



EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data
protection authority

18. Mai 2022

Stellungnahme 9/2022

zu der Empfehlung für einen Beschluss des Rates zur Ermächtigung von Verhandlungen über ein umfassendes internationales Übereinkommen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien für kriminelle Zwecke

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 52 Absatz 2 der Verordnung (EU) 2018/1725 im „Hinblick auf die Verarbeitung personenbezogener Daten ... sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Datenschutz, von den Organen und Einrichtungen der Union geachtet werden“; gemäß Artikel 52 Absatz 3 ist er „für die Beratung der Organe und Einrichtungen der Union und der betroffenen Personen in allen Fragen der Verarbeitung personenbezogener Daten“ zuständig.

Am 5. Dezember 2019 wurde Wojciech Rafał Wiewiorowski für einen Zeitraum von fünf Jahren zum Europäischen Datenschutzbeauftragten ernannt.

Artikel 42 Absatz 1 der Verordnung 2018/1725 besagt: „Nach der Annahme von Vorschlägen für einen Gesetzgebungsakt, für Empfehlungen oder Vorschläge an den Rat nach Artikel 218 AEUV sowie bei der Ausarbeitung von delegierten Rechtsakten und Durchführungsrechtsakten, die Auswirkungen auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten haben, konsultiert die Kommission den EDSB“, und gemäß Artikel 57 Absatz 1 Buchstabe g muss der EDSB „von sich aus oder auf Anfrage alle Organe und Einrichtungen der Union bei legislativen und administrativen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten beraten.“

Diese Stellungnahme ergeht im Hinblick auf den Auftrag des EDSB, die Organe der Union bezüglich der kohärenten und konsequenten Anwendung der unionsrechtlichen Datenschutzgrundsätze im Zusammenhang mit der Aushandlung von Abkommen mit Drittländern im Bereich der Strafverfolgung zu beraten. Dieser Stellungnahme liegt die allgemeine Verpflichtung zugrunde, dass internationale Abkommen den Bestimmungen des AEUV genügen und die Grundrechte, die den Kern des Unionsrechts ausmachen, wahren müssen. Insbesondere ist die Einhaltung von Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union sowie von Artikel 16 AEUV sicherzustellen.

Die vorliegende Stellungnahme schließt künftige zusätzliche Kommentare oder Empfehlungen des EDSB nicht aus, insbesondere wenn weitere Probleme festgestellt oder neue Informationen bekannt werden. Diese Stellungnahme greift etwaigen künftigen Maßnahmen, die der EDSB in Ausübung seiner Befugnisse gemäß der Verordnung (EU) 2018/1725 ergreifen mag, nicht vor. Die Stellungnahme beschränkt sich auf die Bestimmungen des Vorschlags, die unter dem Blickwinkel des Datenschutzes besonders relevant sind.

Zusammenfassung

Am 29. März 2022 veröffentlichte die Europäische Kommission eine Empfehlung für einen Beschluss des Rates über die Ermächtigung der Kommission, im Namen der Europäischen Union an den Verhandlungen der Vereinten Nationen (VN) über ein umfassendes internationales Übereinkommen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien für kriminelle Zwecke teilzunehmen.

Der EDSB ist sich der Tatsache bewusst, dass Strafverfolgungsbehörden elektronische Beweismittel schnell und effizient sichern und erlangen müssen. Er betont jedoch, dass bereits ein ähnliches internationales Instrument in Kraft ist, nämlich das Budapester Übereinkommen und dessen Zweites Zusatzprotokoll, das nun zur Unterzeichnung aufliegt.

Der EDSB stellt fest, dass in den Vereinten Nationen bereits Verhandlungen über ein anderes Übereinkommen zur Bekämpfung der Cyberkriminalität und die grenzüberschreitende Zusammenarbeit in Strafsachen aufgenommen wurden. Er unterstützt daher die Empfehlung, mit der die Kommission ermächtigt wird, im Namen der EU Verhandlungen zu führen, da dies zu einer besseren Wahrung des durch den EU-Datenschutzrahmen garantierten Schutzniveaus beitragen würde. Der EDSB weist jedoch auf die große Zahl von Ländern innerhalb der Vereinten Nationen mit höchst heterogenen Rechtsordnungen hin. Vor diesem Hintergrund ist der EDSB der Auffassung, dass ein erhebliches Risiko besteht, dass der endgültige Wortlaut des Übereinkommens zu einer Schwächung der im EU-Recht verankerten Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihrer Rechte auf Datenschutz und Privatsphäre, führen könnte. Daher ist zu unterstreichen, dass für den Fall, dass der Rat die Kommission ermächtigt, in diesem Rahmen im Namen der EU Verhandlungen zu führen, eine solche Ermächtigung nicht erfordern würde, dass die EU Vertragspartei des Übereinkommens wird, falls es angenommen wird. Nach Auffassung des EDSB sollte die EU nicht anstreben, Vertragspartei eines solchen Übereinkommens zu sein, falls das durch das EU-Recht garantierte Datenschutzniveau für natürliche Personen untergraben wird.

Die vorliegende Stellungnahme soll den Organen, Einrichtungen und sonstigen Stellen der Union konstruktiven und objektiven Rat in der Frage bieten, wie das vom EU-Recht bereits gewährleistete Datenschutzniveau garantiert nicht untergraben wird. Der EDSB begrüßt, dass mit dem Mandat von Anfang an sichergestellt werden soll, dass das Übereinkommen strenge Bedingungen und starke Garantien enthält, um sicherzustellen, dass die EU-Mitgliedstaaten die Grundrechte, Grundfreiheiten und allgemeinen Grundsätze des EU-Rechts, wie sie in den EU-Verträgen und der Charta der Grundrechte der EU verankert sind, achten und schützen können.

In diesem Zusammenhang betont der EDSB, dass insbesondere die uneingeschränkte Achtung der Grundrechte auf Privatsphäre und auf Schutz personenbezogener Daten sichergestellt werden muss. Das Datenschutzrecht der EU sieht grundsätzlich vor, dass Datenübermittlungen an ein Drittland ohne zusätzliche Anforderungen nur dann erfolgen können, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet. Sichert ein Drittland kein angemessenes Schutzniveau zu, gelten Ausnahmen für spezifische Datenübermittlungen, sofern geeignete Schutzmaßnahmen ergriffen werden. Auch wenn sich der EDSB der Tatsache bewusst ist, dass es nicht möglich ist, die Terminologie und Definitionen des Unionsrechts in einer Vereinbarung mit zahlreichen

Drittländern vollständig zu replizieren, muss doch der Schutz des Einzelnen eindeutig und wirksam geregelt sein, um eine vollumfängliche Übereinstimmung mit dem EU-Recht zu gewährleisten. Der Gerichtshof der Europäischen Union hat in den vergangenen Jahren die Grundsätze des Datenschutzes erneut bestätigt, darunter gerichtlicher Rechtsbehelf und die individuellen Rechte des Einzelnen. Diese Grundsätze sind umso wichtiger, wenn man die Sensibilität der für strafrechtliche Ermittlungen erforderlichen Daten bedenkt.

Vor diesem Hintergrund ist der EDSB der Auffassung, dass viele bereits geplante Verhandlungsrichtlinien zwar zu begrüßen sind, sie aber gestärkt werden sollten. Um insbesondere die Einhaltung der EU-Charta und des Artikels 16 AEUV zu gewährleisten, empfiehlt der EDSB zu den Verhandlungsrichtlinien im Wesentlichen,

- die Bestimmungen über die internationale Zusammenarbeit auf die im Übereinkommen definierten Straftaten zu beschränken;
- den direkten Zugriff auf Daten durch Strafverfolgungsbehörden von Drittländern und die grenzüberschreitende direkte Zusammenarbeit mit Diensteanbietern auszuschließen;
- sicherzustellen, dass künftige bilaterale und multilaterale Abkommen mit Drittländern anstelle des Übereinkommens Anwendung finden, falls diese künftigen Abkommen höhere Standards in Bezug auf den Schutz der Grundrechte, insbesondere des Rechts auf Privatsphäre und Datenschutz, gewährleisten;
- sicherzustellen, dass das Übereinkommen keine Wirkung zwischen zwei Vertragsstaaten entfaltet, wenn einer von ihnen notifiziert, dass die Ratifikation, die Annahme, die Genehmigung oder der Beitritt eines anderen Vertragsstaats keine Beziehungen zwischen diesen beiden Vertragsstaaten nach diesem Übereinkommen begründet.

Darüber hinaus bietet die Stellungnahme weitere Empfehlungen zur Verbesserung und Verdeutlichung der Verhandlungsrichtlinien. Die Anmerkungen in dieser Stellungnahme gelten unbeschadet etwaiger zusätzlicher Anmerkungen, die der EDSB nach dem Aufwerfen weiterer Fragen später vorlegt. Diese würden behandelt, sobald weitere Informationen verfügbar sind. Er geht davon aus, zu einem späteren Zeitpunkt vor der abschließenden Bearbeitung des Entwurfs des Übereinkommens zu dessen Bestimmungen konsultiert zu werden.

INHALT

1. Einleitung.....	5
2. Allgemeine Anmerkungen	7
3. Verhältnis zu anderen Rechtsinstrumenten	9
4. Geltungsbereich	10
4.1. Unter das Übereinkommen fallende Straftaten.....	10
4.2. Ausschluss eines direkten Zugriffs von Strafverfolgungsbehörden auf Daten und ihrer direkten Zusammenarbeit mit Diensteanbietern	11
5. Notwendigkeit detaillierter Garantien in Bezug auf die internationale Übermittlung von Daten und die Achtung von Grundrechten.....	12
6. Aussetzung, Überprüfung des Übereinkommens und Begründung von Beziehungen gemäß dem Übereinkommen	15
7. Schlussfolgerungen.....	15

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr¹, insbesondere auf Artikel 42 Absatz 1 –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einleitung

1. Die Vereinten Nationen (VN) sind eine zwischenstaatliche Organisation, die derzeit 193 Mitgliedstaaten umfasst.² Die Vereinten Nationen und ihre Arbeit orientieren sich an den Zielen und Grundsätzen ihrer Gründungscharta. Gemäß der Charta der Vereinten Nationen gehören zu den Zielen der Organisation die Wahrung des Weltfriedens und der internationalen Sicherheit, der Schutz der Menschenrechte, die Bereitstellung humanitärer Hilfe, die Förderung einer nachhaltigen Entwicklung und die Wahrung des Völkerrechts.³
2. Am 17. Dezember 2018 verabschiedete die Generalversammlung der Vereinten Nationen die Resolution 73/187 über die „Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken“.⁴ In der Folge verabschiedete sie am 27. Dezember 2019 die Resolution 74/247⁵, mit der sie beschloss, einen offenen zwischenstaatlichen Ad-hoc-Sachverständigenausschuss (im Folgenden „Ad-hoc-Ausschuss“) einzusetzen, der ein umfassendes internationales Übereinkommen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken ausarbeiten sollte. In der Resolution 74/247 wird betont, dass die Staaten sich bei der Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien für kriminelle Zwecke besser abstimmen und verstärkt zusammenarbeiten müssen, unter anderem indem sie den Entwicklungsländern auf Antrag technische Hilfe bereitstellen. Ferner wird in der Resolution betont, dass die nationalen Rechtsvorschriften und Rahmen verbessert und die Kapazitäten der nationalen Behörden zur Bekämpfung dieser Nutzung in allen ihren Formen, einschließlich der Prävention, Erkennung, Untersuchung und strafrechtlichen Verfolgung, ausgebaut werden müssen⁶, **wobei die bestehenden internationalen Übereinkünfte und die auf nationaler, regionaler und internationaler Ebene unternommenen Anstrengungen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken in vollem Umfang berücksichtigt werden**, insbesondere die Arbeit und die Ergebnisse der offenen zwischenstaatlichen Sachverständigengruppe für die

¹ ABl. L 295 vom 21.11.2018, S. 39.

² Siehe die Mitgliedstaaten der Vereinten Nationen hier: <https://www.un.org/en/about-us/member-states>

³ Siehe Präambel der Charta der Vereinten Nationen, San Francisco, 26. Juni 1945: <https://www.un.org/en/about-us/un-charter/full-text>

⁴ Resolution der Generalversammlung der Vereinten Nationen vom 17. Dezember 2018, [A/RES/73/187](https://www.un.org/en/resolutions/73/187).

⁵ Resolution der Generalversammlung der Vereinten Nationen vom 27. Dezember 2019, [A/RES/74/247](https://www.un.org/en/resolutions/74/247).

⁶ Siehe S. 1 der Resolution.

Durchführung einer umfassenden Untersuchung der Computerkriminalität⁷. Drei EU-Mitgliedstaaten (Estland, Polen und Portugal) sind stellvertretende Vorsitzende des Ad-hoc-Ausschusses.⁸

3. Am 26. Mai 2021 bekräftigte die Generalversammlung der Vereinten Nationen in ihrer Resolution 75/282⁹ nochmals, dass der Ad-hoc-Ausschuss **die bestehenden internationalen Übereinkünfte** und die auf nationaler, regionaler und internationaler Ebene unternommenen Anstrengungen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken **in vollem Umfang berücksichtigen wird**.¹⁰ Sie beschloss, dass dieser Ad-hoc-Ausschuss mindestens sechs Verhandlungsrunden einberufen und nach Abschluss seiner Arbeit der Generalversammlung auf ihrer 48. Tagung, die im September 2023 beginnt und im September 2024 endet, einen Übereinkommensentwurf vorlegen soll.
4. Die erste Verhandlungsrunde fand vom 28. Februar bis zum 11. März 2022 statt. Bei dieser Gelegenheit wurden Ziele, Anwendungsbereich, Struktur und zentrale Elemente des Übereinkommens erörtert.¹¹ Gemäß dem Entwurf des Berichts über diese erste Verhandlungsrunde wurde vereinbart, dass die folgenden Elemente die Struktur des Übereinkommens bilden sollten:¹²

Präambel

1. Allgemeine Bestimmungen
 2. Kriminalisierung
 3. Verfahrensmaßnahmen und Strafverfolgung
 4. Internationale Zusammenarbeit
 5. Technische Hilfe, einschließlich Erfahrungsaustausch
 6. Präventivmaßnahmen
 7. Mechanismen für die Umsetzung
 8. Schlussbestimmungen.
5. Die Europäische Kommission nahm als Beobachter an den Sitzungen des Ad-hoc-Ausschusses teil. Am 24. und 25. März 2022 fand eine Zwischentagung statt, um Beiträge

⁷ Die offene zwischenstaatliche [Sachverständigengruppe](#) für die Durchführung einer umfassenden Untersuchung der Computerkriminalität wurde von der Wiener Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ) auf Ersuchen der [Resolution 65/230](#) der Generalversammlung der Vereinten Nationen eingerichtet und ist ein Nebenorgan der CCPCJ. Die Sachverständigengruppe ist unabhängig vom Ad-hoc-Ausschuss, der das Übereinkommen aushandelt und ein Nebenorgan der Generalversammlung mit einem anderen Mandat ist.

⁸ Dem Ad-hoc-Ausschuss gehören folgende Mitglieder an: Algerien (Vorsitz), Ägypten, Nigeria, China, Japan, Estland, Polen, Russische Föderation, Dominikanische Republik, Nicaragua, Brasilien, Australien, Portugal, Vereinigte Staaten (stellvertretende Vorsitzende), Indonesien (Berichtersteller).

⁹ Resolution der Generalversammlung der Vereinten Nationen vom 26. Mai 2021, [A/RES/75/282](#).

¹⁰ Siehe Ziffer 11 der Resolution.

¹¹ Vorlagen zu dieser ersten Runde finden Sie unter: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.

¹² <https://documents-dds-ny.un.org/doc/UNDOC/LTD/V22/012/09/PDF/V2201209.pdf?OpenElement>.

verschiedener Interessenträger zur Ausarbeitung des Übereinkommensentwurfs einzuholen.¹³ Die nächste Verhandlungsrunde soll am 30. Mai 2022 beginnen.¹⁴

6. Am 29. März 2022 veröffentlichte die Europäische Kommission eine Empfehlung für einen Beschluss des Rates über die Ermächtigung der Kommission, im Namen der Europäischen Union an den Verhandlungen der Vereinten Nationen über ein umfassendes internationales Übereinkommen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken teilzunehmen (im Folgenden „Empfehlung“).¹⁵ Der Empfehlung ist ein Anhang (im Folgenden „Anhang“) beigefügt, in dem die vorgeschlagenen Richtlinien des Rates für die Aushandlung des Übereinkommens dargelegt sind.
7. Die Kommission empfiehlt die Annahme eines Beschlusses des Rates auf der Grundlage des Verfahrens gemäß Artikel 218 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) für Übereinkommen zwischen der EU und Drittländern. Mit dieser Empfehlung ersucht die Kommission den Rat, zum Hauptverhandlungsführer im Namen der EU ernannt zu werden, um eine angemessene Beteiligung der EU an den Verhandlungen der Vereinten Nationen sicherzustellen, da diese voraussichtlich Aspekte betreffen werden, die sich auf die Rechtsvorschriften und die Zuständigkeit der EU, insbesondere im Bereich der Computerkriminalität, beziehen.¹⁶
8. Mit der vorliegenden Stellungnahme des EDSB wird das Konsultationsersuchen der Europäischen Kommission vom 29. März 2022 gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 beantwortet. Der EDSB begrüßt, dass in Erwägungsgrund 5 der Empfehlung auf diese Konsultation verwiesen wird.

2. Allgemeine Anmerkungen

9. Laut Begründung werden sich die Verhandlungen über das Übereinkommen voraussichtlich auf das gemeinsame EU-Regelwerk zur Bekämpfung der Computerkriminalität beziehen, wie die Richtlinie 2011/93/EU zur Bekämpfung der sexuellen Ausbeutung von Kindern im Internet sowie der Kinderpornografie, die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und die Richtlinie (EU) 2019/713 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln.¹⁷ Andere EU-Instrumente enthalten gemeinsame Vorschriften zur Bekämpfung von Straftaten, die durch die Nutzung von Informationssystemen ermöglicht werden, wie Terrorismus, Menschenhandel, illegaler Drogenhandel, illegaler Waffenhandel, Geldwäsche, Korruption und organisierte Kriminalität.¹⁸ Die Verhandlungen werden sich voraussichtlich auch auf Maßnahmen in den Bereichen Strafverfahren und

¹³ https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/intersessional-consultations/1st-intersessional-consultation.

¹⁴ https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.

¹⁵ Empfehlung für einen Beschluss des Rates zur Ermächtigung zur Aufnahme von Verhandlungen über ein umfassendes internationales Übereinkommen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken (COM(2022) 132 final).

¹⁶ Siehe Begründung, S. 2, und Artikel 1 der Empfehlung.

¹⁷ Siehe Begründung S. 4.

¹⁸ Ebenda.

Zusammenarbeit erstrecken. Die Union hat in diesem Bereich mehrere Rechtsakte erlassen.¹⁹

10. Der EDSB stellt fest, dass die Verhandlungen innerhalb der Vereinten Nationen bereits im Einklang mit der oben genannten Resolution 74/247 und der Resolution 75/282 der Generalversammlung der Vereinten Nationen geführt werden. Angesichts der Bedeutung dieser Verhandlungen für die EU-Politik im Bereich der Computerkriminalität und der Erhebung elektronischer Beweismittel in Strafsachen, insbesondere für den Schutz personenbezogener Daten und der Privatsphäre, **befürwortet der EDSB die Annahme eines Ratsbeschlusses, mit dem der Europäischen Kommission ein klares Mandat zur Teilnahme an diesen Verhandlungen im Namen der EU erteilt wird.**
11. Wie in der Empfehlung hervorgehoben²⁰, könnte ein neues internationales Übereinkommen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken die gemeinsamen Regeln der Union beeinträchtigen oder deren Tragweite verändern. Der EDSB betont, dass sichergestellt werden muss, dass das Übereinkommen mit dem EU-Recht, einschließlich der Einhaltung der Charta, insbesondere des Rechts auf Privatsphäre und des Rechts auf Schutz personenbezogener Daten, und mit Artikel 16 AEUV vereinbar ist.
12. Der EDSB ist sich der Tatsache bewusst, dass Strafverfolgungsbehörden elektronische Beweismittel schnell und effizient sichern und erlangen müssen. Er erinnert jedoch an die große Zahl von Ländern innerhalb der Vereinten Nationen mit höchst heterogenen Rechtsordnungen. Vor diesem Hintergrund ist der EDSB der Auffassung, dass ein erhebliches Risiko besteht, dass das Übereinkommen zu einer Schwächung des Schutzes der durch das EU-Recht garantierten Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihrer Rechte auf Datenschutz und Privatsphäre, führen könnte.
13. Der EDSB betont ferner, dass bereits ein ähnliches internationales Instrument in Kraft ist, nämlich das Budapester Übereinkommen und sein Zweites Zusatzprotokoll, das kürzlich ausgehandelt wurde und nun zur Unterzeichnung aufliegt.
14. Vor diesem Hintergrund möchte der EDSB unterstreichen, dass die Ermächtigung des Rates für die Kommission, im Namen der EU Verhandlungen zu führen, nicht als Vorgabe dafür ausgelegt werden sollte, dass die EU Vertragspartei des Übereinkommens wird, falls es angenommen wird, und insbesondere, dass **die EU nicht anstreben sollte, Vertragspartei eines solchen Übereinkommens zu werden, falls dadurch das durch das EU-Recht garantierte Datenschutzniveau für natürliche Personen untergraben werden könnte.**
15. Auch wenn sich der EDSB der Tatsache bewusst ist, dass es nicht möglich ist, die Terminologie und Definitionen des Unionsrechts in einer Vereinbarung mit einer sehr großen Zahl von Drittländern zu replizieren, muss der Schutz des Einzelnen eindeutig und wirksam geregelt sein, um eine vollumfängliche Übereinstimmung mit dem EU-Recht zu gewährleisten. Der Gerichtshof der Europäischen Union hat in den vergangenen Jahren die Grundsätze des Datenschutzes erneut bestätigt, darunter gerichtlicher Rechtsbehelf und

¹⁹ *Ebenda*, S. 5.

²⁰ *Siehe Erwägungsgrund 3.*

individuelle Rechte des Einzelnen. Diese Grundsätze sind umso wichtiger, wenn man die Sensibilität der für strafrechtliche Ermittlungen erforderlichen Daten bedenkt.

16. Die vorliegende Stellungnahme soll konstruktiven und objektiven Rat in der Frage bieten, wie das vom EU-Recht bereits gewährleistete Datenschutzniveau garantiert nicht untergraben wird. Sie enthält Empfehlungen zu folgenden Themen:
 - Verhältnis zwischen dem Übereinkommen und anderen Rechtsinstrumenten;
 - Festlegung des Anwendungsbereichs des Übereinkommens;
 - Garantien für internationale Übermittlungen personenbezogener Daten;
 - Schlussbestimmungen des Übereinkommens (Aussetzung, Überprüfung und Begründung von Beziehungen).
17. Der EDSB steht der Kommission, dem Rat und dem Europäischen Parlament in den weiteren Phasen dieses Prozesses weiterhin beratend zur Verfügung.

3. Verhältnis zu anderen Rechtsinstrumenten

18. In der Empfehlung wird daran erinnert²¹, dass es bereits ein verbindliches internationales Rechtsinstrument gibt, dessen Vertragsparteien verpflichtet sind, in ihrem innerstaatlichen Recht bestimmte Straftaten gegen oder über elektronische Netze zu definieren, die Mindestanforderungen an Ermittlungsbefugnisse im Rahmen strafrechtlicher Ermittlungen festzulegen und die internationale Zusammenarbeit zwischen den Vertragsparteien zu fördern, nämlich **das Übereinkommen des Europarats über Computerkriminalität (SEV Nr. 185) („Budapester Übereinkommen“)**, das den Mitgliedstaaten des Europarats und den Nichtmitgliedern, die sich an der Ausarbeitung des Übereinkommens beteiligt haben, zur Unterzeichnung bzw. Nichtmitgliedern, die nicht an seiner Ausarbeitung mitgewirkt haben, (auf Einladung) zum Beitritt aufliegt. Derzeit sind 66 Länder Vertragsparteien des Budapester Übereinkommens, darunter 26 Mitgliedstaaten der Europäischen Union²² und Drittländer, die Mitgliedstaaten des Europarats sind, wie Armenien, Aserbaidschan oder die Türkei, sowie Nichtmitglieder des Europarats wie Australien, Kanada, Ghana, Israel, Japan, Marokko, Paraguay, die Philippinen, Senegal, Sri Lanka, Tonga und die USA²³. Darüber hinaus nahm das Ministerkomitee des Europarats am 17. November 2021 ein Zweites Zusatzprotokoll zum Budapester Übereinkommen an, das seit dem 12. Mai 2022 zur Unterzeichnung aufliegt. Mit dem Protokoll sollen zusätzliche

²¹ Siehe Begründung S. 1.

²² Alle mit Ausnahme der Republik Irland, die das Übereinkommen zwar unterzeichnet, aber nicht ratifiziert hat, jedoch entschlossen ist, den Beitritt weiter zu verfolgen.

²³ Eine vollständige und aktualisierte Liste der Vertragsparteien des Übereinkommens über Computerkriminalität geht aus den Unterschriften und dem Ratifikationsstand des Übereinkommens über Computerkriminalität hervor, abrufbar unter: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>

Instrumente für die internationale Zusammenarbeit, auch für die Zusammenarbeit in Notsituationen, bereitgestellt werden.²⁴

19. Der EDSB **begrüßt Ziffer 6 des Anhangs**, in der der Union empfohlen wird, dafür zu sorgen, dass das künftige Übereinkommen der Vereinten Nationen „mit **bestehenden** internationalen Übereinkünften **vereinbar [ist] und diese ergänzt**, insbesondere mit dem Budapester Übereinkommen des Europarats von 2001 über Computerkriminalität und seinen Protokollen, dem Übereinkommen der Vereinten Nationen von 2000 gegen die grenzüberschreitende organisierte Kriminalität und seinen Protokollen, aber auch mit anderen einschlägigen internationalen und regionalen Übereinkünften“²⁵, und dass im künftigen Übereinkommen der Vereinten Nationen „**Auswirkungen auf ihre Anwendung** oder den weiteren Beitritt eines Landes zu diesen Übereinkommen ihnen hat und soweit unnötige Überschneidungen möglichst **vermieden werden**“²⁶.
20. Der EDSB **begrüßt** ferner **Ziffer 17 des Anhangs**, wonach die Union sicherstellen sollte, dass die „**Maßnahmen für die Zusammenarbeit [...] mit diesen Übereinkünften und mit internationalen Menschenrechtsnormen im Einklang stehen**“, sowie **Ziffer 23** des Anhangs, in der klargelegt wird, dass die Union darauf hinwirken sollte, dass mit dem Übereinkommen **die bestehenden internationalen und regionalen Übereinkünfte beibehalten werden**.
21. Der EDSB **empfiehlt** jedoch, in den Anhang aufzunehmen, dass die Union darauf hinwirken sollte, **dass künftige Abkommen mit Drittländern anstelle des Übereinkommens gelten, falls diese künftigen Abkommen höhere Standards in Bezug auf den Schutz der Grundrechte, insbesondere des Rechts auf Privatsphäre und Datenschutz, gewährleisten**.²⁷
22. Schließlich begrüßt und unterstützt der EDSB nachdrücklich die Aufnahme **einer „Abkopplungsklausel“** in Ziffer 23 des Anhangs, um sicherzustellen, dass das Sekundärrecht der EU zwischen den EU-Mitgliedstaaten weiterhin Anwendung findet, um die Rechtsordnung der EU zu erhalten.

4. Geltungsbereich

4.1. Unter das Übereinkommen fallende Straftaten

23. Der EDSB begrüßt das Ziel, Straftaten, die unter das Übereinkommen fallen würden, **klar und eng zu definieren**, nämlich als „Straftaten, die nur durch die Nutzung von Informationssystemen begangen werden können“ (**Ziffer 9** des Anhangs) und „Straftaten,

²⁴ Am 5. April 2022 erließ der Rat der Europäischen Union einen Beschluss zur Ermächtigung der Mitgliedstaaten, das Zweite Zusatzprotokoll im Interesse der EU zu unterzeichnen. Am selben Tag beschloss der Rat ferner, dem Parlament den Beschluss zur Ermächtigung der Mitgliedstaaten, das Protokoll zu ratifizieren, zur Billigung zu übermitteln.

²⁵ Hervorhebung hinzugefügt.

²⁶ Hervorhebung hinzugefügt.

²⁷ [Siehe beispielsweise den Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über die Änderung des Abkommens zwischen der Europäischen Union und Japan über die Rechtshilfe in Strafsachen \(12141/21\) und den Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen im Hinblick auf den Abschluss eines Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen \(9114/19\).](#)

die ohne die Nutzung von Informationssystemen begangen werden können, die aber unter bestimmten Umständen durch die Nutzung von Informationssystemen ermöglicht werden können, **jedoch nur in Fällen, in denen die Einbeziehung von Informationssystemen die Merkmale oder Auswirkungen der Straftaten wesentlich verändert**“ (Ziffer 10 des Anhangs) [Hervorhebung hinzugefügt]. Er begrüßt ferner, dass die Definitionen „mit denen anderer einschlägiger internationaler oder regionaler Übereinkünfte, insbesondere im Bereich der organisierten Kriminalität oder der Computerkriminalität, und mit internationalen Menschenrechtsnormen vereinbar“ sein sollten (Ziffer 11 des Anhangs).

24. In **Ziffer 16 des Anhangs** wird Folgendes empfohlen: „Im Übereinkommen *sind Maßnahmen für die Zusammenarbeit vorgesehen, die es den Behörden verschiedener Vertragsstaaten ermöglichen, zu Zwecken strafrechtlicher Ermittlungen oder Verfahren in Bezug auf die in dem Übereinkommen definierten Straftaten wirksam zusammenzuarbeiten oder zusammenzuarbeiten, um im Rahmen strafrechtlicher Ermittlungen oder Verfahren elektronische Beweise für eine Straftat zu sichern oder zu erheben.*“ [Hervorhebung hinzugefügt].²⁸ Der EDSB stellt fest, dass die empfohlenen Richtlinien die Zusammenarbeit bei der Sicherung oder Erlangung elektronischer Beweismittel für alle Straftaten im Rahmen strafrechtlicher Ermittlungen oder Strafverfahren umfassen. Seiner Ansicht nach böte angesichts der höchst heterogenen Rechtsordnungen möglicher künftiger Vertragsparteien des Übereinkommens die Beschränkung des Anwendungsbereichs der internationalen Zusammenarbeit im Rahmen des Übereinkommens auf die im Übereinkommen definierten Straftaten eine wichtige Garantie für die Notwendigkeit und Verhältnismäßigkeit der vorgeschlagenen Lösungen. Daher **ist der EDSB der Auffassung, dass auch der Anwendungsbereich der künftigen Bestimmungen über die Zusammenarbeit auf die im Übereinkommen definierten Straftaten beschränkt werden sollte.**

4.2. **Ausschluss eines direkten Zugriffs von Strafverfolgungsbehörden auf Daten und ihrer direkten Zusammenarbeit mit Diensteanbietern**

25. In diesem frühen Stadium der Verhandlungen ist der Anwendungsbereich des Übereinkommens noch unklar, insbesondere was die Modalitäten der Zusammenarbeit betrifft.
26. Wie der EDSB jedoch bereits im Zusammenhang mit den Verhandlungen über das Zweite Zusatzprotokoll zum Budapester Übereinkommen festgestellt hat²⁹, betrachtet er den **grenzüberschreitenden direkten Zugriff** von Strafverfolgungsbehörden von Drittländern auf Daten als besonders einschneidende Maßnahme, die sich folglich stärker auf die Grundrechte auf Privatsphäre und Datenschutz auswirkt. Daher **ist er der Ansicht, dass solche Bestimmungen nicht in das Übereinkommen aufgenommen werden sollten und eine entsprechende Richtlinie in den Anhang Eingang finden sollte.**
27. Angesichts der Zahl der Länder, die voraussichtlich Vertragsparteien des Übereinkommens werden, mit in Bezug auf die Achtung der Grundrechte und Grundfreiheiten einschließlich der Grundrechte auf Privatsphäre und Datenschutz sehr heterogenen Rechtsordnungen empfiehlt der EDSB ferner, jeglichen Versuch abzuwehren, in das Übereinkommen Bestimmungen über die direkte Zusammenarbeit von Behörden von Drittländern mit

²⁸ Hervorhebung hinzugefügt.

²⁹ [Stellungnahme 3/2019 des EDSB zur Teilnahme an den Verhandlungen über ein zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität, Ziffern 18 und 19.](#)

Diensteanbietern aufzunehmen, die den Rechtsvorschriften der EU unterliegen. In diesem Zusammenhang **sollte klargestellt werden, dass Ziffer 15 des Anhangs sich nur auf die Zusammenarbeit zwischen Strafverfolgungsbehörden und Diensteanbietern im selben Land bezieht** und nicht die grenzüberschreitende Zusammenarbeit zwischen Strafverfolgungsbehörden und Diensteanbietern in einem anderen Land betrifft. Dieser Klärungsbedarf ist umso wichtiger, als in Ziffer 19 des Anhangs festgelegt ist, dass mit dem Übereinkommen sichergestellt wird, dass die EU-Mitgliedstaaten die Anforderungen für die internationale Übermittlung personenbezogener Daten im Sinne der DSGVO erfüllen können, was impliziert, dass eine direkte Zusammenarbeit zwischen Diensteanbietern in der EU und Behörden von Drittländern, die Vertragsparteien des Übereinkommens sind, zum gegenwärtigen Zeitpunkt tatsächlich nicht ausgeschlossen ist.

5. Notwendigkeit detaillierter Garantien in Bezug auf die internationale Übermittlung von Daten und die Achtung von Grundrechten

28. Der EDSB erinnert daran, dass Artikel 216 Absatz 2 AEUV besagt: „Die von der Union geschlossenen internationalen Übereinkünfte *binden die Organe der Union und die Mitgliedstaaten.*“ Darüber hinaus bilden internationale Übereinkünfte gemäß der ständigen Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) ab ihrem Inkrafttreten *„einen integrierenden Bestandteil der Gemeinschaftsrechtsordnung“*³⁰ und haben Vorrang vor den Bestimmungen des abgeleiteten Unionsrechts³¹.
29. Da das Übereinkommen eine bindende internationale Übereinkunft wäre, dem die Union beitreten würde³², merkt der EDSB an, dass nach der Rechtsprechung des EuGH *„die Verpflichtungen aufgrund einer internationalen Übereinkunft nicht die Verfassungsgrundsätze des EG-Vertrags beeinträchtigen können, zu denen auch der Grundsatz zählt, dass alle Handlungen der Gemeinschaft die Menschenrechte achten müssen, da die Achtung dieser Rechte eine Voraussetzung für ihre Rechtmäßigkeit ist“*³³. **Es ist daher unbedingt sicherzustellen, dass die sich aus dem Übereinkommen ergebenden Verpflichtungen das Grundrecht auf Datenschutz in vollem Umfang achten.**
30. Der EDSB begrüßt daher **Ziffer 8 des Anhangs**, wonach die Union sicherstellen sollte, dass die Bestimmungen des Übereinkommens den größtmöglichen Schutz der Menschenrechte erreichen und dass die EU-Mitgliedstaaten in der Lage sein sollten, das EU-Recht, einschließlich der Grundrechte, Grundfreiheiten und allgemeinen Grundsätze des EU-Rechts, wie sie in den Verträgen der Europäischen Union und der Charta verankert sind, einzuhalten. Der EDSB begrüßt in diesem Zusammenhang auch die eindeutige Bezugnahme auf den **Grundsatz der Verhältnismäßigkeit in Ziffer 13 des Anhangs**.
31. Darüber hinaus nimmt der EDSB zur Kenntnis und **unterstützt Ziffer 18 des Anhangs**, mit der erreicht werden soll, dass die Maßnahmen für die Zusammenarbeit den im Recht

³⁰ Urteil des Gerichtshofs vom 30. April 1974, C-181/73, R.&V. Haegemann / Belgischer Staat, ECLI:EU:C:1974:41, Rn. 5.

³¹ Urteil des Gerichtshofs vom 3. Juni 2008, C-308/06, Intertanko u. a., ECLI:EU:C:2008:312, Rn. 42.

³² Siehe Ziffer 25 des Anhangs.

³³ EuGH, Urteil vom 30. April 1974, verbundene Rechtssachen C-402/05 P und C-415/05 P, Kadi gegen Rat der Europäischen Union, ECLI:EU:C:2008:461, Rn. 285.

der ersuchten Partei vorgesehenen Bedingungen unterliegen und weitreichende Ablehnungsgründe wie die Gewährleistung des Schutzes der Grundrechte, einschließlich des Rechts auf den Schutz personenbezogener Daten, auch im Zusammenhang mit der Übermittlung personenbezogener Daten, und gegebenenfalls das Vorliegen der beiderseitigen Strafbarkeit umfassen.

32. Gemäß der Rechtsprechung des EuGH kann nur die Bekämpfung der schweren Kriminalität einen Zugang öffentlicher Stellen zu von Diensteanbietern gespeicherten personenbezogenen Daten rechtfertigen, „aus deren Gesamtheit genaue Schlüsse auf das Privatleben der von diesen Daten betroffenen Personen gezogen werden können“³⁴. Können derartige Schlüsse nicht gezogen werden und könnte der Zugang daher nicht „als ein schwerer Eingriff in die Grundrechte der Personen, deren Daten betroffen sind, definiert werden“, stellte das Gericht weiterhin fest, „kann der Eingriff, den ein Zugriff zu solchen Daten mit sich bringen würde, somit durch den (...) Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von „Straftaten“ im Allgemeinen gerechtfertigt sein, ohne dass es erforderlich wäre, dass diese Straftaten als „schwer“ einzustufen sind“³⁵.
33. Damit Artikel 52 Absatz 1 der Charta Genüge getan wird, sollten nach Auffassung des EDSB die Kategorien von Daten, für die die Erhebung und Übermittlung personenbezogener Daten angeordnet werden könnte, in einem angemessenen Verhältnis zu den betreffenden Arten von Straftaten stehen müssen. **Insbesondere sollte sichergestellt werden, dass nur schwere Straftaten den Datenaustausch rechtfertigen können, der einen schwerwiegenden Eingriff in die Grundrechte auf Datenschutz und Privatsphäre darstellt.**
34. Darüber hinaus begrüßt der EDSB **Ziffer 15 des Anhangs**, in der der Union empfohlen wird, darauf hinzuwirken, dass die Verfahrensmaßnahmen zur Sicherung oder Beschaffung elektronischer Beweismittel eine klare und enge Definition der Art der erfassten Informationen enthalten, und betont er, wie wichtig es ist, klare und einfache Definitionen der Datenkategorien im VN-Übereinkommen festzulegen, um für alle Beteiligten Rechtssicherheit zu gewährleisten. **Der EDSB empfiehlt, die Datenkategorien sauber voneinander abzugrenzen; eine solche Abgrenzung würde dabei helfen, Rechtssicherheit zu gewährleisten.**
35. Der EDSB begrüßt und **unterstreicht die Bedeutung von Ziffer 19 des Anhangs**. Hier heißt es zunächst, dass **im Übereinkommen strenge Bedingungen und strenge Garantien vorgesehen sein sollten**, um sicherzustellen, dass die EU-Mitgliedstaaten die Grundrechte, die Grundfreiheiten und die allgemeinen Grundsätze des EU-Rechts gemäß den Verträgen der Europäischen Union und der Charta der Grundrechte achten und schützen können, wozu insbesondere der Grundsatz der Verhältnismäßigkeit, das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, **das Recht auf Privatsphäre, das Recht auf Schutz personenbezogener Daten und elektronischer Kommunikationsdaten** gehören, wenn solche Daten verarbeitet werden, **einschließlich der Übermittlung von Daten an Behörden in Ländern außerhalb der Europäischen Union**. Zweitens sollte mit dem Übereinkommen sichergestellt werden, dass die EU-Mitgliedstaaten **die Anforderungen für die internationale Übermittlung personenbezogener Daten im**

³⁴ Urteil des Gerichtshofs vom 2. Oktober 2018, *Ministerio fiscal*, C-207/16, ECLI:EU:C:2018:788, Rn. 54, siehe auch Rn. 56.

³⁵ Ebd., Rn. 62. [Hervorhebung hinzugefügt.]

Sinne der Richtlinie (EU) 2016/680³⁶ („Richtlinie zum Datenschutz bei der Strafverfolgung“) und der Richtlinie 2002/58/EG³⁷ erfüllen können.

36. Im spezifischen Kontext der Übermittlung personenbezogener Daten zu Strafverfolgungszwecken durch Strafverfolgungsbehörden der EU erinnert der EDSB daran, dass nach Artikel 37 und Erwägungsgrund 71 der Richtlinie zum Datenschutz bei der Strafverfolgung Datenübermittlungen, die nicht auf der Grundlage eines Angemessenheitsbeschlusses erfolgen, nur dann zulässig sein sollten, wenn in einem rechtsverbindlichen Instrument geeignete Garantien festgelegt sind, die den Schutz personenbezogener Daten gewährleisten, oder wenn der Verantwortliche alle Umstände beurteilt hat, die bei der Datenübermittlung eine Rolle spielen, und auf Grundlage dieser Beurteilung zu der Auffassung gelangt ist, dass geeignete Garantien bestehen. Solche rechtsverbindlichen Instrumente könnten beispielsweise rechtsverbindliche Vereinbarungen sein, die von den betroffenen Personen durchgesetzt werden können, und die sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen einschließlich ihres Rechts auf wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe beachtet werden. Der Verantwortliche sollte außerdem berücksichtigen können, dass die Übermittlung personenbezogener Daten Geheimhaltungspflichten und dem Grundsatz der Spezialität unterliegt, damit gewährleistet wird, dass die Daten nicht zu anderen Zwecken als zu den Zwecken, zu denen sie übermittelt wurden, verarbeitet werden. Darüber hinaus sollte der Verantwortliche berücksichtigen, dass die personenbezogenen Daten nicht verwendet werden, um die Todesstrafe oder eine Form der grausamen und unmenschlichen Behandlung zu beantragen, zu verhängen oder zu vollstrecken. Der Verantwortliche sollte zusätzliche Garantien verlangen können.
37. In diesem Zusammenhang **äußert der EDSB starke Zweifel daran, ob das künftige Übereinkommen eine eigenständige Grundlage für die Übermittlung personenbezogener Daten im Einklang mit dem EU-Recht bieten könnte**, und empfiehlt daher sicherzustellen, dass die Mitgliedstaaten zusätzliche Garantien geltend machen und vorschreiben können, damit Übermittlungen im Rahmen dieses Übereinkommens nur mit dem EU-Recht, einschließlich des EU-Sekundärrechts, im Einklang stehend erfolgen.
38. Schließlich möchte der EDSB noch betonen, dass die jeweiligen Behörden in Drittländern, an die Daten übermittelt würden und die diese Daten verarbeiten würden, genau festgelegt werden sollten, damit sichergestellt ist, dass sie auch für die Zwecke der Übermittlung zuständig sind. In diesem Sinne **empfiehlt der EDSB daher, dass dem geplanten Übereinkommen eine erschöpfende Liste der zuständigen Behörden in den empfangenden Ländern, an die Daten übermittelt würden, sowie eine Kurzbeschreibung ihrer Zuständigkeiten beiliegt. Dies sollte auch in einer der Richtlinien des Anhangs zum Ausdruck gebracht werden.**

³⁶ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

³⁷ Hervorhebung hinzugefügt.

6. Aussetzung, Überprüfung des Übereinkommens und Begründung von Beziehungen gemäß dem Übereinkommen

39. Der EDSB begrüßt die Aufnahme einer spezifischen Bestimmung, die **eine Aussetzung des Übereinkommens ermöglicht**, soweit dies möglich und angemessen ist, und zwar nach dem Vorbild anderer einschlägiger internationaler oder regionaler Übereinkommen, insbesondere im Bereich organisierte Kriminalität oder der Cyberkriminalität.³⁸ Der EDSB **empfiehlt**, in diesem Zusammenhang **weiter zu präzisieren**, dass die Union darauf hinwirken sollte, dass **ein Vertragsstaat zum Zeitpunkt der Unterzeichnung, der Ratifizierung oder des Beitrittserklären kann, dass er einem Ersuchen nach Übermittlung personenbezogener Daten an eine andere Partei nicht nachkommen wird, wenn Hinweise darauf vorliegen³⁹, dass in dem ersuchenden Staat ein wesentliches Datenschutzniveau nicht länger gewährleistet ist.**
40. Ferner **empfiehlt** der EDSB, dass in den Verhandlungsrichtlinien die Einführung einer Klausel gefordert wird, in der die **obligatorische Überprüfung** des Funktionierens des Übereinkommens in der Praxis **in regelmäßigen Abständen** geregelt wird. Im Sinne einer aussagekräftigen Überprüfung sollte diese spätestens fünf Jahre nach Inkrafttreten und dann in regelmäßigen Abständen vorgesehen werden, wobei auch die Häufigkeit dieser weiteren Überprüfungen festgelegt wird. Der Inhalt der Überprüfung sollte spezifiziert werden. Die Überprüfung sollte nicht nur auf die Umsetzung des Übereinkommens, sondern auch auf die Beurteilung seiner Notwendigkeit und seiner Verhältnismäßigkeit abheben. Zu den Überprüfungsteams sollten Datenschutzexperten gehören, darunter Vertreter nationaler Datenschutzbehörden.
41. Angesichts der großen Heterogenität der Länder, die möglicherweise Vertragsparteien des Übereinkommens werden, **empfiehlt der EDSB, in das Mandat aufzunehmen, dass die Union darauf hinwirken sollte, dass das Übereinkommen zwischen zwei Vertragsstaaten keine Wirkung entfaltet, wenn einer von ihnen notifiziert, dass die Ratifikation, die Annahme, die Genehmigung oder der Beitritt eines anderen Vertragsstaats keine Beziehungen zwischen diesen beiden Vertragsstaaten nach diesem Übereinkommen begründet.**⁴⁰

7. Schlussfolgerungen

42. Der EDSB **unterstützt** die Annahme eines Beschlusses des Rates, mit dem der Europäischen Kommission ein klares Mandat erteilt wird, im Namen der EU an den laufenden Verhandlungen der Vereinten Nationen über dieses Übereinkommen teilzunehmen. Er betont jedoch, dass eine Ermächtigung zur Teilnahme an den Verhandlungen nicht voraussetzt, dass die EU Vertragspartei des Übereinkommens ist, falls es angenommen wird, und dass die EU insbesondere nicht versuchen sollte, Vertragspartei

³⁸ Siehe Ziffer 24 des Anhangs.

³⁹ Wie die Aussetzung des Mandats des Menschenrechtsausschusses der Vereinten Nationen.

⁴⁰ Siehe beispielsweise das [Haager Übereinkommen über die Anerkennung und Vollstreckung ausländischer Entscheidungen in Zivil- und Handelssachen](#), Den Haag, 2. Juli 2019, Artikel 29.

eines solchen Übereinkommens zu sein, wenn das durch das EU-Recht garantierte Datenschutzniveau für natürliche Personen untergraben wird.

43. Der EDSB begrüßt und unterstreicht die Bedeutung der Ziffern 6, 17 und 23 des Anhangs, mit denen die bestehenden internationalen und regionalen Instrumente beibehalten werden sollen, sowie der in den Ziffern 8, 9, 10, 11, 13, 18, 19 und 24 des Anhangs enthaltenen Garantien.
44. Vor diesem Hintergrund spricht der EDSB folgende Empfehlungen aus:

Zum Verhältnis zwischen dem Übereinkommen und anderen Rechtsinstrumenten

-) Aufnahme in das Mandat, dass die Union anstreben sollte, dass künftige Abkommen mit Drittländern anstelle des Übereinkommens gelten sollten, falls diese künftigen Abkommen höhere Standards in Bezug auf den Schutz der Grundrechte, insbesondere des Rechts auf Privatsphäre und Datenschutz, gewährleisten.

Zum Anwendungsbereich des Übereinkommens

-) Beschränkung der Bestimmungen über die Zusammenarbeit auf die im Übereinkommen festgelegten Straftaten.
-) Klarstellung im Mandat, dass die Union Bestimmungen über den grenzüberschreitenden direkten Zugang zu Daten und die grenzüberschreitende direkte Zusammenarbeit mit Diensteanbietern ablehnen sollte.
-) Klarstellung, dass die Richtlinien unter Ziffer 15 des Anhangs nicht die grenzüberschreitende Zusammenarbeit betreffen.

Zur Notwendigkeit angemessener Garantien und zur Achtung der Grundrechte

-) Klarstellung im Mandat, dass die Union für eine klare Abgrenzung zwischen den Datenkategorien sorgen sollte.
-) Aufnahme einer Richtlinie in das Mandat, mit der erreicht werden soll, dass dem Übereinkommen eine erschöpfende Liste der zuständigen Behörden in den empfangenden Ländern, an die Daten übermittelt würden, sowie eine Kurzbeschreibung ihrer Zuständigkeiten beigefügt wird.

Zu den Schlussklauseln des Übereinkommens:

-) Spezifizierung im Mandat, dass die Union darauf hinwirken sollte, dass ein Vertragsstaat zum Zeitpunkt der Unterzeichnung, der Ratifizierung oder des Beitritts erklären kann, dass er ein Ersuchen um Übermittlung personenbezogener Daten an eine andere Partei nicht bearbeiten wird, sollte es Hinweise darauf geben, dass im ersuchenden Staat ein wesentliches Datenschutzniveau nicht mehr gewährleistet ist.
-) Aufnahme in das Mandat, dass die Union darauf hinwirken sollte, eine Klausel zur obligatorischen Überprüfung der Anwendung des Übereinkommens in der Praxis in regelmäßigen Abständen aufzunehmen. Diese Überprüfung sollte spätestens ein Jahr nach seinem Inkrafttreten und dann in regelmäßigen Abständen vorgesehen werden, wobei auch

die Häufigkeit dieser zusätzlichen Überprüfungen festgelegt wird. Der Inhalt der Überprüfung sollte spezifiziert werden. Die Überprüfung sollte sich nicht nur auf die Umsetzung des Übereinkommens konzentrieren, sondern auch seine Notwendigkeit und Verhältnismäßigkeit beurteilen. Den Überprüfungssteams sollten Datenschutzexperten angehören, und auch EU-Datenschutzbehörden sollten involviert sein.

J) Aufnahme in das Mandat, dass die Union sicherstellen sollte, dass das Übereinkommen zwischen zwei Vertragsstaaten keine Wirkung entfaltet, wenn einer von ihnen notifiziert, dass die Ratifikation, die Annahme, die Genehmigung oder der Beitritt eines anderen Vertragsstaats keine Beziehungen zwischen diesen beiden Vertragsstaaten nach diesem Übereinkommen begründet.

45. Schließlich steht der EDSB der Kommission, dem Rat und dem Parlament für weitere Ratschläge im Verlauf des weiteren Verfahrens zur Verfügung. Die Anmerkungen in dieser Stellungnahme gelten unbeschadet etwaiger zusätzlicher Anmerkungen, die der EDSB nach dem Aufwerfen weiterer Fragen später vorlegt. Diese würden behandelt, sobald weitere Informationen verfügbar sind. Er erwartet, dass er zum Wortlaut des Entwurfs des Übereinkommens vor dessen Fertigstellung konsultiert wird.

Brüssel, den 18. Mai 2022

(elektronisch unterzeichnet)

Wojciech Rafał Wiewiórowski