllung der anwendbaren Verpflichtungen nach dem Protokoll, vorausgesetzt, dass im Hinblick auf den Schutz personenbezogener Daten, die den Gliedstaaten oder anderen gleichartigen Gebietseinheiten übermittelt werden, nur Artikel 14 Absatz 9 oder, soweit zutreffend, eine Übereinkunft oder Vereinbarung nach Artikel 14 Absatz 1 Buchstaben b oder c Anwendung finden.

(4) Hinsichtlich derjenigen Bestimmungen dieses Protokolls, für deren Anwendung die Gliedstaaten oder anderen gleichartigen Gebietseinheiten die Gesetzgebungszuständigkeit besitzen, ohne nach der Verfassungsordnung des Bundes zum Erlass von Rechtsvorschriften verpflichtet zu sein, bringt die Zentralregierung den zuständigen Behörden dieser Staaten die genannten Bestimmungen befürwortend zur Kenntnis und ermutigt sie, geeignete Maßnahmen zu treffen, um sie durchzuführen.

Artikel 18 – Räumlicher Geltungsbereich

(1) Dieses Protokoll findet auf einzelne oder mehrere Hoheitsgebiete, die eine Vertragspartei in einer Erklärung nach Artikel 38 Absatz 1 oder 2 des Übereinkommens bezeichnet hat, Anwendung, soweit die Erklärung nicht nach Artikel 38 Absatz 3 zurückgenommen wurde.

(2) Eine Vertragspartei kann bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde erklären, dass dieses Protokoll auf einzelne oder mehrere Hoheitsgebiete, die in der Erklärung der

Vertragspartei nach Artikel 38 Absatz 1 und/oder Absatz 2 des Übereinkommens bezeichnet wurden, keine Anwendung findet.

(3) Eine nach Absatz 2 abgegebene Erklärung kann in Bezug auf jedes darin bezeichnete Hoheitsgebiet durch eine an die Generalsekretärin beziehungsweise den Generalsekretär des Europarats gerichtete Notifikation zurückgenommen werden. Die Rücknahme wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Notifikation bei der Generalsekretärin beziehungsweise dem Generalsekretär folgt.

Artikel 19 Vorbehalte und Erklärungen

(1) Jede Vertragspartei des Übereinkommens kann durch eine an die Generalsekretärin beziehungsweise den Generalsekretär des Europarats gerichtete schriftliche Notifikation bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde erklären, dass sie von einem oder mehreren der in Artikel 7 Absatz 9 Buchstaben a und b, Artikel 8 Absatz 13 und Artikel 17 dieses Protokolls vorgesehenen Vorbehalte Gebrauch macht. Weitere Vorbehalte sind nicht zulässig.

(2) Jede Vertragspartei des Übereinkommens kann durch eine an die Generalsekretärin beziehungsweise den Generalsekretär des Europarats gerichtete schriftliche Notifikation bei der Unterzeichnung dieses Protokolls oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde einzelne oder mehrere der in 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 dieses Protokolls bezeichneten Erklärungen abgeben.

(3) Jede Vertragspartei des Übereinkommens gibt durch eine an die Generalsekretärin beziehungsweise den Generalsekretär des Europarats gerichtete schriftliche Notifikation einzelne oder mehrere der in 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 dieses Protokolls bezeichneten Erklärungen, Notifikationen oder Mitteilungen nach den darin festgelegten Vorgaben ab.

Artikel 20 – Status und Rücknahme von Vorbehalten

(1) Eine Vertragspartei, die einen Vorbehalt nach Artikel 19 Absatz 1 angebracht hat, nimmt diesen Vorbehalt ganz oder teilweise zurück, sobald die Umstände es erlauben. Diese Rücknahme wird mit Eingang einer Notifikation über die Rücknahme bei der Generalsekretärin beziehungsweise dem Generalsekretär des Europarats wirksam. Wird in der Notifikation angegeben, dass die Rücknahme eines Vorbehalts zu einem bestimmten Zeitpunkt wirksam werden soll, und liegt dieser nach dem Eingang der Notifikation bei der Generalsekretärin beziehungsweise dem Generalsekretär, so wird die Rücknahme zu diesem späteren Zeitpunkt wirksam.

(2) Die Generalsekretärin beziehungsweise der Generalsekretär des Europarats kann sich in regelmäßigen Zeitabständen bei den Vertragsparteien, die einen oder mehrere Vorbehalte nach Artikel 19 Absatz 1 angebracht haben, nach den Aussichten für eine etwaige Rücknahme erkundigen.

Artikel 21 – Änderungen

(1) Jede Vertragspartei dieses Protokolls kann Änderungen dieses Übereinkommens vorschlagen; die Generalsekretärin beziehungsweise der Generalsekretär des Europarats übermittelt jeden Vorschlag den Mitgliedstaaten des Europarats und den Vertragsparteien und Unterzeichnerstaaten des Übereinkommens sowie jedem Staat, der zum Beitritt zu dem Übereinkommen eingeladen worden ist.

(2) Jede von einer Vertragspartei vorgeschlagene Änderung wird dem Europäischen Ausschuss für Strafrechtsfragen (CDPC) übermittelt; dieser unterbreitet dem Ministerkomitee seine Stellungnahme zu dem Änderungsvorschlag.

(3) Das Ministerkomitee prüft den Änderungsvorschlag und die vom CDPC unterbreitete Stellungnahme und kann nach Konsultation der Vertragsparteien des Übereinkommens die Änderung annehmen.

(4) Der Wortlaut jeder vom Ministerkomitee nach Absatz 3 angenommenen Änderung wird den Vertragsparteien dieses Protokolls zur Annahme übermittelt.

(5) Jede nach Absatz 3 angenommene Änderung tritt am dreißigsten Tag nach dem Tag in Kraft, an dem alle Vertragsparteien dieses Protokolls der Generalsekretärin beziehungsweise dem Generalsekretär mitgeteilt haben, dass sie sie angenommen haben.

Artikel 22 – Beilegung von Streitigkeiten

Artikel 45 des Übereinkommens findet auf dieses Protokoll Anwendung.

Artikel 23 – Konsultationen der Vertragsparteien und Bewertung der Durchführung

(1) Artikel 46 des Übereinkommens findet auf dieses Protokoll Anwendung.

(2) Die Vertragsparteien bewerten in regelmäßigen Abständen die wirksame Anwendung und Durchführung dieses Protokolls. Artikel 2 der Geschäftsordnung des Ausschusses für das Übereinkommen über Computerkriminalität in der Fassung vom 16. Oktober 2020 findet sinngemäß Anwendung. Die Vertragsparteien überprüfen und ändern gegebenenfalls einvernehmlich die in diesem Artikel vorgesehenen Verfahren, soweit sie fünf Jahre nach Inkrafttreten dieses Protokolls auf dieses Protokoll Anwendung finden.

(3) Die Prüfung von Artikel 14 beginnt, sobald zehn Vertragsparteien des Übereinkommens ihre Zustimmung ausgedrückt haben, durch dieses Protokoll gebunden zu sein.

Artikel 24 – Kündigung

(1) Jede Vertragspartei kann dieses Protokoll jederzeit durch eine an die Generalsekretärin beziehungsweise den Generalsekretär des Europarats gerichtete Notifikation kündigen.

(2) Die Kündigung wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Notifikation bei der Generalsekretärin beziehungsweise dem Generalsekretär folgt.

(3) Die Kündigung des Übereinkommens durch eine Vertragspartei dieses Protokolls bedeutet gleichzeitig die Kündigung dieses Protokolls.

(4) Informationen oder Beweismaterial, die beziehungsweise das vor dem Wirksamwerden der Kündigung übermittelt wurden, werden weiterhin nach Maßgabe dieses Protokolls behandelt.

Artikel 25 – Notifikation

Die Generalsekretärin beziehungsweise der Generalsekretär des Europarats notifiziert den Mitgliedstaaten des Europarats, den Vertragsparteien und den Unterzeichnern des Übereinkommens und jedem Staat, der zum Beitritt zu dem Übereinkommen eingeladen worden ist,

a) jede Unterzeichnung;

b) jede Hinterlegung einer Ratifikations-, Annahme- oder Genehmigungsurkunde;

c) jeden Zeitpunkt des Inkrafttretens dieses Protokolls nach Artikel 16 Absätze 3 und 4;

d) jede Erklärung und jeden Vorbehalt nach Artikel 19 und jede Rücknahme von Vorbehalten nach Artikel 20;

e) jede andere Handlung, Notifikation oder Mitteilung in Zusammenhang mit diesem Protokoll.

Zu Urkund dessen haben die hierzu gehörig befugten Unterzeichneten dieses Protokoll unterschrieben.

Geschehen zu [Ort] am [Datum] in englischer und französischer Sprache, wobei jeder Wortlaut gleichermaßen verbindlich ist, in einer Urschrift, die im Archiv des Europarats hinterlegt wird. Die Generalsekretärin beziehungsweise der Generalsekretär des Europarats übermittelt allen Mitgliedstaaten des Europarats, den Vertragsparteien und den Unterzeichnern des Übereinkommens sowie jedem Staat, der zum Beitritt zu dem Übereinkommen eingeladen worden ist, beglaubigte Abschriften.