EUROPÄISCHE
KOMMISSION

Brüssel, den 16.7.2025
COM(2025) 415 final

2025/0230 (NLE)

Vorschlag für einen

BESCHLUSS DES RATES

über die Unterzeichnung – im Namen der Europäischen Union – des Übereinkommens der Vereinten Nationen gegen Cyberkriminalität; Stärkung der internationalen Zusammenarbeit bei der Bekämpfung bestimmter mithilfe von Informations- und Kommunikationstechnologiesystemen begangener Straftaten und bei der Weitergabe von Beweismitteln in elektronischer Form für schwere Straftaten

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Ziele des Vorschlags

Mit dem vorgeschlagenen Beschluss soll die Europäische Kommission (im Folgenden „Kommission“) vom Rat der Europäischen Union (im Folgenden „Rat“) ermächtigt werden, das Übereinkommen der Vereinten Nationen gegen Cyberkriminalität (im Folgenden „Übereinkommen“) im Namen der Europäischen Union zu unterzeichnen[1].

Die Kommission wird auch einen Vorschlag für einen Beschluss des Rates zur Ermächtigung der Kommission, das Übereinkommen im Namen der Europäischen Union zu schließen, vorlegen. Zusammen erfüllen diese Vorschläge die Zusage der Kommission in ProtectEU, der Europäischen Strategie für die innere Sicherheit[2].

Cyberkriminalität stellt eine nach wie vor wachsende Bedrohung für die Sicherheit der Bürgerinnen und Bürger und der Unternehmen in der Europäischen Union (EU) dar[3]. Der Europol-Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet zufolge haben sich die von der Cyberkriminalität ausgehenden Bedrohungen hinsichtlich Umfang, Intensität und Gefahrenpotential in den letzten zehn Jahren dynamisch weiterentwickelt[4]. Cyberkriminelle nutzen neue Technologien wie künstliche Intelligenz (KI) für die Automatisierung von Angriffen, für Social Engineering und für die Umgehung von Sicherheitsmaßnahmen, wodurch Cyberangriffe an Skalierbarkeit und Effizienz gewinnen. Die wirtschaftliche Rezession, die geopolitische Instabilität und die zunehmende globale Ungleichheit haben den Anreiz verstärkt, aus finanziellen Gründen Cyberstraftaten zu begehen[5]. Größe und Umfang von durch den Cyberraum ermöglichten Straftaten wie Online-Betrug und sexuellem Missbrauch von Kindern nehmen stetig zu. Schätzungen zufolge beliefen sich die weltweiten Schäden durch Online-Betrug 2024 auf 1,03 Billionen EUR[6]. Die weltweiten Meldungen von sexuellem Missbrauch von Kindern sind von 1 Million im Jahr 2010 auf fast 36 Millionen im Jahr 2023 gestiegen, davon 1,3 Millionen in der EU[7].

Cyberkriminalität ist ein globales und grenzenloses Phänomen, und die Intensivierung der internationalen Zusammenarbeit zu ihrer Bekämpfung gehört seit über einem Jahrzehnt zu den Prioritäten der Länder weltweit. Der Umstand, dass es im Internet keine Grenzen gibt, macht Ermittlungen im Zusammenhang mit Cyberkriminalität fast immer grenzübergreifend,

---

1 Der Wortlaut des Übereinkommens wird dem Vorschlag für einen Beschluss des Rates über den Abschluss des Übereinkommens im Namen der Union als Anhang beigefügt.

2 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „ProtectEU – eine Europäische Strategie für die innere Sicherheit“ (COM(2025) 148 final).

3 Im Jahr 2023 waren Ransomware-Angriffe, sexuelle Ausbeutung von Kindern und Online-Betrug nach wie vor die gefährlichsten Formen von Cyberkriminalität in der Europäischen Union (EU). Einige Cyberkriminelle, deren Angriffe sich gegen die EU richteten, waren in der EU ansässig, während andere es vorzogen, vom Ausland aus zu operieren und für ihre illegalen Aktivitäten und Gelder den Schutz von Drittländern zu suchen. Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet (IOCTA) 2024.

4 Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet (IOCTA) 2024.

5 Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität (SOCTA) 2025.

6 *Global State of Scams Report* 2025 (GASA).

7 *National Centre for Missing and Exploited Children*, https://www.missingkids.org/cybertiplinedata.

was eine enge Zusammenarbeit zwischen den Behörden verschiedener Länder notwendig macht. In den letzten Jahren ist eine Zusammenarbeit mit immer mehr Ländern erforderlich geworden, da Cyberkriminelle für ihre Angriffe auf die EU und ihre Partnerländer den Schutz geeigneter Hoheitsgebiete rund um den Globus suchen.

Elektronische Beweismittel werden für strafrechtliche Ermittlungen sowohl bei Online-Straftaten als auch bei herkömmlichen Straftaten wie Drogenhandel, die häufig im Internet Spuren hinterlassen, weil Kriminelle ihre Aktivitäten online und auf Anwendungen planen und koordinieren, immer wichtiger. Eine Erhebung der Kommission ergab, dass die Strafverfolgungs- und Justizbehörden schon 2018 bei mindestens 85 % der strafrechtlichen Ermittlungen, einschließlich Cyberkriminalität, Zugang zu elektronischen Beweismitteln benötigten[8]. Beweismittel für Straftaten liegen zunehmend in elektronischer Form bei Diensteanbietern in ausländischen Hoheitsgebieten vor. Bei mindestens 55 % der Ermittlungen wird ein Antrag auf grenzüberschreitenden Zugang zu Beweismitteln gestellt[9]. Eine wirksame strafgerichtliche Reaktion erfordert geeignete Maßnahmen zur Erlangung solcher Beweismittel, um die Rechtsstaatlichkeit zu wahren.

Daher werden auf nationaler Ebene, auf EU-Ebene[10] und auf internationaler Ebene Maßnahmen zur Verbesserung der Weitergabe elektronischer Beweismittel für strafrechtliche Ermittlungen getroffen.

Das Übereinkommen ist Teil dieser Maßnahmen. Es enthält gemeinsame Vorschriften auf globaler Ebene, um die Zusammenarbeit im Bereich der Cyberkriminalität und die Erhebung von Beweismitteln in elektronischer Form für strafrechtliche Ermittlungen oder Verfahren zu verbessern, schafft damit eine Grundlage für die Zusammenarbeit mit vielen Ländern, mit denen weder die EU noch ihre Mitgliedstaaten Vereinbarungen getroffen haben, und gewährleistet gleichzeitig die Achtung der Rechtsvorschriften und Werte der EU. Es ist mit den bestehenden EU-Instrumenten und internationalen Instrumenten vereinbar und ergänzt diese.

Hintergrund

Das Übereinkommen des Europarats über Computerkriminalität (im Folgenden „Budapester Übereinkommen“)[11] aus dem Jahr 2001 ist der erste internationale Vertrag über Cyberkriminalität. Es erleichtert die Bekämpfung von Straftaten, bei denen Computernetze genutzt werden. Das Budapester Übereinkommen steht den Mitgliedstaaten des Europarats und auf Einladung auch Nichtmitgliedern offen. Bislang sind darin 80 Vertragsstaaten zusammengeschlossen, darunter 26 Mitgliedstaaten der Europäischen Union. Das Zweite

8 SWD(2018) 118 final.

9 SWD(2018) 118 final.

10 Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl. L 191 vom 28.7.2023, S. 118), ELI:. http://data.europa.eu/eli/reg/2023/1543/oj) und Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren (ABl. L 191 vom 28.7.2023, S. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

11 SEV Nr. 185.

Zusatzprotokoll[12] zum Budapester Übereinkommen enthält aktualisierte Vorschriften für den Austausch elektronischer Beweismittel[13].

Die Europäische Union und ihre Mitgliedstaaten sind auch Vertragsparteien von zwei der wichtigsten Strafrechtsinstrumente der Vereinten Nationen, die nahezu weltweit angenommen wurden, dem Übereinkommen der Vereinten Nationen gegen die organisierte Kriminalität (UNTOC)[14] und dem Übereinkommen der Vereinten Nationen gegen Korruption (UNCAC)[15].

Die Bestimmungen des neuen Übereinkommens sind an diese drei etablierten und weithin angenommenen internationalen Instrumente angeglichen und mit ihnen vereinbar.

Der Aufstieg der Informationstechnologie und die rasche Entwicklung neuer Telekommunikations- und Computernetzsysteme sowie die Nutzung und der Missbrauch von Technologien zu kriminellen Zwecken stehen auch auf der Tagesordnung der Vereinten Nationen (VN). Am 21. Dezember 2010 hat die Generalversammlung der Vereinten Nationen die Resolution 65/230 verabschiedet, in der sie die Kommission für Verbrechensverhütung und Strafrechtspflege (*Commission on Crime Prevention and Criminal Justice* – CCPCJ) aufforderte, eine offene zwischenstaatliche Sachverständigengruppe (*intergovernmental expert group* – IEG) mit dem Auftrag einzusetzen, eine umfassende Studie zum Problem der Cyberkriminalität durchzuführen.

---

12 SEV Nr. 224.

13 Der Rat hat Beschlüsse erlassen, mit denen die Mitgliedstaaten ermächtigt werden, im Interesse der EU das Zweite Zusatzprotokoll zu unterzeichnen und zu ratifizieren: Beschluss (EU) 2022/722 des Rates vom 5. April 2022 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 (ABl. L 134 vom 11.5.2022, S. 15, ELI: http://data.europa.eu/eli/dec/2022/722/oj) und Beschluss (EU) 2023/436 des Rates vom 14. Februar 2023 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 (ABl. L 63 vom 28.2.2023, S. 48, ELI: http://data.europa.eu/eli/dec/2023/436/oj).

14 Dok. A/55/383. Die EU hat das UNTOC am 12. Dezember 2000 unterzeichnet und am 21. Mai 2004 ratifiziert, ebenso die dazugehörigen Protokolle über Schleuserkriminalität und Menschenhandel. Siehe 2004/579/EG: Beschluss des Rates vom 29. April 2004 über den Abschluss – im Namen der Europäischen Gemeinschaft – des Übereinkommens der Vereinten Nationen gegen die grenzüberschreitende organisierte Kriminalität (ABl. L 261 vom 6.8.2004, S. 69, ELI: http://data.europa.eu/eli/dec/2004/579/oj), 2006/616/EG: Beschluss des Rates vom 24. Juli 2006 über den Abschluss – im Namen der Europäischen Gemeinschaft – des Zusatzprotokolls gegen die Schleusung von Migranten auf dem Land-, See- und Luftweg zum Übereinkommen der Vereinten Nationen gegen die grenzüberschreitende organisierte Kriminalität in Bezug auf diejenigen Bestimmungen des Zusatzprotokolls, die in den Anwendungsbereich der Artikel 179 und 181a des Vertrags zur Gründung der Europäischen Gemeinschaft fallen (ABl. L 262 vom 22.9.2006, S. 24, ELI: http://data.europa.eu/eli/dec/2006/616/oj) und 2006/619/EG: Beschluss des Rates vom 24. Juli 2006 über den Abschluss – im Namen der Europäischen Gemeinschaft – des Zusatzprotokolls zur Verhütung, Bekämpfung und Bestrafung des Menschenhandels, insbesondere des Frauen– und Kinderhandels, zum Übereinkommen der Vereinten Nationen gegen die grenzüberschreitende organisierte Kriminalität in Bezug auf diejenigen Bestimmungen des Zusatzprotokolls, die in den Anwendungsbereich von Titel IV des Dritten Teils des Vertrags zur Gründung der Europäischen Gemeinschaft fallen (ABl. L 262 vom 22.9.2006, S. 51, ELI: http://data.europa.eu/eli/dec/2006/619/oj).

15 *United Nations Treaty Series* (Vertragssammlung der Vereinten Nationen), Bd. 2349, S. 41; Dok. A/58/422. Die EU hat das UNCAC am 15. September 2005 unterzeichnet und am 12. November 2008 ratifiziert. Siehe 2008/801/EG: Beschluss des Rates vom 25. September 2008 über den Abschluss – im Namen der Europäischen Gemeinschaft – des Übereinkommens der Vereinten Nationen gegen Korruption (ABl. L 287 vom 29.10.2008, S. 1, ELI: http://data.europa.eu/eli/dec/2008/801/oj).

Die Generalversammlung der Vereinten Nationen hat die Resolution 73/187 vom 17. Dezember 2018 zur „Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken“ verabschiedet. Am 27. Dezember 2019 hat die Generalversammlung der Vereinten Nationen eine zweite Resolution, 74/247, zum gleichen Thema verabschiedet und damit einen offenen zwischenstaatlichen Ad-hoc-Sachverständigenausschuss (im Folgenden „Ad-hoc-Ausschuss“) für die Ausarbeitung eines umfassenden internationalen Übereinkommens zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken eingesetzt. Nach der Resolution hatte der Ad-hoc-Ausschuss die bestehenden internationalen Instrumente und die auf nationaler, regionaler und internationaler Ebene unternommenen Anstrengungen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken und insbesondere die Arbeit der IEG und die von ihr erzielten Ergebnisse in vollem Umfang zu berücksichtigen.

Am 24. Mai 2022 hat der Rat die Kommission ermächtigt, im Namen der Europäischen Union an den Verhandlungen über das Übereinkommen teilzunehmen[16]. Die Kommission hat im Einklang mit dem Beschluss des Rates daran teilgenommen und sich dabei von den darin festgelegten Verhandlungsrichtlinien leiten lassen. Die Kommission ist vom Europäischen Auswärtigen Dienst (EAD) unterstützt worden. Sie hat den Sonderausschuss des Rates für die Verhandlungen konsequent zum Standpunkt der Union konsultiert und die Vereinbarkeit des Übereinkommens mit dem einschlägigen Besitzstand der Union sichergestellt.

Im Einklang mit der Rahmenvereinbarung über die Beziehungen zwischen dem Europäischen Parlament und der Europäischen Kommission[17] hat die Kommission auch das Europäische Parlament über die Verhandlungen informiert.

Die Kommission hat ferner den Europäischen Datenschutzbeauftragten (EDSB) und den Europäischen Datenschutzausschuss (EDSA) während und nach Abschluss der Verhandlungen unterrichtet.

Der Ad-hoc-Ausschuss ist zwischen dem 28. Februar 2022 und dem 9. August 2024 achtmal zu förmlichen Tagungen zusammengetreten. Darüber hinaus haben zwischenzeitlich informelle Tagungen und fünf intersessionelle Tagungen stattgefunden, bei denen ein breites Spektrum von Interessenträgern konsultiert wurde, darunter globale und regionale zwischenstaatliche Organisationen, nichtstaatliche Organisationen, Organisationen der Zivilgesellschaft, akademische Einrichtungen und der Privatsektor.

Am 8. August 2024 hat der Ad-hoc-Ausschuss den Entwurf des Übereinkommens und den diesem beigefügten Entwurf einer Resolution der Generalversammlung der Vereinten Nationen einvernehmlich gebilligt. Die Generalversammlung der Vereinten Nationen hat beide Dokumente am 24. Dezember 2024 einvernehmlich angenommen[18]. Das Übereinkommen soll am 25. Oktober 2025 in Hanoi (Vietnam) und danach bis zum 31. Dezember 2026 am Sitz der Vereinten Nationen in New York zur Unterzeichnung aufgelegt werden.

Das Übereinkommen tritt in Kraft, sobald 40 Vertragsstaaten ihre Zustimmung bekundet haben, durch das Übereinkommen nach Artikel 65 Absätze 1 und 2 gebunden zu sein.

---

16 Beschluss (EU) 2022/895 des Rates vom 24. Mai 2022 zur Ermächtigung zur Aufnahme von Verhandlungen im Namen der Europäischen Union über ein umfassendes internationales Übereinkommen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken (ABl. L 155 vom 8.6.2022, S. 42, ELI: http://data.europa.eu/eli/dec/2022/895/oj).

17 ABl. L 304/47.

18 Resolution der Generalversammlung vom 24. Dezember 2024, A/RES/79/243.

Im Einklang mit der gängigen Praxis beim UNTOC und beim UNCAC sieht das Übereinkommen vor, dass eine Organisation der regionalen Wirtschaftsintegration wie die Europäische Union das Übereinkommen unterzeichnen und ratifizieren kann, wenn mindestens einer der Mitgliedstaaten es unterzeichnet und ratifiziert.

Gründe für den Vorschlag

Das Übereinkommen steht mit den Zielen der Union im Einklang, die in ProtectEU, der 2025 verabschiedeten Europäischen Strategie für die innere Sicherheit, festgelegt sind, um Kriminalität zu bekämpfen und den Zugang zu digitalen Beweismitteln für alle Straftaten durch internationale Instrumente wie das Übereinkommen zu erleichtern. Es ergänzt die bestehenden EU-Instrumente und internationalen Instrumente, deren Vertragsparteien die EU und/oder ihre Mitgliedstaaten sind, wie das Budapester Übereinkommen des Europarats, und trägt damit zur Bekämpfung der grenzüberschreitenden Kriminalität durch die EU bei.

Erstens hat das Übereinkommen als Instrument der Vereinten Nationen hinsichtlich der Mitgliederzahl eine größere Reichweite als die bestehenden EU-Instrumente und internationalen Instrumente. In dieser Hinsicht gleicht es den nahezu weltweit angenommenen bisherigen Instrumenten der Vereinten Nationen über die Zusammenarbeit in Strafsachen wie dem UNTOC und dem UNCAC. Es kann somit eine verstärkte Zusammenarbeit bei der Bekämpfung der Cyberkriminalität auf globaler Ebene ermöglichen.

Zweitens orientiert sich das Übereinkommen an den Kriminalisierungsbestimmungen des Budapester Übereinkommens, was die Zusammenarbeit auf der Grundlage eines seit Langem bestehenden und erprobten Rechtsrahmens weiter verbessern kann. Da das Übereinkommen erst vor Kurzem angenommen wurde, werden mit ihm auch weitere Bestimmungen über die Kriminalisierung von Straftaten eingeführt, die in den letzten Jahren drastisch zugenommen haben: Online-Betrug, Grooming oder die Kontaktaufnahme zur Begehung einer Sexualstraftat gegen ein Kind und die nicht einvernehmliche Verbreitung intimer Bilder. Diese sind bereits auf EU-Ebene, aber noch nicht auf globaler Ebene unter Strafe gestellt.

Drittens ermöglicht das Übereinkommen den Austausch elektronischer Beweismittel für ebenfalls zunehmende Formen schwerer Kriminalität, einschließlich Straftaten im Zusammenhang mit Terrorismus und grenzüberschreitender organisierter Kriminalität, zwischen den Behörden seiner Vertragsstaaten. Diese Begrenzung auf schwere Straftaten beschränkt die Anwendung des Mechanismus auf schwere Fälle, was dazu beiträgt, Verhältnismäßigkeit zu gewährleisten. Sie verhindert auch, dass die nationalen Behörden mit Ersuchen überlastet werden, und trägt dem unterschiedlichen Maß an Vertrauen in die Zusammenarbeit auf internationaler Ebene Rechnung.

Viertens ergänzt das Übereinkommen die bestehenden internationalen Instrumente wie das Budapester Übereinkommen, indem es Verfahrensmaßnahmen zum Schutz von Opfern und Zeugen, Instrumente zur Einziehung der Erträge aus Cyberkriminalität sowie Maßnahmen der internationalen Zusammenarbeit bei der Überstellung verurteilter Personen und der Übertragung der Strafverfolgung, bei gemeinsamen Ermittlungen und bei der Zusammenarbeit bei der Strafverfolgung enthält.

Fünftens enthält das Übereinkommen ein Kapitel über technische Hilfe und Kapazitätsaufbau, um Entwicklungsländern beim Ausbau ihrer Fähigkeiten zu helfen und sie in die Lage zu versetzen, einen Beitrag zur weltweiten Bekämpfung der Cyberkriminalität zu leisten.

Sechstens verpflichtet das Übereinkommen die Vertragsstaaten des Übereinkommens, die Menschenrechte, einschließlich der Verfahrensrechte und Garantien im Strafverfahren (wie das Recht auf ein faires Verfahren, die Verteidigungsrechte und das Recht auf eine gerichtliche oder andere unabhängige Überprüfung), und das Recht auf Schutz

personenbezogener Daten bei jeder Maßnahme nach dem Übereinkommen zu achten. Angesichts seiner universellen Ausrichtung und in Anerkennung der bestehenden Unterschiede beim Niveau des Schutzes der Menschenrechte in der Welt enthält das Übereinkommen Bestimmungen, mit denen seine Verwendung zur Begehung von Menschenrechtsverletzungen ausgeschlossen wird und den Vertragsstaaten erstmals Gründe für die Ablehnung einer Zusammenarbeit mit anderen Vertragsparteien in solchen Fällen an die Hand gegeben werden. Weitere Informationen hierzu finden Sie in den nachstehenden Abschnitten „Kohärenz mit den bestehenden Vorschriften in diesem Bereich", „Grundrechte" und „Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags". Diese Bestimmungen machen das Übereinkommen mit einem so umfassenden Schutz der Menschenrechte und so umfassenden Menschenrechtsgarantien zum ersten seiner Art. Mit seinem Inkrafttreten wird das Übereinkommen zu einem Maßstab für künftige internationale Instrumente werden und dazu beitragen, dass diese Menschenrechtsgarantien in der globalen Zusammenarbeit in Strafsachen durchgängig berücksichtigt werden.

- **Kohärenz mit den bestehenden Vorschriften in diesem Bereich**

Die Bekämpfung der Cyberkriminalität ist eine Priorität der Europäischen Union; anerkannt wurde dies vom Rat in seinen strategischen Leitlinien für die gesetzgeberische und operative Programmplanung im Raum der Freiheit, der Sicherheit und des Rechts[19] aus dem Jahr 2024 und von der Kommission in ProtectEU – Europäische Strategie für die innere Sicherheit der Europäischen Union aus dem Jahr 2025, in der Maßnahmen der EU zur Bekämpfung der Online-Kriminalität und zur Erleichterung des Zugangs zu digitalen Beweismitteln für alle Straftaten, unter anderem durch internationale Instrumente für den Austausch von Informationen und Beweismitteln, angekündigt werden, z. B. die zeitnahe Unterzeichnung und der zeitnahe Abschluss des Übereinkommens.

Die Kommission erkennt an, dass die Kapazitäten der Strafverfolgungs- und Justizbehörden in diesem Bereich weiter ausgebaut und gestärkt werden müssen, um nationale Rechtsvorschriften über Cyberkriminalität zu entwickeln, sofern diese nicht ausreichend vorhanden sind. Sie erkennt auch an, dass die internationale Zusammenarbeit bei der Bekämpfung der Cyberkriminalität gefördert werden muss, und unterstützt eine Reihe von Programmen für den Kapazitätsaufbau in verschiedenen Ländern weltweit, auch in Entwicklungsländern[20]. Die Kommission hat die Arbeit der IEG, der Kommission der Vereinten Nationen für Verbrechensverhütung und Strafrechtspflege, des Büros der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC), des Ausschusses des Budapester Übereinkommens über Computerkriminalität und anderer Gremien unterstützt.

Die Bestimmungen des Übereinkommens stehen mit den Vorschriften und der Politik der EU in den Bereichen justizielle Zusammenarbeit in Strafsachen, polizeiliche Zusammenarbeit und Datenschutz sowie mit den einschlägigen bilateralen und multilateralen Übereinkünften im Einklang, deren Vertragspartei die Europäische Union bereits ist.

Vorbehalte und Notifikationen

Das Übereinkommen enthält keine eigene Bestimmung über Vorbehalte. Jedoch sind Vorbehalte in einigen Bestimmungen ausdrücklich vorgesehen (Artikel 11 Absatz 3, Artikel 23 Absatz 3 Buchstabe a, Artikel 23 Absatz 3 Buchstabe b letzter Teil, Artikel 42 Absatz 5 sowie Artikel 63 Absatz 3 und 4), und das Übereinkommen gestattet implizit weitere

[19] Strategische Leitlinien für die gesetzgeberische und operative Programmplanung im Raum der Freiheit, der Sicherheit und des Rechts, 28. November 2024, Nummer 19.

[20] Siehe z. B. das Projekt „*Global Action on Cybercrime Enhanced* (GLACY-e)", abrufbar unter https://www.coe.int/en/web/cybercrime/glacy-e.

Vorbehalte, sofern diese mit Artikel 19 Buchstabe c des Wiener Übereinkommens über das Recht der Verträge[21] und dem Völkergewohnheitsrecht im Einklang stehen und daher nicht mit Ziel und Zweck des Übereinkommens unvereinbar sind. Das Übereinkommen bietet daher erhebliche Flexibilität in Bezug auf Vorbehalte. Bei Vorbehalten und Notifikationen sollten die Mitgliedstaaten einen einheitlichen Ansatz verfolgen, der in Anhang I dieses Beschlusses festgelegt ist. Vorbehalte und Notifikationen müssen mit dem Unionsrecht und dem Völkerrecht vereinbar sein und dürfen Ziel und Zweck des Übereinkommens nicht zuwiderlaufen. Die in diesem Übereinkommen anerkannten und vorgesehenen Menschenrechtsbedingungen und -garantien sind Teil seines Ziels und Zwecks und können daher keinen Vorbehalten unterworfen werden.

- **Kohärenz mit der Politik der Union in anderen Bereichen**

Das Übereinkommen steht im Einklang mit den Vorschriften und der Politik der Europäischen Union in den von ihm erfassten Bereichen (internationale Zusammenarbeit und Rechtshilfe zwischen Behörden der Mitgliedstaaten und zwischen Behörden von Mitgliedstaaten und Drittländern, wie im Abschnitt „Kohärenz mit den bestehenden Vorschriften in diesem Bereich“ beschrieben) sowie mit den einschlägigen bilateralen und multilateralen Übereinkünften, deren Vertragspartei die Europäische Union bereits ist. Andere Politikbereiche der Union bleiben unberührt.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

- **Rechtsgrundlage**

Rechtsgrundlage des Vorschlags ist Artikel 218 Absatz 5 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Artikel 218 AEUV enthält Verfahrensvorschriften für die Aushandlung und den Abschluss von Übereinkünften zwischen der Europäischen Union und Drittländern oder internationalen Organisationen. Insbesondere sieht Absatz 5 vor, dass der Rat auf Vorschlag der Kommission als Verhandlungsführer einen Beschluss über die Unterzeichnung der Übereinkunft im Namen der Europäischen Union erlässt.

Die materielle Rechtsgrundlage für einen Beschluss nach Artikel 218 Absatz 5 AEUV hängt in erster Linie von Ziel und Inhalt der geplanten internationalen Übereinkunft ab, zu der ein im Namen der Union zu vertretender Standpunkt festgelegt wird. Liegt der internationalen Übereinkunft ein doppelter Zweck oder Gegenstand zugrunde und ist einer davon der wesentliche und der andere von untergeordneter Bedeutung, so muss der Beschluss nach Artikel 218 Absatz 5 AEUV auf eine einzige materielle Rechtsgrundlage gestützt werden, nämlich auf diejenige, die der wesentliche oder vorrangige Zweck oder Gegenstand verlangt.

Hat eine geplante internationale Übereinkunft gleichzeitig mehrere Zwecke oder Gegenstände, die untrennbar miteinander verbunden sind, ohne dass einer dem anderen untergeordnet ist, so muss die materielle Rechtsgrundlage eines Beschlusses nach Artikel 218 Absatz 5 AEUV ausnahmsweise die verschiedenen zugehörigen Rechtsgrundlagen umfassen.

Für Angelegenheiten im Bereich der Erleichterung der Zusammenarbeit zwischen Justizbehörden oder entsprechenden Behörden im Rahmen der Strafverfolgung sowie des Vollzugs und der Vollstreckung von Entscheidungen ist die materielle Rechtsgrundlage Artikel 82 Absatz 1 AEUV. Für die Definition von Straftaten im Bereich der Cyberkriminalität ist die materielle Rechtsgrundlage Artikel 83 Absatz 1 AEUV. Für Maßnahmen zur Zusammenarbeit im Bereich der Strafverfolgung ist die materielle

[21] *United Nations Treaty Series* (Vertragssammlung der Vereinten Nationen), Bd. 1155, S. 331.

Rechtsgrundlage Artikel 87 Absatz 2 AEUV. Für den Schutz personenbezogener Daten ist die materielle Rechtsgrundlage Artikel 16 AEUV.

- **Zuständigkeit der Union**

Gegenstand des Übereinkommens ist die Bekämpfung der Cyberkriminalität, unter anderem durch die Kriminalisierung bestimmter sehr schädlicher Verhaltensweisen und den Aufbau einer internationalen Zusammenarbeit zu diesem Zweck, auch in Bezug auf elektronische Beweismittel. Dies fällt nach Artikel 4 Absatz 2 Buchstabe j AEUV in die von der Union mit den Mitgliedstaaten geteilte Zuständigkeit.

Einige Bestimmungen des Übereinkommens, insbesondere die Datenschutzbestimmung, fallen in Bereiche, die weitgehend von gemeinsamen Regeln erfasst sind, die durch das Übereinkommen beeinträchtigt werden könnten oder deren Tragweite durch das Übereinkommen verändert werden könnte. In diesen Bereichen hat die Union daher nach Artikel 3 Absatz 2 AEUV die ausschließliche Außenkompetenz für die Unterzeichnung des Übereinkommens.

Die Unterzeichnung des Übereinkommens durch die Europäische Kommission im Interesse der Union kann daher auf der Grundlage des Artikels 16, des Artikels 82 Absatz 1, des Artikels 83 Absatz 1, des Artikels 87 Absatz 1 und des Artikels 218 Absatz 5 AEUV erfolgen.

- **Subsidiarität (bei nicht ausschließlicher Zuständigkeit)**

Ein Tätigwerden auf EU-Ebene dient der Förderung einer harmonischen Anwendung der Bestimmungen des Übereinkommens in den EU-Mitgliedstaaten und gewährleistet dessen Vereinbarkeit mit den bestehenden und künftigen EU-Instrumenten. Ferner verstärken die Maßnahmen der EU in diesem Bereich die kombinierte Hebelwirkung und Durchschlagskraft der EU und ihrer Mitgliedstaaten bei den Mechanismen für die Durchführung des Übereinkommens, wie der Konferenz der Vertragsstaaten (Artikel 57), sowie bei den künftigen Verhandlungen über Protokolle zu dem Übereinkommen (Artikel 62).

- **Verhältnismäßigkeit**

Die von der Union mit diesem Vorschlag verfolgten Ziele, die im Abschnitt „Gründe für den Vorschlag“ dargelegt wurden, können nur erreicht werden, wenn eine verbindliche internationale Übereinkunft geschlossen wird, die die notwendigen Maßnahmen der Zusammenarbeit vorsieht und gleichzeitig einen angemessenen Schutz der Grundrechte gewährleistet. Mit dem Übereinkommen wird dieses Ziel erreicht. Die Bestimmungen des Übereinkommens beschränken sich auf das zur Erreichung seiner Hauptziele erforderliche Maß und greifen nicht in die bestehenden EU-Instrumente oder internationalen Instrumente ein, deren Vertragspartei die EU ist.

- **Wahl des Instruments**

Nach Artikel 218 Absatz 5 AEUV legt je nach Gegenstand der geplanten Übereinkunft die Kommission oder der Hohe Vertreter der Union für Außen- und Sicherheitspolitik dem Rat einen Vorschlag vor, der dann einen Beschluss über die Unterzeichnung der internationalen Übereinkunft erlässt. Angesichts des Gegenstands des Übereinkommens sollte die Kommission einen entsprechenden Vorschlag vorlegen.

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

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

Entfällt.

- **Konsultation der Interessenträger**

Die Kommission leitete am 14. Januar 2022 auf ihrer Website eine Aufforderung zur Stellungnahme zu dieser Initiative ein, in deren Rahmen vier Wochen lang Beiträge eingereicht werden konnten. Die einzelnen Antworten auf die Aufforderung zur Stellungnahme wurden auf der Konsultationswebsite veröffentlicht. Diese Erwägungen wurden bei der Ausarbeitung des Vorschlags der Kommission für die Teilnahme an den Verhandlungen über das Übereinkommen berücksichtigt.

Um eine größere Transparenz des Prozesses zu gewährleisten, wurde mit der Resolution 75/282 der Generalversammlung, in der die organisatorischen Angelegenheiten im Zusammenhang mit dem Ad-hoc-Ausschuss geregelt sind, sichergestellt, dass Vertreter interessierter globaler und regionaler zwischenstaatlicher Organisationen, darunter Vertreter von Organen, Sonderorganisationen und Fonds der Vereinten Nationen, sowie Vertreter der Fachkommissionen des Wirtschafts- und Sozialrats als Beobachter in die Arbeitstagungen eingebunden wurden. Ferner ermöglichte es diese Resolution nichtstaatlichen Organisationen (einschließlich globaler und regionaler zwischenstaatlicher Organisationen, nichtstaatlicher Organisationen, Organisationen der Zivilgesellschaft, akademischer Einrichtungen und des Privatsektors), sich registrieren zu lassen und an den Tagungen des Ad-hoc-Ausschusses teilzunehmen, wo sie regelmäßig Gelegenheit erhielten, auf den Plenartagungen zu den erörterten Kapiteln Stellung zu nehmen. Nach dieser Resolution fanden fünf intersessionelle Konsultationstagungen mit Interessenträgern statt. Die Interessenträger konnten auch schriftliches Material einreichen, das dann auf der Website des Ad-hoc-Ausschusses veröffentlicht wurde.

Die Kommission hat in ihrer Rolle als Verhandlungsführer während der gesamten Verhandlungen auch regelmäßig aktiv das Gespräch mit verschiedenen Interessenträgern gesucht und deren Beiträge berücksichtigt.

- **Einholung und Nutzung von Expertenwissen**

Während der Verhandlungen konsultierte die Kommission als Vertreter der Union nach dem Beschluss des Rates vom 22. Mai 2022 zur Ermächtigung der Kommission, im Namen der Union an den Verhandlungen teilzunehmen, den Sonderausschuss des Rates für die Verhandlungen. Als Mitglieder der Vereinten Nationen konnten die EU-Mitgliedstaaten an allen Verhandlungstagungen teilnehmen. Die Kommission konsultierte die Vertreter der Mitgliedstaaten während der gesamten Verhandlungen zu ihrer Formulierung des Standpunkts der Union. Die Kommission konsultierte auch regelmäßig Interessenträger (siehe oben Abschnitt „Konsultation der Interessenträger“).

- **Folgenabschätzung**

Die relevanten Auswirkungen sind in dieser Begründung dargelegt.

- **Effizienz der Rechtsetzung und Vereinfachung**

Das Übereinkommen kann Auswirkungen für bestimmte Behörden und Kategorien von Diensteanbietern haben. Aufgrund der verstärkten internationalen Zusammenarbeit bei der Weitergabe elektronischer Beweismittel zur Bekämpfung von Cyberkriminalität und durch den Cyberraum ermöglichten Straftaten könnte es zu einer Zunahme der Zahl der Ersuchen um elektronische Beweismittel kommen, die die zentralen Behörden der EU-Mitgliedstaaten für Rechtshilfe von ihren Pendants in anderen Vertragsstaaten des Übereinkommens erhalten und dann unter Beachtung aller geltenden nationalen Vorschriften und Verfahren an in ihrem Staat niedergelassene Diensteanbieter übermitteln. Gleichzeitig werden der Rechtsrahmen für die internationale Zusammenarbeit bei der Bekämpfung der Cyberkriminalität, den das Übereinkommen auf globaler Ebene schafft, sowie die darin enthaltenen Garantien und

Bedingungen den Diensteanbietern mehr Rechtssicherheit hinsichtlich der Anträge auf Zugang zu Daten bieten, mit denen sie infolge der Zusammenarbeit zwischen Staaten in Strafsachen konfrontiert sein können.

- **Grundrechte**

Das Übereinkommen enthält Garantien, die es den EU-Mitgliedstaaten ermöglichen, ihren Menschenrechtsverpflichtungen nach internationalem, EU- und nationalem Recht nachzukommen. Diese Garantien verhindern auch einen Missbrauch dieses Instruments der Vereinten Nationen durch Vertragsstaaten zu dem Zweck, Menschenrechtsverletzungen zu begehen oder zu legitimieren.

Das Übereinkommen enthält Bestimmungen über verfahrensrechtliche Maßnahmen und Maßnahmen der internationalen Zusammenarbeit in Strafsachen wie Auslieferung, Rechtshilfe und den Austausch elektronischer Beweismittel, die einen Eingriff in Grundrechte wie das Recht auf Freiheit und den Schutz vor unmenschlicher und erniedrigender Behandlung sowie das Recht auf Privatsphäre und den Schutz personenbezogener Daten darstellen können. Das Übereinkommen verfolgt einen rechtebasierten Ansatz und sieht sowohl horizontale als auch kontextspezifische solide Menschenrechtsbedingungen und -garantien vor, die mit den bestehenden internationalen Instrumenten über Menschenrechte und die Zusammenarbeit in Strafsachen im Einklang stehen. Das Übereinkommen trägt auch den Gefahren für die Menschenrechte Rechnung, die zwangsläufig mit der Bekämpfung der Cyberkriminalität und dem Wesen des Internets verbunden sind. Hinsichtlich der Menschenrechtsverpflichtungen seiner Vertragsstaaten ist im Übereinkommen wiederholt von „internationalen Menschenrechtsnormen“ die Rede. Diese weit gefasste Formulierung bezieht sich sowohl auf internationale Instrumente als auch auf das Völkergewohnheitsrecht im Bereich der Menschenrechte und gewährleistet somit eine möglichst breite Anwendung der internationalen Menschenrechtsverpflichtungen auf alle künftigen Vertragsparteien des Übereinkommens, unabhängig davon, welchen spezifischen internationalen Menschenrechtsinstrumenten sie beigetreten sind.

Artikel 6 sieht als übergeordnetes Erfordernis vor, dass die Vertragsstaaten bei der Durchführung des Übereinkommens ihren Verpflichtungen aus den internationalen Menschenrechtsnormen nachkommen müssen. Er verbietet den Vertragsparteien auch die Auslegung des Übereinkommens in einer Weise, die es ihnen erlauben würde, dieses Rechtsinstrument zur Unterdrückung der Menschenrechte oder Grundfreiheiten zu nutzen. Um diese Verpflichtung in dem digitalen Kontext, in dem dieses Übereinkommen gilt, zu unterstreichen, enthält Artikel 6 Absatz 2 auch eine nicht abschließende Liste von Menschenrechten und Grundfreiheiten, die durch potenziellen Missbrauch im digitalen Raum besonders gefährdet sind, darunter die Freiheit der Meinungsäußerung, die Gewissensfreiheit, die Meinungsfreiheit, die Religions- und Weltanschauungsfreiheit, die Versammlungsfreiheit und die Vereinigungsfreiheit. Diese horizontale Bestimmung gilt aufgrund ihrer Platzierung und ihres Wesens für das gesamte Übereinkommen und ist Teil des Ziels und Zwecks des Übereinkommens.

Auch Artikel 21 Absatz 4 ist eine horizontale Bestimmung, die die Harmonisierung der Verfolgung, Aburteilung und Ahndung der Straftaten im Sinne des Übereinkommens betrifft. Danach müssen die Vertragsstaaten sicherstellen, dass jede Person, die wegen einer der nach dem Übereinkommen festgelegten Straftaten verfolgt wird, alle Rechte und Garantien im Einklang mit dem innerstaatlichen Recht und den geltenden internationalen Verpflichtungen des Vertragsstaats genießt, einschließlich des Rechts auf ein faires Verfahren und der Verteidigungsrechte.

Artikel 24 enthält ebenfalls horizontale Bedingungen und Garantien, die sich auf die Befugnisse und Verfahrensmaßnahmen nach dem Übereinkommen sowohl auf innerstaatlicher als auch auf internationaler Ebene beziehen. Er verpflichtet die Vertragsstaaten sicherstellen, dass ihre Verfahrensbefugnisse bei der Ausübung Bedingungen und Garantien unterliegen, die den Schutz der Menschenrechte im Einklang mit ihren Verpflichtungen nach den internationalen Menschenrechtsnormen gewährleisten und die den Grundsatz der Verhältnismäßigkeit umfassen. Zu diesen Bedingungen und Garantien, die für die Befugnisse und Verfahren nach dem Übereinkommen gelten, gehören unter anderem die gerichtliche oder andere unabhängige Überprüfung, das Recht auf einen wirksamen Rechtsbehelf (das mehrere Maßnahmen für Personen umfasst, deren Menschenrechte verletzt wurden), die die Anwendung rechtfertigenden Gründe sowie die Begrenzung des Umfangs und der Dauer der Befugnisse und Verfahren.

Artikel 36 sieht erstmals in einem Strafrechtsinstrument der Vereinten Nationen eine eigene Bestimmung über den Schutz personenbezogener Daten vor. Diese Bestimmung gilt für jede Übermittlung personenbezogener Daten nach dem Übereinkommen. Solche Übermittlungen dürfen nur im Einklang mit dem innerstaatlichen Recht und den völkerrechtlichen Verpflichtungen des übermittelnden Vertragsstaats erfolgen. Die Vertragsstaaten können die Übermittlung personenbezogener Daten ablehnen, wenn die Daten nicht im Einklang mit ihren geltenden Datenschutzvorschriften bereitgestellt werden können, bevor personenbezogene Daten einem anderen Vertragsstaat zur Verfügung gestellt werden können. Um die Einhaltung seiner nationalen Rechtsvorschriften über den Schutz personenbezogener Daten zu gewährleisten und einem Ersuchen um internationale Zusammenarbeit nachkommen zu können, kann ein Vertragsstaat dem ersuchenden Staat geeignete Bedingungen auferlegen. Die Vertragsstaaten müssen sicherstellen, dass für personenbezogene Daten, die sie nach diesem Übereinkommen entweder als Teil eines Ersuchens um internationale Zusammenarbeit oder als Antwort auf ein Ersuchen erhalten, in ihrem jeweiligen Rechtsrahmen wirksame und geeignete Garantien bestehen. Die Vertragsstaaten dürfen die erhaltenen personenbezogenen Daten einem Drittland oder einer internationalen Organisation nur mit vorheriger Genehmigung des ursprünglichen übermittelnden Vertragsstaats übermitteln, der verlangen kann, dass eine solche Genehmigung schriftlich erteilt werden muss.

Das Übereinkommen sieht umfassende Garantien in Bezug auf Auslieferung und Rechtshilfe vor. Die Vertragsstaaten können Auslieferungs- oder Rechtshilfeersuchen ablehnen, wenn keine beiderseitige Strafbarkeit besteht (Artikel 37 Absatz 1 und Artikel 40 Absatz 8).

Das Übereinkommen enthält weitere Gründe für eine Ablehnung der Zusammenarbeit, die mit den bestehenden internationalen Instrumenten im Einklang stehen. Artikel 37 Absätze 8 und 15 und Artikel 40 Absätze 8, 21 und 22 ermöglichen es den Vertragsstaaten, Ersuchen um internationale Zusammenarbeit in einer Vielzahl von Fällen abzulehnen, zum Beispiel, wenn ein Rechtshilfeersuchen nicht im Einklang mit Artikel 40 gestellt wird, wenn der ersuchte Vertragsstaat der Auffassung ist, dass die Erledigung des Ersuchens seine Souveränität, seine Sicherheit, seine öffentliche Ordnung oder andere wesentliche Interessen beeinträchtigen könnte (was nach häufiger internationaler Auslegung auch Menschenrechtserwägungen einschließt), wenn es den Behörden des ersuchten Vertragsstaats nach seinem innerstaatlichen Recht untersagt wäre, die erbetene Maßnahme in Bezug auf eine vergleichbare Straftat durchzuführen, wenn das Ersuchen gegen die Rechtsordnung des ersuchten Vertragsstaats in Bezug auf die Rechtshilfe verstoßen würde oder wenn der ersuchte Vertragsstaat stichhaltige Gründe für die Annahme hat, dass das Ersuchen zum Zwecke der Verfolgung oder Bestrafung einer Person aufgrund ihres Geschlechts, ihrer Sprache, ihrer Religion, ihrer Staatsangehörigkeit, ihrer ethnischen Herkunft oder ihrer politischen Überzeugungen gestellt

wurde oder dass die Erledigung des Ersuchens aus einem dieser Gründe die Stellung der Person beeinträchtigen würde. Die Anwendung der letztgenannten Garantie auf Rechtshilfemaßnahmen wie den Austausch elektronischer Beweismittel ist in internationalen Übereinkünften über die Zusammenarbeit in Strafsachen die Ausnahme. Sie stellt aber eine wichtige zusätzliche Garantie dar, um zu verhindern, dass Einzelne, Organisationen des privaten Sektors, Medien oder Organisationen der Zivilgesellschaft und ihre Vermögenswerte Opfer von Angriffen werden. Diese Garantie, die anderen Ablehnungsgründe und das Erfordernis der beiderseitigen Strafbarkeit ermöglichen es den Vertragsstaaten, eine internationale Zusammenarbeit in Fällen abzulehnen, die sie als politisch motiviert ansehen.

Die in diesem Übereinkommen anerkannten und vorgesehenen Menschenrechtsbedingungen und -garantien sind Teil seines Ziels und Zwecks und untrennbar mit den darin vorgesehenen Befugnissen und Verfahren verbunden. Für diese Bedingungen und Garantien können daher keine Vorbehalte gelten.

Das Übereinkommen sieht auch einen Mechanismus für die regelmäßige Überprüfung der Durchführung des Übereinkommens durch die Konferenz der Vertragsstaaten vor (Artikel 57 Absatz 5 Buchstabe f). Wie bei den bestehenden anderen internationalen Instrumenten und Mechanismen in diesem Bereich sollte sich diese Überprüfung auf alle Bestimmungen des Übereinkommens einschließlich seiner Bedingungen und Garantien erstrecken.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Es ergeben sich keine Auswirkungen auf den Unionshaushalt. Für die EU-Mitgliedsstaaten können einmalige Kosten für die Durchführung des Übereinkommens anfallen, und den Behörden der Mitgliedstaaten könnten aufgrund des erwarteten Anstiegs der Zahl der Ersuchen um internationale Zusammenarbeit etwas höhere Kosten entstehen.

5. WEITERE ANGABEN

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

Einen Durchführungsplan gibt es nicht, da die Mitgliedstaaten nach der Unterzeichnung und Ratifikation des Übereinkommens zu dessen Durchführung verpflichtet sind.

Was das Monitoring betrifft, so wird die Kommission an den Tagungen der Konferenz der Vertragsstaaten, in der die Europäische Union als Vertragspartei des Übereinkommens anerkannt wird, teilnehmen und kann bei der Annahme von Änderungen und Zusatzprotokollen zum Übereinkommen ihr Stimmrecht mit der Zahl der Stimmen ausüben, die der Zahl der Mitgliedstaaten entspricht, die Vertragspartei des Übereinkommens sind. Die Kommission wird das Europäische Parlament regelmäßig über die Ergebnisse der Überprüfung und des Monitorings der Durchführung des Übereinkommens durch die Konferenz der Vertragsstaaten unterrichten.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Ziel des Übereinkommens ist es, die internationale Zusammenarbeit im Bereich der im Übereinkommen festgelegten Straftaten und der Erhebung elektronischer Beweismittel für die im Übereinkommen definierten Straftaten und andere schwere Straftaten für die Zwecke spezifischer strafrechtlicher Ermittlungen oder Verfahren zu verbessern. In diesem Zusammenhang zielt das Übereinkommen auch darauf ab, technische Hilfe und Kapazitätsaufbau zu fördern, insbesondere zugunsten der Entwicklungsländer.

Allgemeine Bestimmungen (Kapitel I (Artikel 1 bis 6))

In Kapitel I werden der allgemeine Anwendungsbereich und der Zweck des Übereinkommens dargelegt und die darin verwendeten Begriffe bestimmt. Diese Bestimmungen sind größtenteils Standardformulierungen und orientieren sich am Budapester Übereinkommen und an den beiden bestehenden Strafrechtsinstrumenten der Vereinten Nationen (UNTOC und UNCAC).

Artikel 2 enthält Begriffsbestimmungen, die mit denen des Budapester Übereinkommens, des dazugehörigen Zweiten Zusatzprotokolls und der beiden bestehenden Strafrechtsinstrumente der Vereinten Nationen (UNTOC und UNCAC) im Einklang stehen. Im Vergleich zu diesen Instrumenten wurde mit dem Übereinkommen nur eine neue Definition, die der „Inhaltsdaten“, hinzugefügt, die sich an das UNODC-Mustergesetz über die Rechtshilfe in Strafsachen[22] und an die Definition in der Verordnung über elektronische Beweismittel[23] anlehnt.

In Artikel 3 ist der Anwendungsbereich des Übereinkommens so definiert, dass er die Verhütung, Untersuchung und Verfolgung der im Übereinkommen festgelegten Straftaten sowie die Einziehung der Erträge aus diesen Straftaten umfasst. Ferner erstreckt sich der Anwendungsbereich des Übereinkommens auf die Erhebung und die Weitergabe elektronischer Beweismittel im Rahmen spezifischer strafrechtlicher Ermittlungen oder Verfahren nach den Artikeln 23 und 35 (weitere Einzelheiten unten in den Abschnitten „Verfahrensrechtliche Maßnahmen und Strafverfolgung (Kapitel IV (Artikel 23 bis 34))“ und „Internationale Zusammenarbeit (Kapitel V (Artikel 35 bis 52))“).

Nach Artikel 4 sind die Straftaten, die in den anderen geltenden Übereinkommen und Protokollen der Vereinten Nationen (deren Vertragspartei die Vertragsstaaten sind) festgelegt sind, unabhängig davon unter Strafe zu stellen, ob sie offline oder online begangen werden. Absatz 2 schränkt den Anwendungsbereich dieses Artikels durch die ausdrückliche Feststellung ein, dass diese Bestimmung keine Rechtsgrundlage für die Schaffung neuer oder zusätzlicher Straftatbestände bietet, die über die in den geltenden Übereinkommen und Protokollen der Vereinten Nationen festgelegten Straftaten hinausgehen.

Artikel 5 ist eine Standardbestimmung über die Achtung des Grundsatzes der Souveränität, in die der Wortlaut der entsprechenden Bestimmungen des UNTOC und des UNCAC übernommen wurde.

Artikel 6 ist im Vergleich zu den beiden Strafrechtsinstrumenten der Vereinten Nationen und dem Budapester Übereinkommen eine bisher einmalige Bestimmung. Er enthält eine klare Abgrenzung des Ziels und Zwecks des Übereinkommens und dient als wichtige Garantie zur Verhinderung einer unangemessenen Nutzung des Übereinkommens. Absatz 1 nennt als übergeordnetes hochrangiges Ziel, dass Richtschnur für alle Maßnahmen zur Durchführung des Übereinkommens die von jedem Vertragsstaat eingegangenen internationalen Menschenrechtsverpflichtungen sein müssen. Absatz 2 nimmt dieses Ziel als Grundlage und bekräftigt, dass das Übereinkommen nicht für die Zwecke einer Verletzung von Menschenrechten ausgelegt werden darf, unabhängig davon, ob es sich um wirtschaftliche, soziale und kulturelle oder um bürgerliche und politische Rechte handelt. Diese Bestimmung

---

22 *UNODC Model Law on Mutual Assistance in Criminal Matters* (2007) in der geänderten Fassung mit Bestimmungen über elektronische Beweismittel und den Einsatz spezieller Ermittlungstechniken (2022); E/CN.15/2022/CRP.6.

23 Siehe Artikel 3 Nummer 12 der Verordnung (EU) 2023/1543 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren.

enthält eine nicht abschließende Liste von Rechten, bei denen die Gefahr einer Verletzung durch Maßnahmen zur Bekämpfung der Cyberkriminalität als besonders groß angesehen wird, darunter die Freiheit der Meinungsäußerung, die Gewissensfreiheit, die Meinungsfreiheit, die Religions- und Weltanschauungsfreiheit, die Versammlungsfreiheit und die Vereinigungsfreiheit. Deshalb wird der Anwendungsbereich des Übereinkommens auch durch diese Bestimmung begrenzt, wodurch künftige Versuche von Vertragsstaaten, nach dem Übereinkommen getroffene Maßnahmen der internationalen Zusammenarbeit zu extensiv anzuwenden, verhindert werden.

Kriminalisierung (Kapitel II (Artikel 7 bis 21))

In den Artikeln 7 bis 17 wird die Harmonisierung der Kriminalisierung von Verhaltensweisen und Elementen von durch den Cyberraum bedingten Straftaten und bestimmten durch den Cyberraum ermöglichten Straftaten festgelegt. Die Definition der durch den Cyberraum bedingten Straftaten (Artikel 7 bis 11) orientiert sich an den im Budapester Übereinkommen festgelegten Straftaten. Die Definition der durch den Cyberraum ermöglichten Straftaten (Artikel 12 bis 16) orientiert sich ebenfalls am Budapester Übereinkommen und harmonisiert unter anderem den Straftatbestand des Betrugs im Zusammenhang mit Informations- und Kommunikationstechnologiesystemen (einschließlich des Internetbetrugs („Scam“) als Betrugsform), die Straftatbestände im Zusammenhang mit Darstellungen sexuellen Missbrauchs von Kindern im Internet sowie die Straftatbestände der Kontaktaufnahme zum Zwecke der Begehung einer Sexualstraftat gegen ein Kind und der nicht einvernehmlichen Verbreitung intimer Bilder. Für alle im Übereinkommen festgelegten Straftaten müssen zwei wesentliche Elemente erfüllt sein: Vorsatz und unrechtmäßige Begehung der Tat. Der Begriff „unrechtmäßig“ ist eine kontextspezifische Voraussetzung für die strafrechtliche Verantwortlichkeit, die den Vertragsstaaten eine flexible Anwendung im Einklang mit ihrem innerstaatlichen Recht und ihren internationalen Verpflichtungen ermöglicht. In diesem Zusammenhang soll mit der Voraussetzung „unrechtmäßig“ sichergestellt werden, dass beispielsweise Verhaltensweisen von Strafverfolgungsbehörden bei der Untersuchung von Straftaten und Verhaltensweisen zu sicherheitsrelevanten, wissenschaftlichen, medizinischen, künstlerischen oder anderen legitimen, gerechtfertigten oder genehmigten Zwecken vom Anwendungsbereich der Kriminalisierung ausgenommen sind. So ist nach Artikel 14 Absatz 4 das Verhalten von Kindern in Bezug auf selbst erstelltes Material, in dem sie dargestellt sind, oder auf die einvernehmliche Herstellung, die einvernehmliche Übermittlung oder den einvernehmlichen Besitz von Material im Sinne des Artikels 14 Absatz 2 Buchstaben a bis c ausdrücklich von der Kriminalisierung ausgenommen, wenn das dargestellte zugrunde liegende Verhalten nach innerstaatlichem Recht rechtmäßig ist und wenn dieses Material ausschließlich für die private und einvernehmliche Nutzung der beteiligten Personen aufbewahrt wird.

Artikel 17, der die Kriminalisierung des Waschens der Erträge aus Straftaten vorschreibt, orientiert sich an den entsprechenden Bestimmungen des UNTOC und des UNCAC. Nach den Auslegungsvermerken zu bestimmten Artikeln des Übereinkommens, die der Resolution zur Annahme des Übereinkommens beigefügt sind, gilt nach Artikel 17 ein Verhalten nur dann als Straftat, wenn es sich bei dem zugrunde liegenden strafbaren Verhalten, das mit der komplexeren Straftat des Waschens der Erträge in Verbindung steht, um eine nach den Artikeln 7 bis 16 des Übereinkommens festgelegte Straftat handelt.

In Artikel 18 wurden die entsprechenden Bestimmungen des UNTOC und des UNCAC zur Festlegung von Mindestvorschriften für die Verantwortlichkeit juristischer Personen für die nach diesem Übereinkommen festgelegten Straftaten (d. h. die in den Artikeln 7 bis 17 festgelegten Straftaten) übernommen. Diese Verantwortlichkeit ist an die Beteiligung der juristischen Person an einer der in den Artikeln 7 bis 17 festgelegten Straftaten geknüpft und

unterliegt der auch für natürliche Personen geltenden Voraussetzung, dass die Tat „vorsätzlich und unrechtmäßig“ begangen worden sein muss, und den Rechtsgrundsätzen des betreffenden Vertragsstaats (Absätze 1 und 2).

Die Artikel 19 und 20 stimmen mit den entsprechenden Bestimmungen des UNTOC und des UNCAC überein und enthalten Mindestvorschriften für die Feststellung der Straftatbestände der Beteiligung, des Versuchs und der Vorbereitung und für die Verjährungsfristen im Einklang mit den innerstaatlichen Rechtsvorschriften der Vertragsstaaten und soweit für die im Übereinkommen festgelegten Straftaten erforderlich. Wenngleich für die Online-Übermittlung und -Kontrolle von Daten, die für eine Straftat relevant sein könnten, die Unterstützung eines Diensteanbieters erforderlich ist, sollen Diensteanbieter, die keine strafbare Absicht verfolgen, nicht nach Artikel 19 verantwortlich sein. Deshalb sind Diensteanbieter nicht verpflichtet, Inhalte aktiv zu überwachen, um der strafrechtlichen Verantwortlichkeit nach dieser Bestimmung zu entgehen.

Artikel 21 orientiert sich ebenfalls am UNTOC und am UNCAC und enthält Mindestvorschriften für die Verfolgung, Aburteilung und Ahndung der nach dem Übereinkommen festgelegten Straftaten. Nach Absatz 4 müssen die Vertragsstaaten sicherstellen, dass jede Person, die wegen einer nach dem Übereinkommen festgelegten Straftat verfolgt wird, über alle Rechte und Garantien verfügt, die mit den internationalen Verpflichtungen der Vertragsstaaten, einschließlich des Rechts auf ein faires Verfahren und der Verteidigungsrechte, im Einklang stehen.

Gerichtliche Zuständigkeit (Kapitel III (Artikel 22))

Auch Artikel 22 spiegelt die entsprechenden Bestimmungen des UNTOC, des UNCAC und des Budapester Übereinkommens wider und regelt, soweit erforderlich, die Festlegung obligatorischer und fakultativer Formen der gerichtlichen Zuständigkeit für die nach dem Übereinkommen festgelegten Straftaten.

Verfahrensrechtliche Maßnahmen und Strafverfolgung (Kapitel IV (Artikel 23 bis 34))

Artikel 23 bestimmt den Umfang der innerstaatlichen Befugnisse und verfahrensrechtlichen Maßnahmen, die für die internationale Zusammenarbeit erforderlich sind. Er gilt für spezifische strafrechtliche Ermittlungen oder Verfahren im Zusammenhang mit den nach dem Übereinkommen festgelegten Straftaten und anderen Straftaten, die mithilfe eines Informations- und Kommunikationstechnologiesystems begangen wurden, sowie für die Erhebung elektronischer Beweismittel für Straftaten. In den Auslegungsvermerken zu bestimmten Artikeln des Übereinkommens, die der Resolution zur Annahme des Übereinkommens beigefügt sind, heißt es: „Der Begriff ‚strafrechtliche Ermittlungen“ umfasst Situationen, in denen aufgrund tatsächlicher Umstände Grund zu der Annahme besteht, dass eine Straftat (einschließlich einer Straftat nach Artikel 19 des Übereinkommens) begangen wurde oder begangen wird, auch wenn diese Ermittlungen darauf abzielen, die Begehung der betreffenden Straftat zu unterbinden oder zu behindern.“ Somit bietet das Übereinkommen keine Grundlage für eine internationale Zusammenarbeit zu präventiven Zwecken; Daten dürfen nur ausgetauscht werden, wenn es sich um spezifische strafrechtliche Ermittlungen handelt.

Artikel 24 übernimmt mit einigen Änderungen den entsprechenden Wortlaut des Artikels 15 des Budapester Übereinkommens. Er sieht übergeordnete Bedingungen und Garantien vor, die bei den in Kapitel IV festgelegten Befugnissen und Verfahren einen angemessenen Schutz der Grundrechte, einschließlich der Anwendung des Grundsatzes der Verhältnismäßigkeit, sicherstellen sollen. Zu diesen Bedingungen und Garantien gehören unter anderem die gerichtliche oder andere unabhängige Überprüfung, das Recht auf einen wirksamen

Rechtsbehelf, die die Anwendung rechtfertigenden Gründe und die Begrenzung des Umfangs und der Dauer der genannten Befugnisse oder Verfahren. Ferner gelten die nach diesem Artikel festgelegten Bedingungen und Garantien auf innerstaatlicher Ebene für die in Kapitel IV festgelegten Befugnisse und Verfahren sowohl für die Zwecke innerstaatlicher strafrechtlicher Ermittlungen und Verfahren als auch für die Zwecke der internationalen Zusammenarbeit des ersuchten Vertragsstaats nach Kapitel V.

Die Artikel 25 bis 30 orientieren sich an den entsprechenden innerstaatlichen Befugnissen und verfahrensrechtlichen Maßnahmen des Budapester Übereinkommens. Hierzu zählen die beschleunigte Sicherung gespeicherter elektronischer Daten, die beschleunigte Sicherung und teilweise Offenlegung von Verkehrsdaten, die Herausgabeanordnung, die Durchsuchung und die Beschlagnahme gespeicherter elektronischer Daten sowie die Erhebung von Verkehrsdaten in Echtzeit und das Abfangen von Inhaltsdaten.

Artikel 31 spiegelt Artikel 31 des UNCAC wider. Er verpflichtet die Vertragsstaaten, Maßnahmen zu treffen, die die Sicherstellung, Beschlagnahme und Einziehung der Erträge aus Straftaten ermöglichen.

Artikel 32, der sich am UNTOC und am UNCAC orientiert, bietet den Vertragsstaaten die Möglichkeit, Strafregister zu führen, um die entsprechenden Informationen in Strafverfahren im Zusammenhang mit den nach dem Übereinkommen festgelegten Straftaten zu verwenden.

Artikel 33 orientiert sich am UNTOC und verpflichtet die Vertragsstaaten, im Einklang mit ihren innerstaatlichen Rechtsvorschriften geeignete Maßnahmen zu treffen, um Zeugen angemessen zu schützen.

Artikel 34 orientiert sich am UNTOC und verpflichtet die Vertragsstaaten, im Einklang mit ihren innerstaatlichen Rechtsvorschriften geeignete Maßnahmen zu treffen, um Opfern, insbesondere Opfern der in den Artikeln 14 bis 16 des Übereinkommens festgelegten Straftaten, angemessene Hilfe zu leisten. Nach Artikel 34 müssen die Vertragsstaaten bei der Anwendung von dessen Absätzen 2 bis 4 das Alter, das Geschlecht und die besonderen Umstände und Bedürfnisse der Opfer, einschließlich der besonderen Umstände und Bedürfnisse von Kindern, berücksichtigen. In Absatz 6 werden die Vertragsstaaten aufgefordert, wirksame Maßnahmen zu treffen, um sicherzustellen, dass Anträgen auf Entfernung oder Unzugänglichmachung der in den Artikeln 14 und 16 des Übereinkommens beschriebenen Inhalte in dem Umfang stattgegeben wird, der ihrem innerstaatlichen Rechtsrahmen entspricht.

Internationale Zusammenarbeit (Kapitel V (Artikel 35 bis 52))

In Artikel 35 sind die allgemeinen Grundsätze und der Anwendungsbereich der internationalen Zusammenarbeit festgelegt, in dem die Vertragsstaaten verpflichtet sind, zum Zwecke der Untersuchung und Verfolgung von nach dem Übereinkommen festgelegten Straftaten und der Erhebung und Weitergabe diesbezüglicher elektronischer Beweismittel sowie zum Zwecke der Erhebung und Weitergabe elektronischer Beweismittel für schwere Straftaten, die mit einer Freiheitsstrafe im Höchstmaß von mindestens vier Jahren oder einer schwereren Strafe bewehrt sind, zusammenzuarbeiten. Der Anwendungsbereich der internationalen Zusammenarbeit ist somit auf nach dem Übereinkommen festgelegte Straftaten und schwere Straftaten mit einem bestimmten Mindeststrafmaß begrenzt.

Artikel 36 enthält eine ausdrückliche Bestimmung über den Schutz personenbezogener Daten. In dieser Bestimmung ist die Übermittlung personenbezogener Daten im Rahmen der internationalen Zusammenarbeit geregelt. Die Übermittlung darf nur im Einklang mit dem innerstaatlichen Recht und den völkerrechtlichen Verpflichtungen des übermittelnden Vertragsstaats erfolgen. Die Vertragsstaaten können die Übermittlung personenbezogener

Daten ablehnen, wenn die Daten nicht im Einklang mit ihren geltenden Rechtsvorschriften über den Schutz personenbezogener Daten bereitgestellt werden können. Für die EU bedeutet dies, dass wichtige Datenschutzgrundsätze, unter anderem Zweckbindung, Datenminimierung, Verhältnismäßigkeit und Notwendigkeit, im Einklang mit der Charta der Grundrechte der Europäischen Union angewendet werden müssen, bevor personenbezogene Daten einem anderen Vertragsstaat übermittelt werden können. Die Vertragsstaaten können sich auch bemühen, zur Einhaltung der Vorschriften geeignete Bedingungen festzulegen, um einem Ersuchen um personenbezogene Daten nachkommen zu können. Die Vertragsstaaten müssen sicherstellen, dass für personenbezogene Daten, die sie nach dem Übereinkommen erhalten, in ihrem jeweiligen Rechtsrahmen wirksame und geeignete Garantien gelten. Die Vertragsstaaten dürfen die erhaltenen personenbezogenen Daten einem Drittland oder einer internationalen Organisation nur mit vorheriger Genehmigung des ursprünglichen übermittelnden Vertragsstaats übermitteln, der verlangen kann, dass eine solche Genehmigung schriftlich erteilt werden muss.

Artikel 37, der sich am UNCAC und am Budapester Übereinkommen orientiert, enthält detaillierte Vorschriften über die Auslieferung. Nach Absatz 8 erlaubt das Übereinkommen die Ablehnung einer Auslieferung auf der Grundlage von Bedingungen, die im nationalen Recht des ersuchten Vertragsstaats festgelegt sind. Absatz 15 sieht einen weiteren Grund für die Ablehnung eines Auslieferungsersuchens vor, wenn dieses zum Zwecke der Verfolgung oder Bestrafung einer Person aufgrund ihres Geschlechts, ihrer Sprache, ihrer Religion, ihrer Staatsangehörigkeit, ihrer ethnischen Herkunft oder ihrer politischen Überzeugungen gestellt wurde oder wenn die Erledigung des Ersuchens aus einem dieser Gründe die Stellung der Person beeinträchtigen würde.

Die Artikel 38 und 39, die sich am UNTOC und am UNCAC orientieren, sehen die Möglichkeit vor, verurteilte Personen zu überstellen und die Strafverfolgung zu übertragen.

Artikel 40 entspricht den Bestimmungen des UNTOC, des UNCAC und des Budapester Übereinkommens und enthält detaillierte Bestimmungen über die Grundsätze und Verfahren der Rechtshilfe. Nach Absatz 17 sind Rechtshilfeersuchen nach dem innerstaatlichen Recht des ersuchten Vertragsstaats zu erledigen. Absatz 19 verbietet es einem ersuchenden Vertragsstaat, Informationen oder Beweismittel, die vom ersuchten Vertragsstaat geliefert wurden, ohne vorherige Zustimmung des ersuchten Vertragsstaats für andere als die im Ersuchen genannten Ermittlungen, Strafverfolgungsmaßnahmen oder Gerichtsverfahren zu übermitteln oder zu verwenden. Die Absätze 8, 21 und 22 enthalten umfassende Gründe für die Ablehnung von Rechtshilfeersuchen, wie im Abschnitt „Grundrechte“ beschrieben.

Mit Artikel 41, der sich an Artikel 35 des Budapester Übereinkommens orientiert, werden die Vertragsstaaten verpflichtet, rund um die Uhr verfügbare Netze einzurichten, die Unterstützung bei spezifischen Ermittlungen, Strafverfolgungsmaßnahmen oder Gerichtsverfahren im Zusammenhang mit den nach dem Übereinkommen festgelegten Straftaten oder bei der Erhebung elektronischer Beweismittel bieten.

In den Artikeln 42 bis 46, die den Artikeln 29 bis 33 des Budapester Übereinkommens entsprechen, sind die Einzelheiten zu bestimmten Arten von Maßnahmen der internationalen Zusammenarbeit im Bereich der Rechtshilfe festgelegt. Hierzu zählen die beschleunigte Sicherung gespeicherter elektronischer Daten, die beschleunigte Offenlegung gesicherter Verkehrsdaten, der Zugriff auf gespeicherte elektronische Daten sowie die Erhebung von Verkehrsdaten in Echtzeit und das Abfangen von Inhaltsdaten. Hinsichtlich der einschneidendsten Maßnahmen – Erhebung von Verkehrsdaten in Echtzeit und Abfangen von Inhaltsdaten – haben die Vertragsstaaten die stärker begrenzte Verpflichtung, sich zu „bemühen“, eine solche Unterstützung zu leisten. Diese Verpflichtung stellt im Wesentlichen

eine Handlungspflicht dar und ist daher für die Vertragsstaaten weniger zwingend als die Verpflichtungen im Zusammenhang mit anderen Rechtshilfemaßnahmen, die eine Zusammenarbeit mit anderen Vertragsstaaten erfordern, es sei denn, die geltenden Bedingungen sind nicht erfüllt oder einer der anwendbaren Ablehnungsgründe wird geltend gemacht. Ferner kann um Unterstützung beim Abfangen von Inhaltsdaten nur bei schweren Straftaten ersucht werden, soweit dies nach den für die Vertragsstaaten geltenden Verträgen oder nach ihren innerstaatlichen Rechtsvorschriften zulässig ist.

Mit den Artikeln 47 und 48, die sich am UNTOC und am UNCAC orientieren, werden die Vertragsstaaten aufgefordert zusammenzuarbeiten, um die Strafverfolgung zur Bekämpfung der nach dem Übereinkommen festgelegten Straftaten zu verbessern und für diesen Zweck gemeinsame Ermittlungsstellen einzurichten.

Die Artikel 49 bis 52, die sich am UNTOC und/oder am UNCAC orientieren. enthalten Mindestvorschriften für Maßnahmen zur Einziehung, Abschöpfung und Rückgabe der Erträge aus den nach dem Übereinkommen festgelegten Straftaten oder der durch sie erlangten Vermögensgegenstände.

Präventivmaßnahmen (Kapitel VI (Artikel 53))

Mit Artikel 53 werden die Vertragsstaaten aufgefordert, sich im Einklang mit den wesentlichen Grundsätzen ihrer Rechtsordnung darum zu bemühen, wirksame und koordinierte Strategien und bewährte Verfahren zu erarbeiten und umzusetzen oder beizubehalten, um bestehende oder künftige Möglichkeiten für Cyberkriminalität durch geeignete legislative, administrative oder sonstige Maßnahmen einzuschränken. Die Vertragsstaaten sollen die aktive Beteiligung relevanter Einzelner und Einrichtungen außerhalb des öffentlichen Sektors, wie nichtstaatliche Organisationen, Organisationen der Zivilgesellschaft, akademische Einrichtungen und privatwirtschaftliche Unternehmen, sowie der breiten Öffentlichkeit an den einschlägigen Aspekten der Verhütung der nach dem Übereinkommen festgelegten Straftaten fördern. Absatz 3 enthält eine nicht abschließende und nicht verbindliche Liste von Präventivmaßnahmen. Absatz 3 Buchstabe e enthält einen ausdrücklichen Verweis auf Präventivmaßnahmen, mit denen die Beiträge der legitimen Tätigkeiten von Sicherheitsforschern anerkannt werden, wenn sie ausschließlich darauf abzielen, die Sicherheit der Produkte, Dienstleistungen und Kunden von Diensteanbietern zu stärken und zu verbessern.

Technische Hilfe und Informationsaustausch (Kapitel VII (Artikel 54 bis 56))

In den Artikeln 54 bis 56, die sich am UNTOC und/oder am UNCAC orientieren, sind Bestimmungen über technische Hilfe, Kapazitätsaufbau und Informationsaustausch unter besonderer Berücksichtigung der Interessen und Bedürfnisse der Vertragsstaaten, die Entwicklungsländer sind, festgelegt.

Durchführungsmechanismus (Kapitel VIII (Artikel 57 bis 58))

In den Artikeln 57 und 58, die sich am UNCAC orientieren, sind Einzelheiten zur Konferenz der Vertragsstaaten festgelegt, die die Durchführung des Übereinkommens überwachen und für die Ausarbeitung und Annahme von Zusatzprotokollen zum Übereinkommen auf der Grundlage der Artikel 61 und 62 des Übereinkommens zuständig sein wird. Der Generalsekretär der Vereinten Nationen stellt die Sekretariatsdienstleistungen zur Verfügung und beruft spätestens ein Jahr nach Inkrafttreten des Übereinkommens die Konferenz der Vertragsstaaten ein. Danach finden regelmäßige Tagungen der Konferenz nach Maßgabe der von der Konferenz angenommenen Geschäftsordnung statt.

Schlussbestimmungen (Kapitel IX (Artikel 59 bis 68))

Kapitel IX des Übereinkommens enthält die Schlussbestimmungen. Unter anderem gewährleistet Artikel 60 Absatz 1, dass EU-Mitgliedstaaten, die Vertragspartei des Übereinkommens sind, in ihren Beziehungen untereinander weiterhin Unionsrecht anwenden können. Ferner können die Vertragsparteien des Budapester Übereinkommens und anderer internationaler Instrumente diese Instrumente untereinander weiterhin anwenden.

Nach Artikel 64 Absatz 1 liegt das Übereinkommen im Oktober 2025 in Hanoi und danach bis zum 31. Dezember 2026 am Sitz der Vereinten Nationen in New York für alle Staaten zur Unterzeichnung auf. Nach Absatz 2 liegt das Übereinkommen auch für Organisationen der regionalen Wirtschaftsintegration wie die Union zur Unterzeichnung auf, sofern mindestens ein Mitgliedstaat das Übereinkommen nach Absatz 1 unterzeichnet hat.

Nach Artikel 64 Absatz 3 und Artikel 65 Absatz 1 tritt das Übereinkommen in Kraft, sobald vierzig Staaten ihre Zustimmung ausgedrückt haben, durch das Übereinkommen gebunden zu sein, indem sie ihre Ratifikations-, Annahme- oder Genehmigungsurkunde beim Generalsekretär der Vereinten Nationen hinterlegt haben. Organisationen der regionalen Wirtschaftsintegration wie die Union können ihre Ratifikations-, Annahme- oder Genehmigungsurkunde hinterlegen, wenn mindestens einer ihrer Mitgliedstaaten dies ebenfalls getan hat. In ihrer Ratifikations-, Annahme- oder Genehmigungsurkunde muss die Organisation der regionalen Wirtschaftsintegration erklären, in welchem Umfang sie für die im Übereinkommen geregelten Angelegenheiten zuständig ist. Nach Artikel 64 Absatz 4 steht das Übereinkommen Organisationen der regionalen Wirtschaftsintegration wie der Union unter der Voraussetzung zum Beitritt offen, dass mindestens ein Mitgliedstaat Vertragspartei des Übereinkommens ist. Zum Zeitpunkt ihres Beitritts muss die Union erklären, in welchem Umfang sie für die im Übereinkommen geregelten Angelegenheiten zuständig ist.

Nach Artikel 66 Absatz 1 kann ein Vertragsstaat nach Ablauf von fünf Jahren nach Inkrafttreten dieses Übereinkommens eine Änderung vorschlagen und sie dem Generalsekretär der Vereinten Nationen übermitteln; dieser leitet die vorgeschlagene Änderung dann den Vertragsstaaten und der Konferenz der Vertragsstaaten des Übereinkommens zu, damit diese den Vorschlag prüfen und darüber entscheiden. Nach Absatz 2 üben Organisationen der regionalen Wirtschaftsintegration wie die Union in Angelegenheiten, die in ihre Zuständigkeit fallen, ihr Stimmrecht mit der Zahl der Stimmen ausüben, die der Zahl ihrer Mitgliedstaaten entspricht, die Vertragspartei des Übereinkommens sind. Eine im Einklang mit Absatz 1 angenommene Änderung bedarf der Ratifikation, Annahme oder Genehmigung durch die Vertragsstaaten.

Die Artikel 61 und 62 enthalten Vorschriften für Zusatzprotokolle zum Übereinkommen. Artikel 61 Absatz 2 gestattet es Organisationen der regionalen Wirtschaftsintegration wie der Union nur dann, Vertragspartei eines Protokolls zu werden, wenn die Organisation Vertragspartei des Übereinkommens ist. Nach Absatz 4 ist jedes Protokoll zum Übereinkommen zusammen mit dem Übereinkommen auszulegen, wobei dem Zweck des betreffenden Protokolls Rechnung zu tragen ist. Artikel 62 Absatz 1 verlangt, dass ein Zusatzprotokoll von mindestens sechzig Vertragsstaaten unterstützt werden muss, bevor seine Annahme von der Konferenz der Vertragsstaaten geprüft werden kann. Dieser Artikel sieht ferner vor, dass die Konferenz der Vertragsstaaten alle Anstrengungen unternimmt, um Konsens über ein Zusatzprotokoll zu erzielen, und dass nur dann, wenn alle Anstrengungen ausgeschöpft sind, für seine Annahme als letztes Mittel eine Mehrheit von mindestens zwei Dritteln der auf der Tagung der Konferenz der Vertragsstaaten anwesenden und abstimmenden Vertragsstaaten verlangt wird. Nach Artikel 62 Absatz 2 üben Organisationen der regionalen Wirtschaftsintegration wie die Union in Angelegenheiten, die in ihre

Zuständigkeit fallen, ihr Stimmrecht nach diesem Artikel mit der Zahl von Stimmen aus, die der Zahl ihrer Mitgliedstaaten entspricht, die Vertragspartei des Übereinkommens sind.

Nach Artikel 67 Absatz 2 sind Organisationen der regionalen Wirtschaftsintegration wie die Union nicht mehr Vertragspartei des Übereinkommens, wenn alle ihre Mitgliedstaaten das Übereinkommen gekündigt haben.

Der Resolution zur Annahme des Übereinkommens sind Auslegungsvermerke zu den Artikeln 2, 17, 23 und 35 beigefügt. Solche Auslegungsvermerke bieten keine verbindliche Auslegung des Übereinkommens, sondern sollen die Vertragsparteien bei dessen Anwendung leiten und unterstützen. In den während der Verhandlungen verteilten Auslegungsvermerken des Vorsitzenden des Ad-hoc-Ausschusses der Vereinten Nationen sind ebenfalls mehrere zentrale Aspekte der Auslegung behandelt. Die Website des Ad-hoc-Ausschusses enthält alle während der Verhandlungen erstellten Vorschläge und Fassungen des Entwurfs des Übereinkommens, bietet somit nützliche Informationen über die Entwicklung der zentralen Bestimmungen innerhalb des Textes und kann für die Auslegung von Bedeutung sein. Ferner kann auch der Erläuternde Bericht zum Budapester Übereinkommen[24] als nützliches, wenn auch informelles Instrument zur Information der Staaten über viele Bestimmungen dienen, die sich am Budapester Übereinkommen orientieren, wie die meisten Bestimmungen des Übereinkommens über Strafbarkeit und Verfahrensbefugnisse.

[24] Sammlung Europäischer Verträge – Nr. 185.

2025/0230 (NLE)

Vorschlag für einen

BESCHLUSS DES RATES

über die Unterzeichnung – im Namen der Europäischen Union – des Übereinkommens der Vereinten Nationen gegen Cyberkriminalität; Stärkung der internationalen Zusammenarbeit bei der Bekämpfung bestimmter mithilfe von Informations- und Kommunikationstechnologiesystemen begangener Straftaten und bei der Weitergabe von Beweismitteln in elektronischer Form für schwere Straftaten

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16, Artikel 82 Absatz 1, Artikel 83 Absatz 1 und Artikel 87 Absatz 2 in Verbindung mit Artikel 218 Absatz 5,

auf Vorschlag der Europäischen Kommission,

in Erwägung nachstehender Gründe:

(1) Am 24. Mai 2022 wurde die Kommission mit dem Beschluss (EU) 2022/895 des Rates ermächtigt, im Namen der Europäischen Union an den Verhandlungen über ein Übereinkommen der Vereinten Nationen gegen Cyberkriminalität teilzunehmen.

(2) Der Wortlaut des Übereinkommens der Vereinten Nationen gegen Cyberkriminalität; Stärkung der internationalen Zusammenarbeit bei der Bekämpfung bestimmter mithilfe von Informations- und Kommunikationstechnologiesystemen begangener Straftaten und bei der Weitergabe von Beweismitteln in elektronischer Form für schwere Straftaten (im Folgenden „Übereinkommen“) wurde am 24. Dezember 2024 von der Generalversammlung der Vereinten Nationen angenommen und soll am 25. Oktober 2025 in Hanoi (Vietnam) und danach bis zum 31. Dezember 2026 am Sitz der Vereinten Nationen in New York zur Unterzeichnung aufgelegt werden.

(3) Das Übereinkommen steht mit den in Artikel 67 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union genannten Sicherheitszielen der Europäischen Union im Einklang, nämlich durch Maßnahmen zur Verhütung und Bekämpfung von Kriminalität und durch Maßnahmen zur Koordinierung und Zusammenarbeit von Polizeibehörden und Organen der Strafrechtspflege und den anderen zuständigen Behörden sowie durch die Angleichung der strafrechtlichen Rechtsvorschriften ein hohes Maß an Sicherheit zu gewährleisten.

(4) Die Bestimmungen des Übereinkommens gelten für spezifische strafrechtliche Ermittlungen oder Verfahren im Zusammenhang mit den nach dem Übereinkommen festgelegten Straftaten und erlauben einen Datenaustausch nur zu diesem Zweck.

(5) Mit dem Übereinkommen wird eine begrenzte Zahl klar definierter Straftatbestände harmonisiert, gleichzeitig jedoch den Vertragsstaaten die notwendige Flexibilität geboten, um eine Überkriminalisierung in Bezug auf legitimes Verhalten zu vermeiden.

(6) Das Übereinkommen enthält nur Mindestvorschriften über die Verantwortlichkeit juristischer Personen für die darin festgelegten Straftaten, verlangt aber nicht, dass eine

solche strafrechtliche Verantwortlichkeit in einer Weise geregelt wird, die mit den Rechtsgrundsätzen eines Vertragsstaats unvereinbar wäre.

(7) Das Übereinkommen steht auch mit den Zielen der Europäischen Union zum Schutz personenbezogener Daten, der Privatsphäre und der Grundrechte nach Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union und der Charta der Grundrechte der Europäischen Union im Einklang.

(8) Das Übereinkommen sieht solide Menschenrechtsgarantien vor und schließt jede Auslegung aus, die zur Unterdrückung von Menschenrechten oder Grundfreiheiten, insbesondere der Freiheit der Meinungsäußerung, der Gewissensfreiheit, der Meinungsfreiheit, der Religions- und Weltanschauungsfreiheit, der Versammlungsfreiheit und der Vereinigungsfreiheit, führen würde. Mit diesen Garantien wird auch gewährleistet, dass eine internationale Zusammenarbeit abgelehnt werden kann, wenn sie gegen innerstaatliche Rechtsvorschriften der Vertragsstaaten verstoßen würde oder eine solche Ablehnung erforderlich wäre, um jede Form von Diskriminierung zu vermeiden.

(9) In Bezug auf die Befugnisse und Verfahrensmaßnahmen sowohl auf innerstaatlicher als auch auf internationaler Ebene sieht das Übereinkommen horizontale Bedingungen und Garantien vor, die den Schutz der Menschenrechte im Einklang mit den Verpflichtungen der Vertragsstaaten nach den internationalen Menschenrechtsnormen sicherstellen und die den Grundsatz der Verhältnismäßigkeit umfassen. Zu diesen Bedingungen und Garantien gehören unter anderem die gerichtliche oder andere unabhängige Überprüfung, das Recht auf einen wirksamen Rechtsbehelf, die die Anwendung rechtfertigenden Gründe und die Begrenzung des Umfangs und der Dauer der Befugnisse und Verfahren.

(10) Das Übereinkommen enthält eine eigene Bestimmung über den Schutz personenbezogener Daten, mit der sichergestellt wird, dass wichtige Datenschutzgrundsätze, unter anderem Zweckbindung, Datenminimierung, Verhältnismäßigkeit und Notwendigkeit, im Einklang mit der Charta der Grundrechte der Europäischen Union angewendet werden müssen, bevor personenbezogene Daten einem anderen Vertragsstaat zur Verfügung gestellt werden können.

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

(12) Damit die Vereinbarkeit des Übereinkommens mit Recht und Politik der Union sowie die einheitliche Anwendung des Übereinkommens durch die Mitgliedstaaten in ihren Beziehungen zu Vertragsstaaten, die keine EU-Mitgliedstaaten sind, und die wirksame Anwendung des Übereinkommens gewährleistet sind, ist eine Reihe von Vorbehalten und Notifikationen von Belang.

(13) Die Vorbehalte und Notifikationen, zu denen Anhang I dieses Beschlusses Leitlinien enthält, lassen andere Vorbehalte oder Erklärungen unberührt, die die Mitgliedstaaten gegebenenfalls individuell vorlegen möchten, soweit dies zulässig ist.

(14) Da das Übereinkommen Verfahren zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln und ein hohes Maß an Garantien vorsieht, wird die Kohärenz in den Anstrengungen der Europäischen Union zur Bekämpfung der Cyberkriminalität und anderer Formen der Kriminalität auf globaler Ebene gefördert, wenn die Europäische Union Vertragspartei des Übereinkommens wird. Damit wird die Zusammenarbeit zwischen den Vertragsstaaten des Übereinkommens, die EU-Mitgliedstaaten sind, und denen, die keine

EU-Mitgliedstaaten sind, erleichtert und gleichzeitig ein hohes Schutzniveau für den Einzelnen gewährleistet.

(15) Nach seinem Artikel 64 liegt das Übereinkommen für die Union zur Unterzeichnung auf.

(16) Die Union sollte neben ihren Mitgliedstaaten Vertragspartei des Übereinkommens werden, da sowohl die Union als auch ihre Mitgliedstaaten über Zuständigkeiten in den unter das Übereinkommen fallenden Bereichen verfügen. Dieser Beschluss berührt nicht die Unterzeichnung des Übereinkommens durch die Mitgliedstaaten nach ihren internen Verfahren.

(17) Durch die zeitnahe Unterzeichnung des Übereinkommens durch die Europäische Union wird ferner sichergestellt, dass die Union frühzeitig ein Mitspracherecht bei der Umsetzung dieses neuen globalen Rahmens für die Bekämpfung der Cyberkriminalität erhält.

(18) Der Europäische Datenschutzbeauftragte wurde nach Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates konsultiert und hat am […] eine Stellungnahme abgegeben.

(19) [Nach Artikel 3 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 hat Irland [*mit Schreiben vom …*] mitgeteilt, dass es sich an der Annahme und Anwendung dieses Beschlusses beteiligen möchte.]

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 beteiligt sich Irland nicht an der Annahme dieses Beschlusses, der daher weder für Irland bindend noch Irland gegenüber anwendbar ist.]

(20) 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 des Königreichs Dänemarks beteiligt sich das Königreich Dänemark nicht an der Annahme dieses Beschlusses, der daher weder für das Königreich Dänemark bindend noch dem Königreich Dänemark gegenüber anwendbar ist.

(21) Das Übereinkommen sollte unterzeichnet und die beigefügten Vorbehalte und Notifikationen sollten genehmigt werden —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Die Unterzeichnung des Übereinkommens der Vereinten Nationen gegen Cyberkriminalität; Stärkung der internationalen Zusammenarbeit bei der Bekämpfung bestimmter mithilfe von Informations- und Kommunikationstechnologiesystemen begangener Straftaten und bei der Weitergabe von Beweismitteln in elektronischer Form für schwere Straftaten (im Folgenden „Übereinkommen“) wird – vorbehaltlich des Abschlusses – im Namen der Europäischen Union genehmigt.

Der Wortlaut des Übereinkommens ist diesem Beschluss beigefügt (Anhang II).

Artikel 2

Die diesem Beschluss in Anhang I beigefügten Vorbehalte und Notifikationen werden genehmigt.

Artikel 3

Dieser Beschluss tritt am Tag nach seiner Annahme in Kraft.

Geschehen zu Brüssel am

Im Namen des Rates
Der Präsident/Die Präsidentin
[…]