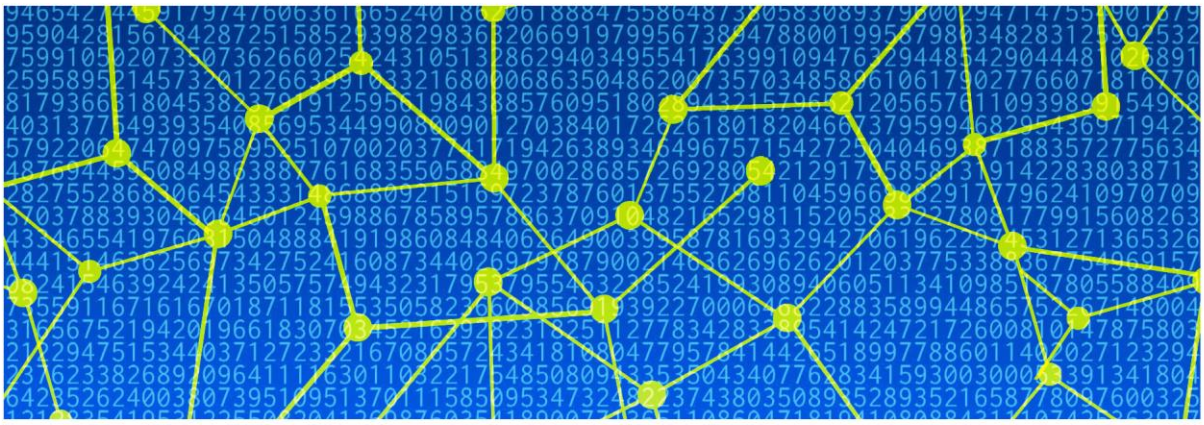

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 3/2019

Stellungnahme des EDSB zu der Teilnahme an den Verhandlungen mit Blick auf ein Zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität

EDPS

2. April 2019

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 52 Absatz 2 der Verordnung 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"; er ist gemäß Artikel 52 Absatz 3 „für die Beratung der Organe und Einrichtungen der Union und der betroffenen Personen in allen Fragen der Verarbeitung personenbezogener Daten" zuständig. 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."

Der Europäische Datenschutzbeauftragte wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und speziell mit einem konstruktiven und proaktiven Vorgehen beauftragt. In seiner im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.

In dieser Stellungnahme geht es um den Auftrag des EDSB, die EU-Organe bezüglich der kohärenten und konsequenten Anwendung der EU-Datenschutzgrundsätze bei der Aushandlung von Abkommen im Bereich Strafverfolgung im Einklang mit Maßnahme 5 der Strategie des EDSB: „Durchgängige Einbeziehung des Datenschutzes in internationale Politikbereiche" zu beraten. Diese Stellungnahme basiert auf der allgemeinen Verpflichtung, dass internationale Vereinbarungen mit den Bestimmungen des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) übereinstimmen und die Grundrechte, die ein zentraler Grundsatz des Unionsrechts sind, wahren müssen. Insbesondere muss die Einhaltung von Artikeln 7, 8 und 47 der Charta der Grundrechte der Europäischen Union sowie von Artikel 16 AEUV sichergestellt sein.

Zusammenfassung

Am 5. Februar 2019 veröffentlichte die Europäische Kommission eine Empfehlung über einen Beschluss des Rates zur Ermächtigung der Kommission, im Namen der Union an den Verhandlungen mit Blick auf ein Zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität teilzunehmen. Im Anhang der Empfehlung werden die empfohlenen Richtlinien des Rates zur Verhandlung des Protokolls niedergelegt. Ziele dieses Protokolls sind die Verbesserung der traditionellen Kooperationskanäle und die Aufnahme von Bestimmungen über eine unmittelbare, grenzüberschreitende Zusammenarbeit zwischen Strafverfolgungsbehörden und Diensteanbietern sowie von Bestimmungen über grenzüberschreitenden direkten Zugriff auf Daten durch Strafverfolgungsbehörden.

Der EDSB begrüßt die Empfehlung über die Ermächtigung der Europäischen Kommission, im Namen der Europäischen Union ein Zweites Zusatzprotokoll zu dem Übereinkommen über Computerkriminalität auszuhandeln, und unterstützt sie aktiv. Der EDSB weist bereits seit langem darauf hin, dass die EU nachhaltige Abkommen über den Austausch personenbezogener Daten mit Drittländern zum Zwecke der Strafverfolgung braucht, die vollumfänglich mit den EU-Verträgen und der Charta der Grundrechte übereinstimmen. Sogar bei Ermittlungen im Inland sind Strafverfolgungsbehörden immer häufiger mit „grenzüberschreitenden Situationen“ konfrontiert, weil Informationen elektronisch in Drittländern gespeichert werden. Bestehende Kooperationsmodelle wie Rechtshilfeabkommen werden durch das wachsende Volumen von Ersuchen und die Volatilität digitaler Informationen stark beansprucht. Der EDSB versteht, dass die Behörden bei der Beschaffung von Daten für ihre Ermittlungen unter Zeitdruck stehen, und unterstützt Bemühungen zur Konzipierung neuer Kooperationsmodelle, und zwar auch im Rahmen der Kooperation mit Drittländern.

Mit dieser Stellungnahme sollen die EU-Organe konstruktiv und objektiv beraten werden, da der Rat seine Richtlinien vor der Aufnahme dieser diffizilen Aufgabe mit weitreichenden Auswirkungen erfüllen muss. Der EDSB betont, dass Grundrechte, einschließlich des Datenschutzes und des Schutzes personenbezogener Daten, voll und ganz respektiert werden müssen. Auch wenn sich der EDSB bewusst ist, dass es nicht möglich ist, die Terminologie und Definitionen des Unionsrechts in einer Vereinbarung mit einem Drittland vollständig zu replizieren, muss der Schutz des Einzelnen eindeutig und wirksam geregelt sein, um eine vollumfängliche Übereinstimmung mit dem Primärrecht der EU zu gewährleisten. Der Gerichtshof der Europäischen Union hat in den vergangenen Jahren die Grundsätze des Datenschutzes bestätigt, hierin eingeschlossen Gerechtigkeit, Richtigkeit und Relevanz von Informationen, unabhängige Kontrolle und individuelle Rechte des Einzelnen. Die Relevanz dieser Grundsätze ist für öffentliche Einrichtungen und für private Unternehmen dieselbe, und angesichts der Sensitivität der für Ermittlungsverfahren erforderlichen Daten ist ihre Bedeutung umso größer.

Viele der bereits getroffenen Vorkehrungen werden begrüßt, sollten aber noch verstärkt werden. Der EDSB hat drei wesentliche Verbesserungen ermittelt, deren Umsetzung er für die Verhandlungsrichtlinien empfiehlt, um eine Übereinstimmung mit der Charta und Artikel 16 AEUV zu gewährleisten:

- Gewährleistung, dass das geplante Protokoll obligatorisch ist,
- einschließlich detaillierter Vorkehrungen wie etwa des Grundsatzes der Zweckbindung aufgrund der verschiedenen potenziellen Unterzeichnerstaaten, von denen nicht alle das

Übereinkommen Nr. 108 oder eine dem EU-US-Rahmenabkommen entsprechende Vereinbarung unterzeichnet haben,

- Ablehnung jeglicher Bestimmungen über den direkten Zugriff auf Daten.

Darüber hinaus bietet die Stellungnahme weitere Empfehlungen zur Verbesserung und Verdeutlichung der Verhandlungsrichtlinien. Für weitere Beratung während der Verhandlungen und vor dem Abschluss des Protokolls steht der EDSB den Organen zur Verfügung.

INHALTSVERZEICHNIS

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf die Artikel 7 und 8,

gestützt auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)[1],

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, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG[2], insbesondere von Artikel 42 Absatz 1, Artikel 57 Absatz 1 Buchstabe g und Artikel 58 Absatz 3 Buchstabe c,

gestützt auf die 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[3] —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG UND HINTERGRUND

1. Am 17. April 2018 legte die Kommission ein Paket mit zwei Legislativvorschlägen vor: einem Vorschlag für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen [4] (im Weiteren „der e-Beweismittel-Vorschlag“) und einem Vorschlag für eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren[5]. Während die Arbeit im Europäischen Parlament noch nicht abgeschlossen ist, hat der Rat der Europäischen Union (der Rat) bereits einen allgemeinen Standpunkt in Bezug auf diese beiden Vorschläge festgelegt[6].

2. Am 5. Februar 2019 nahm die Kommission zwei Empfehlungen für Beschlüsse des Rates an: eine Empfehlung über die Ermächtigung zur Aufnahme von Verhandlungen über ein internationales Abkommen zwischen der Europäischen Union (EU) und den Vereinigten Staaten von Amerika (USA) über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen[7] und eine Empfehlung zur Genehmigung der Teilnahme der Kommission an Verhandlungen über ein Zweites Zusatzprotokoll zum Übereinkommen des Europarats über Computerkriminalität im Namen der EU (SEV Nr. 185) (im Weiteren „die Empfehlung“)[8]. Die erste Empfehlung ist Gegenstand einer separaten EDSB-Stellungnahme.[9] Nach Ansicht des Europäischen Datenschutzbeauftragten (EDSB) besteht jedoch eine enge Verbindung zwischen beiden Verhandlungen mit den USA und dem Europarat.

3. Die Empfehlung wurde auf der Grundlage des Verfahrens gemäß Artikel 218 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) für Übereinkommen zwischen der EU und Drittländern angenommen. Mit dieser Empfehlung ersucht die Kommission um die Genehmigung des Rates, zur Verhandlungsführerin im Namen der EU bei Verhandlungen über ein Zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität (SEV Nr. 185)[10] entsprechend den der Empfehlung beiliegenden Verhandlungsrichtlinien ernannt zu werden. Der Anhang der Empfehlung (im Weiteren „der Anhang") ist von ausschlaggebender Bedeutung, da dort die Richtlinien des Rates an die Kommission für die Verhandlung des Protokolls im Namen der EU festgelegt werden. Nach Abschluss der Verhandlungen muss das Europäische Parlament zum Abschließen des Abkommens dem Wortlaut des ausgehandelten Abkommens zustimmen, wonach der Rat einen Beschluss über den Abschluss des Abkommens erlassen muss. Der EDSB geht davon aus, dass er gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 zu gegebener Zeit bezüglich des Wortlauts des Entwurfs des Abkommens konsultiert wird.

4. Der EDSB begrüßt es, dass er nach der Annahme der Empfehlung durch die Europäische Kommission gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 konsultiert worden ist. Weiterhin begrüßt der EDSB den Hinweis auf diese Stellungnahme in Erwägungsgrund 8 der Empfehlung. Er möchte betonen, dass diese Stellungnahme unbeschadet etwaiger zusätzlicher Anmerkungen erfolgt, die der EDSB auf der Grundlage weiterer verfügbarer Informationen, der Bestimmungen des Protokollentwurfs während der Verhandlungen und der legislativen Entwicklungen in Drittländern machen könnte.

2. ZIELE DES ZWEITEN ZUSATZPROTOKOLLS

5. Das Übereinkommen des Europarats über die verstärkte internationale Zusammenarbeit bei Computerkriminalität und elektronischen Beweismitteln (im Weiteren das „**Übereinkommen über Computerkriminalität**") steht Mitgliedstaaten des Europarats und Nicht-Mitgliedstaaten (auf Einladung) zum Beitritt offen. Derzeit sind 62 Länder Vertragsparteien des Übereinkommens, darunter 26 Mitgliedstaaten der Europäischen Union (alle außer Irland und Schweden, die es unterzeichnet haben) und andere Drittländermitgliedstaaten des Europarats wie Armenien, Aserbaidschan, die Türkei sowie Nicht-Mitgliedstaaten des Europarats wie Australien, Kanada, Ghana, Israel, Japan, Marokko, Paraguay, die Philippinen, Senegal, Sri Lanka, Tonga und die USA[11]. Das Übereinkommen über Computerkriminalität liegt für die EU nicht zur Unterschrift auf.

6. Das Übereinkommen über Computerkriminalität ist eine verbindliche internationale Übereinkunft, mit der sich die Vertragsstaaten verpflichten, spezifische, gegen elektronische Netzwerke gerichtete oder durch elektronische Netzwerke begangene Straftaten in ihr nationales Recht aufzunehmen und spezifische Vollmachten und Verfahren festzulegen, mit Hilfe derer ihre nationalen Behörden ihre Ermittlungsverfahren, einschließlich des Sammelns von Beweisen einer Straftat in elektronischer Form, durchführen können. Dabei bestehen Mindestanforderungen an Ermittlungsvollmachten, die bei Ermittlungen zur Verfügung stehen. Das Übereinkommen über Computerkriminalität fördert auch die internationale Zusammenarbeit zwischen den Vertragsstaaten.

7. In dem 2014 angenommenen Leitfaden # 3 des Ausschusses für das Übereinkommen über Computerkriminalität (im Weiteren der „T-CY")[12] heißt es, dass *„[s]ich insgesamt sowohl*

Praktiken, Verfahren als auch Bedingungen und Vorkehrungen zwischen verschiedenen Vertragsparteien stark unterscheiden. Nach wie vor bestehen Bedenken über Verfahrensrechte von Verdächtigen, den Schutz der Privatsphäre und den Schutz personenbezogener Daten, die Rechtsgrundlage für den Zugriff auf Daten, die in ausländischen Rechtsordnungen oder „in der Cloud" gespeichert sind, sowie über nationale Souveränität, und diese Bedenken müssen angegangen werden".

8. Zur Klärung der Mängel und Mehrdeutigkeiten des Rahmens des Übereinkommens beschlossen die Vertragsparteien des Übereinkommens über Computerkriminalität im Juni 2017, die Arbeit an einem **Zweiten Zusatzprotokoll** des Übereinkommens aufzunehmen, um diesen Prozess bis Ende 2019 abschließen zu können[13]. Das Protokoll kann Folgendes umfassen:
    - **Bestimmungen für eine effektivere Rechtshilfe:**
        - eine vereinfachte Regelung für im Rahmen der Rechtshilfe gestellte Ersuchen um Bestandsdaten;
        - internationale Herausgabeanordnungen;
        - unmittelbare Zusammenarbeit zwischen den Justizbehörden bei Rechtshilfeersuchen;
        - gemeinsame Ermittlungen und gemeinsame Ermittlungsgruppen;
        - Ersuchen in englischer Sprache;
        - audiovisuelle Befragung von Zeugen, Opfern und Sachverständigen;
        - Verfahren zur Rechtshilfe in Notfällen.
    - **Bestimmungen,** die im Hinblick auf Ersuchen um **Bestandsdaten, Ersuchen um Datensicherungen und Ersuchen in Notfällen eine unmittelbare Zusammenarbeit mit Diensteanbietern**[14] in anderen Ländern **erlauben.**
    - Einen klarer definierten Rahmen und stärkere Garantien für bestehende Praktiken des **grenzüberschreitenden Zugangs zu Daten**[15].
    - **Garantien einschließlich Datenschutzanforderungen**[16].

    Die Europäische Kommission nimmt als Beobachterorganisation an Plenarsitzungen des T-CY teil.

3. HAUPTEMPFEHLUNGEN

3.1. Mandat auf EU-Niveau und Verbindlichkeit des Protokolls

9. Der Kommission zufolge ist das Protokoll „*von unmittelbarer Relevanz für die gegenwärtige und künftige Entwicklung von gemeinsamen EU-Regeln*". Nach Abschluss der Verhandlungen kann das Protokoll „*schlussendlich Maßnahmen in Bereichen umfassen, in denen die EU bereits gesetzliche Regelungen getroffen hat – wie bei der justiziellen Zusammenarbeit und dem Schutz der Grundrechte*". Die Verhandlungen über das Protokoll „*können sich auch auf künftige gesetzliche Regelungen der EU beziehen – insbesondere auf den grenzüberschreitenden Zugang zu elektronischen Beweismitteln*"[17] (der oben genannte e-Beweismittel-Vorschlag). Es ist wichtig, dass die EU an den Verhandlungen teilnimmt, um zu der Gestaltung dieses Protokolls beizutragen. Angesichts der Bedeutsamkeit der Themen, die auf internationaler Ebene für Unionspolitik im Bereich des Sammelns von elektronischen Beweismitteln in Strafsachen, insbesondere für den Schutz personenbezogener Daten und den Schutz der Privatsphäre diskutiert werden, und in Anbetracht des bereits fortgeschrittenen Stadiums der Gespräche nach zweijähriger

Verhandlungsdauer **befürwortet der EDSB uneingeschränkt die Annahme eines Ratsbeschlusses, durch die der Europäischen Kommission ein klares Mandat** zur Teilnahme an diesen laufenden Verhandlungen im Namen der EU **erteilt wird.** Die Kommission ist am besten in der Lage sicherzustellen, dass das Protokoll mit der derzeitigen und künftigen EU-Gesetzgebung kompatibel ist. Dies würde der EU zusammen mit ihren Mitgliedstaaten gestatten, die Rechtmäßigkeit der künftigen Vereinbarung im Rahmen der Rechtsordnung der Union, einschließlich der Einhaltung der Charta der Grundrechte der Europäischen Union (im Weiteren die „Charta"), insbesondere des Rechts auf Schutz der Privatsphäre und auf Schutz personenbezogener Daten, sowie von Artikel 16 AEUV besser zu gewährleisten. Daher bezweckt diese Stellungnahme, die Organe der EU konstruktiv und objektiv zu beraten. Der EDSB steht der Kommission, dem Rat und dem Europäischen Parlament in weiteren Stadien dieses Prozesses zur Konsultation zur Verfügung.

10. Da sich die verschiedenen internationalen Übereinkünfte, die für den grenzüberschreitenden Austausch von Beweismaterial sorgen, auf die Grundrechte von betroffenen Personen sowie auf den Schutz von personenbezogenen Daten und den Schutz der Privatsphäre auswirken, ist es wichtig, dass der rechtliche Rahmen, innerhalb dessen dieser Austausch stattfindet, so klar wie möglich ist. In **Absatz e** des Anhangs heißt es: „*Das Zweite Zusatzprotokoll kann gelten, wenn keine anderen, spezifischeren internationalen Übereinkünfte bestehen, die die Europäische Union oder ihre Mitgliedstaaten und andere Vertragsparteien des Übereinkommens binden; wenn es aber solche internationalen Übereinkünfte gibt, gilt das Zusatzprotokoll nur insoweit, als bestimmte Fragen nicht durch diese Übereinkünfte geregelt werden*"[18]. Durch die Verwendung des Verbs „kann" ist die Art des geplanten Protokolls nicht eindeutig. **Zur Gewährleistung von Rechtssicherheit empfiehlt der EDSB die Verdeutlichung der verbindlichen und obligatorischen Natur des Instruments als Grundsatz**[19] sowie der Tatsache, dass es bilateralen Abkommen zwischen Vertragsparteien des Protokolls, die zum selben Thema abgeschlossen wurden, unterliegt, „*vorausgesetzt, dies erfolgt in Übereinstimmung mit den Zielen und Grundsätzen des Übereinkommens*". **Es sollte klargestellt werden, dass derartige bilaterale Abkommen auch künftige Abkommen betreffen, wie aus der Begründung der Empfehlung hervorgeht[20]. Gemäß der Empfehlung des EDSB sollte angegeben werden, dass dies nur zutreffen sollte, wenn bei der Anwendung der anderen spezifischen internationalen Übereinkunft im Vergleich zu dem geplanten Protokoll dasselbe oder ein höheres Schutzniveau hinsichtlich des Schutzes der Privatsphäre und von personenbezogenen Daten zum Tragen kommt**.

3.2. Notwendigkeit von detaillierten Garantien in Bezug auf die internationale Weitergabe von Daten und die Achtung der Grundrechte

11. Der EuGH befand, dass „*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*"[21].

12. Nach Ansicht des EDSB gehört zu den angemessenen Garantien des Rechts auf Schutz personenbezogener Daten in erster Linie **volle Übereinstimmung mit Artikel 8 der Charta in den Drittländern, in die personenbezogene Daten übermittelt würden**. Gemäß der Rechtsprechung des EuGH, so der EDSB, müssen sowohl Artikel 7 als auch

Artikel 8 der Charta in Verbindung mit **dem Recht auf einen wirksamen Rechtsbehelf gemäß Artikel 47 der Charta** beurteilt werden[22].

13. **Der EDSB begrüßt daher, dass dem Schutz der Privatsphäre und dem Schutz personenbezogener Daten im Anhang Aufmerksamkeit geschenkt wird.** Der EDSB teilt nämlich die Ansicht, dass Garantien für „*alle Ermittlungsbefugnisse gelten, also sowohl für die im Rahmen des Übereinkommens bestehenden als auch die durch das Zweite Zusatzprotokoll geschaffenen Ermittlungsbefugnisse*“[23]. Insbesondere scheinen **Absätze b und c** den Schutz personenbezogener Daten dem Schutz elektronischer Kommunikationsdaten gegenüberzustellen. Nach der Empfehlung des EDSB sollte klargestellt werden, dass das geplante Protokoll die Achtung sowohl der Grundrechte auf Privatsphäre einerseits als auch des Schutzes personenbezogener Daten andererseits, unabhängig davon, ob sie elektronische Kommunikationsdaten darstellen oder nicht, sicherstellt.

14. **Zweckbindung** ist ein wesentlicher Datenschutzgrundsatz. In den empfohlenen Verhandlungsrichtlinien werden weder Grenzen für die Zusammenarbeit im Rahmen des geplanten Protokolls genannt noch enthalten sie spezifische Einschränkungen der Weiterverarbeitung der übermittelten personenbezogenen Daten durch die ersuchende Behörde des Drittlandes. **Der EDSB empfiehlt die genaue Spezifizierung der Übermittlungszwecke im Anhang sowie das Verbot einer Weiterverarbeitung, die mit diesen Zwecken nicht vereinbar ist.**

15. Der EDSB betont, dass die Einhaltung dieses Grundsatzes eng mit den Zuständigkeitsbereichen der Empfänger in den empfangenden Drittländern verknüpft ist. Der Zuständigkeitsbereich der jeweiligen Behörden in den Drittländern, an die Daten übermittelt würden und die diese Daten verarbeiten würden, sollte genau definiert werden, damit sichergestellt ist, dass sie auch für die Zwecke der Übermittlung zuständig sind. In diesem Sinne **empfiehlt** der EDSB daher, **dass dem geplanten Protokoll 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 der Anlange zum Ausdruck gebracht werden.**

16. A rüber hinaus würde es beim Schicken und Beantworten von Anweisungen zur Datenherausgabe gemäß dem geplanten Protokoll zu der **Übermittlung von personenbezogenen Daten** kommen. Im Juli 2017 erging das Gutachten 1/15[24] des EuGH über das internationale Abkommen über die Übermittlung von Fluggastdatensätzen (PNR) nach Kanada, in dem das Gericht die Bedingungen festlegt, unter denen ein internationales Abkommen eine Rechtsgrundlage für die Übermittlung von personenbezogenen Daten darstellen kann. In dem Gutachten des EuGH heißt es, dass „*eine Weitergabe personenbezogener Daten aus der Union in ein Drittland nur zulässig ist, wenn das Drittland ein Schutzniveau der Grundrechte und Grundfreiheiten gewährleistet, das dem in der Union garantierten Niveau der Sache nach gleichwertig ist*“[25]. **Aus dem Gutachten 1/15 folgt also, dass das sich aus dem geplanten Protokoll über den Austausch personenbezogener Daten mit Drittländern ergebende Schutzniveau ähnlich** (wie beim Abkommen zwischen der EU und Kanada über den Austausch von PNR-Daten) **der Sache nach dem Schutzniveau im Unionsrecht gleichwertig sein sollte.**

17. In dieser Beziehung betont der EDSB, dass zwar alle Mitgliedstaaten Vertragsparteien des im Strafverfolgungsbereich geltenden Übereinkommens 108[26] des Europarats sind, aber nicht alle Drittländer-Vertragsparteien des Übereinkommens über Computerkriminalität auch Vertragsparteien des Übereinkommens 108 sind.[27] Es ist daher **besonders wichtig, die Aufnahme von wirksamen und detaillierten Garantien in das geplante Protokoll sicherzustellen**. Des Weiteren betont der EDSB die Bedeutung des Sammelns von Informationen über das Niveau des Schutzes von personenbezogenen Daten von Drittländervertragsparteien des Übereinkommens über Computerkriminalität[28] sowie über ihren politischen Kontext, **um genau die Garantien definieren zu können, die notwendig sind.**

3.3. Direkter Zugriff von Strafverfolgungsbehörden auf Daten

18. Gemäß der Empfehlung[29] kann das Protokoll „*Bestimmungen in Bezug auf die „Erweiterung von Abfragen/Zugriffen auf der Grundlage von Benutzerrechten"*[30] *und „Ermittlungstechniken" einschließen*". In ihrer Folgenabschätzung für den e-Beweismittel-Vorschlag beurteilte die Kommission die Möglichkeit der Einführung einer Bestimmung über direkten Zugriff auf EU-Niveau und entschied sich dagegen. Aus der Empfehlung geht jedoch hervor[31], dass die Annahme eines e-Beweismittel-Pakets auf der Grundlage der Vorschläge der Kommission nach Ansicht der Kommission Mitgliedstaaten nicht daran hindern würde, derartige Maßnahmen beizubehalten oder anzunehmen[32].

19. Der EDSB merkt an, dass Garantien in dem Mandat gemäß **Absatz m des Anhangs** vorgesehen sind. **Der EDPS ist** jedoch **der Ansicht, dass diese Maßnahme besonders eingreifend ist und sich daher stärker auf die Grundrechte auf Privatsphäre und den Schutz von personenbezogenen Daten auswirkt.** Ohne weitere Verdeutlichungen der spezifischen Maßnahmen und ohne geplante wirksamere Garantien **empfiehlt er** somit **die Ablehnung der Aufnahme derartiger Bestimmungen in das Protokoll.** Er bezieht sich auf die Anmerkungen der Artikel 29 Datenschutzgruppe über den direkten Zugriff von Drittländer-Strafverfolgungsbehörden auf Daten, die in anderen Gerichtsbarkeiten gespeichert sind, wie in den Entwurfselementen für ein Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität vorgeschlagen[33]. Er lehnt **Absatz n des Anhangs** ab, nach dem die Europäische Union „*auch sicherstellen sollte, dass sie die derzeit in den Mitgliedstaaten vorgesehenen Möglichkeiten für einen solchen Zugriff nicht einschränkt*".

4. WEITERE EMPFEHLUNGEN

20. Zu den Verhandlungsrichtlinien im Anhang der Empfehlungen möchte der EDSB folgende allgemeine Anmerkungen und spezifische Empfehlungen aussprechen. Der EDSB begrüßt es, dass in mehreren Richtlinien auf die Sicherstellung angemessener Datenschutzgarantien eingegangen wird. Nach seiner Ansicht sollten jene Grundsätze und Garantien weiter spezifiziert und verstärkt werden.

21. Der EDSB möchte auf die Bedeutung des Vorsehens konkreter, spezifischer und wirksamer Garantien bestehen. In Anbetracht des Strafverfolgungskontexts und der potenziellen Risiken, die solche Datenübermittlungen für betroffene Personen bedeuten

können, sollten die in diesem Protokoll mit Drittländern vorgesehenen Garantien auf zufriedenstellende Weise auf diese Risiken eingehen und sie mindern.

4.1. Rechtsgrundlage des Beschlusses des Rats

22. In der Begründung der Empfehlung heißt es: „*Der Gegenstand des Zweiten Zusatzprotokolls würde [...] fallen, was insbesondere auf Rechtsinstrumente zur justiziellen Zusammenarbeit in Strafsachen (Artikel 82 Absatz 1 AEUV) und zum Datenschutz (Artikel 16 AEUV) zutrifft [...]*“[34]. Diese beiden Bestimmungen werden auch in Erwägungsgrund 6 der Empfehlung erwähnt; dort heißt es wie folgt: „*In Artikel 82 Absatz 1 und Artikel 16 des Vertrags über die Arbeitsweise der Union werden die Zuständigkeiten der Union auf dem Gebiet der justiziellen Zusammenarbeit in Strafsachen sowie beim Datenschutz und Schutz der Privatsphäre festgelegt. Um die Integrität des Unionsrechts zu schützen und den Fortbestand der Kohärenz zwischen den Regeln des Völkerrechts und denen des Unionsrechts sicherzustellen, muss sich die Union an den Verhandlungen über das Zweite Zusatzprotokoll beteiligen*“. Die materielle Rechtsgrundlage des Rechtsakts wird jedoch in den Bezugsvermerken in der Präambel der Empfehlung nicht genannt.

23. Gemäß Artikel 296 Absatz 2 AEUV und der ständigen Rechtsprechung des EuGH[35] beanstandet der EDSB die Tatsache, dass in den Bezugsvermerken in der Präambel des Beschlusses des Rates nur die angemessene Verfahrensrechtsgrundlage und nicht gleichermaßen die relevante materielle Rechtsgrundlage genannt wird.

24. **Der EDSB empfiehlt, dass in den Bezugsvermerken in der Präambel des Beschlusses des Rates nicht nur die angemessene Verfahrensrechtsgrundlage, sondern auch die relevante materielle Rechtsgrundlage, darunter Artikel 16 AEUV, genannt werden.** Es folgt bereits aus Abschnitt 1 des Anhangs über die Verhandlungsrichtlinien, dass die Kommission während der Verhandlungen über das geplante Protokoll gleichzeitig mehrere Ziele verfolgen sollte, zu denen die Sicherstellung der Achtung der in der Charta verankerten Grundrechte, einschließlich der Rechte auf Schutz der Privatsphäre und auf Schutz personenbezogener Daten gehört, so dass die rechtmäßige Übermittlung von personenbezogenen Daten erfolgen kann. Das geplante Protokoll würde sich somit tatsächlich direkt auf den von Artikel 16 AEUV verfolgten Zweck beziehen.

25. Der EDSB erinnert daran, dass der EuGH in einem ähnlichen Strafverfolgungskontext feststellte, dass „*der Beschluss des Rates über den Abschluss des geplanten Abkommens [zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen] auf Artikel 16 Absatz 2 gemeinsam mit Artikel 87 Absatz 2 Buchstabe a AEUV zu stützen ist* “[36].

4.2. Weitergaben

26. Hinsichtlich der Weitergabe durch die annehmende Behörde im Drittland an ein weiteres Drittland weist der EDSB darauf hin, dass gemäß dem Gutachten 1/15 des EuGH vom Juli 2017 dasselbe Erfordernis der Gewährleistung eines Schutzniveaus, das dem in der Union garantierten Niveau der Sache nach gleichwertig ist, „*auch im Fall der [...] Weitergabe von PNR-Daten durch Kanada an Drittländer gilt. Damit soll verhindert werden, dass das im Abkommen vorgesehene Schutzniveau durch die Weitergabe personenbezogener Daten an Drittländer umgangen werden könnte, und gewährleistet werden, dass das vom Unionsrecht gewährte Schutzniveau fortbesteht*“. Der Gerichtshof fügte Folgendes hinzu: „*Die Weitergabe personenbezogener Daten an ein Drittland*

erfordert daher ein Abkommen zwischen der Union und dem betreffenden Drittland, das dem geplanten Abkommen äquivalent ist, oder einen [Angemessenheits-]Beschluss der Kommission [...], der sich auf die Behörden erstreckt, an die PNR-Daten weitergegeben werden sollen“[37]. **Der EDSB empfiehlt** daher **die Aufnahme dieses zusätzlichen Erfordernisses in die Verhandlungsrichtlinien.**

4.3. Rechte betroffener Personen

27. Der EDSB nimmt ferner die Tatsache zur Kenntnis, dass die Anlage keine spezifische Richtlinie über die Rechte betroffener Personen enthält. Das Recht auf Auskunft und das Recht auf Berichtigung sind als wesentliche Elemente des Rechts auf den Schutz personenbezogener Daten in Artikel 8 Absatz 2 der Charta festgeschrieben. Der EDSB ist sich der Tatsache bewusst, dass die Ausübung der Rechte betroffener Personen im Strafverfolgungskontext üblicherweise eingeschränkt ist, um laufende Ermittlungen nicht zu gefährden. Dessen ungeachtet stellte der EuGH jüngst in seinem Gutachten 1/15 fest, dass „*den Fluggästen die Weitergabe ihrer PNR-Daten an Kanada und die Verwendung dieser Daten mitgeteilt werden [muss], sobald dies die Ermittlungen der im geplanten Abkommen genannten Behörden nicht mehr beeinträchtigen kann*“, wenn berücksichtigt wird, dass „ *[d]iese Mitteilung nämlich der Sache nach erforderlich [ist], damit die Fluggäste ihr Recht auf Auskunft über die sie betreffenden PNR-Daten und gegebenenfalls auf Berichtigung der Daten sowie ihr Recht, gemäß Artikel 47 der Charta bei einem Gericht einen wirksamen Rechtsbehelf einzulegen, ausüben können*“ [38].

28. **Der EDSB empfiehlt** daher **die Aufnahme des Rechts auf Information und des Rechts auf Auskunft in die Verhandlungsrichtlinien, so dass die Vertragsparteien des geplanten Protokolls sicherstellen, dass die Einschränkungen der Ausübung des Rechts auf Auskunft gezielt auf das Unerlässliche begrenzt sind, um die damit verfolgten öffentlichen Interessen zu wahren und die Verpflichtung der zuständigen Behörden zur Transparenz Nachdruck erhält.**

4.4. Überwachung durch eine unabhängige Behörde

29. Sowohl Artikel 16 AEUV als auch Artikel 8 Absatz 3 der Charta sehen als wesentliche Garantie des Rechts auf Datenschutz die Überwachung durch eine unabhängige Behörde vor. Zwar ernennt jeder Mitgliedstaat eine unabhängige Behörde, die für die Aufsicht über die Datenverarbeitungstätigkeiten einschließlich der Weitergabe von Daten an Drittländer zuständig ist, doch bedarf es auch in den empfangenden Drittländern einer wirksamen unabhängigen Aufsicht, sobald die Daten übermittelt wurden.

30. Der EDSB erinnert daran, dass nach der Rechtsprechung des EuGH[39] eine unabhängige Aufsichtsbehörde im Sinne von Artikel 8 Absatz 3 der Charta eine Behörde ist, die ihre Entscheidungen ohne jede unmittelbare oder mittelbare äußere Einflussnahme erlassen kann. Eine solche Aufsichtsbehörde muss nicht nur von den von ihr kontrollierten Stellen unabhängig sein, sondern sie sollte auch nicht „*einer Aufsichtsbehörde untergeordnet sein, von der sie Weisungen erhalten kann*“, da dies implizieren würde, dass sie „*nicht vor jeder äußeren Einflussnahme auf ihre Entscheidungen geschützt ist*“[40].

31. Der EDSB merkt an, dass in den Verhandlungsrichtlinien nicht spezifisch auf dieses Erfordernis eingegangen wird.

32. Der EDSB empfiehlt, dass die Verhandlungsrichtlinien auf die Aufnahme eines **Mechanismus** in das Protokoll abzielen sollten, **nach dem jedes Land, das eine**

Vertragspartei des Protokolls ist, die spezifische Behörde oder spezifischen Behörden klar kennzeichnen muss, die von ihm mit der unabhängigen Überwachung der Einhaltung der Regeln des geplanten Protokolls **betraut wird bzw. werden.** Im Protokoll sollten die **Befugnisse** genannt werden, die diese spezifische Behörde oder spezifischen Behörden gegenüber Behörden haben können, an die personenbezogene Daten auf der Grundlage des geplanten Protokolls übermittelt würden.

4.5. Gerichtliche und administrative Rechtsbehelfe

33. Der EDSB erinnert daran, dass der EuGH festgestellt hat,[41] dass das Fehlen eines wirksamen gerichtlichen Rechtsbehelfs im Falle der Übermittlung personenbezogener Daten an ein Drittland dem Wesensgehalt von Artikel 47 der Charta, der das Recht auf wirksamen gerichtlichen Rechtsschutz vorsieht, widerspricht. In diesem Zusammenhang befand der EuGH, dass „*eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz*“ verletzt und stellte fest: „*Nach Art. 47 Abs. 1 der Charta hat nämlich jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht* ***einen wirksamen Rechtsbehelf*** *einzulegen*“[42].

34. Der EuGH hat außerdem betont, dass es für natürliche Personen wesentlich ist, Beschwerden bei unabhängigen Kontrollstellen vorbringen[43] und somit einen administrativen Rechtsbehelf einlegen zu können.

35. **Nach der Empfehlung des EDSB sollte das Ziel der Sicherstellung, dass die Gewährleistung durch das Protokoll, dass beide Rechtsbehelfe allen betroffenen Personen zur Verfügung stehen, in das Mandat aufgenommen werden,** und zwar umso mehr, als nicht alle Vertragsparteien des Übereinkommens über Computerkriminalität unter die Zuständigkeit des Europäischen Gerichtshofs für Menschenrechte fallen.

4.6. Straftaten, die von dem Protokoll abgedeckt werden, und Kategorien personenbezogener Daten

36. Gemäß der Rechtsprechung des EuGH kann der Zugriff durch öffentliche Behörden auf personenbezogene Daten, die von Diensteanbietern auf Vorrat gespeichert werden, nur mit der Bekämpfung schwerer Straftaten begründet werden, denn „*[a]us der Gesamtheit solcher Daten können nämlich sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden*“[44]. Können derartige Schlussfolgerungen nicht gezogen werden und Zugriff daher nicht „*als ein schwerer Eingriff in die Grundrechte der Personen, deren Daten betroffen sind, definiert werden kann*“, stellte das Gericht weiterhin fest, dass „*der Eingriff, zu dem es durch den Zugriff auf derartige Daten kommt, durch den Zweck der (...) Prävention, Ermittlung, Aufdeckung und der strafrechtlichen Verfolgung von „Straftaten“ allgemein gerechtfertigt werden kann, ohne dass diese Straftaten als „schwer“ kategorisiert werden müssten*“[45].

37. Hinsichtlich des Erwerbs von Erkenntnissen über die **Inhaltsdaten** geht aus der Rechtsprechung des EuGH hervor, dass dadurch dem Wesen des Rechts auf Achtung der Privatsphäre zuwidergehandelt wird[46].

38. In Bezug auf Nichtinhaltsdaten stellte der EuGH hinsichtlich Metadaten wie Verkehrs- und Standortdaten, die von Anbietern öffentlich verfügbarer elektronischer Kommunikationen auf Vorrat gespeichert werden, Folgendes fest: „*Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren*“[47] und „*[diese Daten] ermöglichen […] die Erstellung des Profils der betroffenen Personen, das im Hinblick auf das Recht auf Achtung der Privatsphäre eine genauso sensible Information darstellt wie der Inhalt der Kommunikationen selbst*“[48].

39. **Der EDSB betont die Bedeutung der Festlegung von klaren und unkomplizierten Definitionen von Datenkategorien in dem geplanten Protokoll, um Rechtssicherheit** für alle Beteiligten **sicherzustellen**. Insoweit die Definitionen von Datenkategorien in dem e-Beweismittel-Vorschlag als Bezug verwendet würden, wie vom EDSB bereits erwähnt[49], **empfiehlt der EDSB die Sicherstellung einer klaren Abgrenzung zwischen Datenkategorien und die Vermeidung von Überschneidungen, was einen entscheidenden Beitrag zur Gewährleistung von Rechtssicherheit** hinsichtlich der materiellrechtlichen Bestimmungen des Protokolls **leisten würde.**

40. Zur Einhaltung der Verhältnismäßigkeitsbedingung von Artikel 52 Absatz 1 der Charta ist der EDSB der Ansicht, dass ein Gleichgewicht zwischen den Arten von Straftaten, für die die Herausgabe und die Weitergabe von personenbezogenen Daten angeordnet werden könnten, und den betreffenden Datenkategorien erreicht werden sollte. Unterscheidungen sollten somit auf der Schwere der ermittelten oder strafrechtlich verfolgten Straftaten und auf dem geforderten Niveau von Intrusivität und Sensitivität der Datenkategorien beruhen. Daher **empfiehlt der EDSB, dass in den Verhandlungsrichtlinien festgelegt wird, dass auch Unterscheidungen auf der Grundlage der Schwere der betreffenden Straftaten getroffen werden sollten.** In dieser Beziehung **spricht sich der EDSB für die Definierung einer gemeinsamen Liste von Straftaten aus, bei der nach Schwere der Straftaten unterschieden wird und die je nach der Intrusivität der im Protokoll vorgesehenen Maßnahmen variieren kann.**

4.7. Informationssicherheit

41. Nach Ansicht des EDSB ergeben sich durch das geplante Protokoll wichtige Fragen über die Sicherheit der grenzüberschreitenden eingehenden und abgehenden Übermittlung von personenbezogenen Daten. Der EDSB möchte betonen, dass die Gewährleistung der Sicherheit von personenbezogenen Daten nicht nur ein klares Erfordernis nach EU-Recht ist[50], sondern auch vom EuGH in Bezug auf das Wesen des Grundrechts auf Datenschutz erwogen wird. Auch bei der Gewährleistung der Vertraulichkeit von Ermittlungen und Strafverfahren ist Datensicherheit wesentlich.

42. **Der EDSB empfiehlt** daher **die Aufnahme weiterer zusätzlicher Garantien über den Schutz der Privatsphäre und den Datenschutz in dem Mandat, um ein angemessenes Niveau an Sicherheit für die herausgegebenen und übermittelten personenbezogenen Daten sicherzustellen. Darüber hinaus sollte in dem Mandat insbesondere auf die Fragen der Authentizität von Anordnungen und die Sicherheit der Übermittlung von personenbezogenen Daten an die ersuchenden Behörden, die sichergestellt werden sollten, eingegangen werden**.

4.8. Vorrechte und Immunitäten

43. Das Mandat sollte nach Empfehlung des EDSB außer der Bereitstellung angemessener Garantien für den Schutz personenbezogener Daten auch Anweisungen dahingehend enthalten, dass das Protokoll die Beachtung anderer Garantien im Zusammenhang mit Daten wie Vorrechte und Immunitäten sicherstellt.

4.9. Ersuchen um Rechtshilfe in Notfällen[51]

44. Gemäß **Absatz g** sollte die Europäische Union den Entwurf und den vorläufig angenommenen erläuternden Bericht unterstützen und der Umfang der Rechtshilfe sollte mit dem in Artikel 25 des Übereinkommens über Computerkriminalität dargelegten Umfang übereinstimmen. Solange ein Querverweis auf eine bestimmte Version des Entwurfs fehlt, beruhen die Anmerkungen des EDSB auf dem vorläufigen Entwurf vom 28. November 2018, der online auf der Website des Europarats abrufbar ist[52]. **Gemäß der Empfehlung des EDSB sollte die Möglichkeit vorgesehen werden, die beiden Zielsetzungen der Verbrechensbekämpfung und der Wahrung der Grundrechte miteinander zu vereinbaren, indem sichergestellt wird, dass die ersuchende Vertragspartei gemäß dem Protokoll spezifische Garantien und Bedingungen** für die Übermittlung **verlangen** und in der Lage sein kann, die Rechtshilfe aus Datenschutzgründen zu verweigern[53].

4.10. Unmittelbare grenzüberschreitende Zusammenarbeit zwischen Strafverfolgungsbehörden und Diensteanbietern

a) Spezielle EU-rechtliche Bedingungen für die direkte Übermittlung von personenbezogenen Daten durch mitgliedstaatliche Strafverfolgungsbehörden an Diensteanbieter in Drittländern

45. In diesem Zusammenhang wird auf Artikel 35 Absatz 1 der Richtlinie zum Datenschutz bei der Strafverfolgung verwiesen[54], in dem spezifische Bedingungen festgelegt werden, die eine mitgliedstaatliche Strafverfolgungsbehörde erfüllen muss, damit Daten rechtmäßig an in Drittländern niedergelassene Empfänger übermittelt werden, einschließlich des Grundsatzes, dass der Empfänger derartiger Übermittlungen in der Regel eine zuständige Behörde eines Drittlandes sein muss, für die Zwecke der „Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“. Übermittlungen durch mitgliedstaatliche Strafverfolgungsbehörden an andere Empfänger, einschließlich an in Drittländern niedergelassene nichtöffentliche Stellen, sind nur in Ausnahmefällen gemäß Artikel 39 der Richtlinie zum Datenschutz bei der Strafverfolgung[55] und nur dann gestattet, wenn weitere spezifische Bedingungen[56] erfüllt sind. Zu diesen spezifischen Bedingungen zählen insbesondere, dass die zuständige Datenschutzbehörde in ihrem Mitgliedstaat informiert werden muss und dass die Übermittlung dokumentiert werden muss[57]. **Nach dem Dafürhalten des EDSB sollte das geplante Protokoll zumindest jene durch Artikel 39 der Richtlinie zum Datenschutz bei der Strafverfolgung angeregten zusätzlichen Bedingungen enthalten, damit der durch diese Richtlinie geforderte Datenschutz nicht verwässert wird.**

b) Definitionen und Datenarten

46. Gemäß der Empfehlung würde die geplante Bestimmung Bestandsdaten betreffen[58]. Der EDSB begrüßt **Absatz k**, in dem vorgesehen ist, dass das Protokoll „*geeignete Grundrechtegarantien*" enthalten sollte, „*wobei die verschiedenen Sensibilitätsebenen der betroffenen Datenkategorien und die in den europäischen Herausgabeanordnungen für die verschiedenen Datenkategorien enthaltenen Garantien zu berücksichtigen sind* ".

47. Das Protokoll wäre eine Gelegenheit, die Definitionen der Datenkategorien zu verfeinern, um die Implementierung des Übereinkommens gegebenenfalls unter Berücksichtigung des Ergebnisses der Verhandlungen über den e-Beweismittel-Vorschlag zu erleichtern. **Der EDSB betont in dieser Beziehung die Bedeutung der Festlegung von klaren und unkomplizierten Definitionen von Datenkategorien in dem geplanten Protokoll, um Rechtssicherheit für alle Beteiligten in der EU und in Drittvertragsstaaten sicherzustellen.** Die Möglichkeit, die Herausgabe und die Übermittlung von Inhaltsdaten oder Nichtinhaltsdaten anzuordnen, aus deren Gesamtheit sehr genaue Schlüsse auf das Privatleben der betreffenden Personen gezogen werden können, sollte ausschließlich auf Schwerverbrechen beschränkt werden (siehe Absatz 4.6 oben).

c) Beteiligung von Justizbehörden in anderen Ländern, die Vertragsparteien des Protokolls sind

48. In Bezug auf **Absatz I des Anhangs**[59] weist der EDSB darauf hin, dass er die Annahme, dass die Garantien, die aus „*Mitteilung und Zustimmung des Staates des Diensteanbieters und eine vorherige Überprüfung durch ein Gericht oder eine unabhängige Verwaltungsstelle*" bestehen, ein Zusatz zu dem e-Beweismittel-Vorschlag sind, als verfrüht hält, da die Verhandlungen über diesen Vorschlag noch laufen. Der EDSB **empfiehlt, vorsichtiger vorzugehen, indem im Anhang Richtlinien zur Unterstützung relevanter zusätzlicher Garantien und Verweigerungsgründe im Vergleich zum EU-Sekundärrecht über das Sammeln elektronischer Beweismittel in Strafsachen bereitgestellt werden, wie dies für die Sicherstellung des angemessenen Niveaus an Garantien insbesondere hinsichtlich Datenschutz und des Schutzes der Privatsphäre erforderlich ist.**

49. Insbesondere fand der EDSA, zu dessen Mitgliedern der EDSB zählt, sogar im EU-Kontext „*keine Rechtfertigung für das im Entwurf der Verordnung über elektronische Beweismittel vorgesehene Verfahren, das die Herausgabe von Inhaltsdaten ohne Beteiligung zumindest der zuständigen Behörden des Mitgliedstaats, in dem sich die betroffene Person befindet, ermöglicht*"[60]. Im Rat wurde keine Notifizierung an die Behörden des Mitgliedstaats, in dem sich die betroffene Person aufhält, eingeführt.

50. In seiner Stellungnahme zu dem e-Beweismittel-Vorschlag äußerte der EDSA ferner „*seine Bedenken hinsichtlich der Aufhebung jeglicher (doppelten) Überprüfung der übermittelten Anordnung durch die empfangende zuständige Behörde im Vergleich zu den anderen Instrumenten*"[61]. Im Rat forderten mehrere Mitgliedstaaten größere Vollmachten für die notifizierte Behörde, die über die Notifizierung gemäß der allgemeinen Ausrichtung hinausgehen und auch Nichtinhaltsdaten abdecken[62].

51. Bei dem herkömmlichen Ansatz zu dem grenzüberschreitenden Zugriff auf elektronische Beweismittel obliegt die Sicherstellung, dass begrenzte Verweigerungsgründe überprüft

werden, in erster Linie der verfolgenden Behörde. Der EDSB erkennt die Notwendigkeit, dass alternative Ansätze für das Sammeln von Beweismaterial in einem grenzüberschreitenden Kontext identifiziert werden müssen, zwar an, aber es ist und bleibt von ausschlaggebender Bedeutung, dass wirksame Garantien für die Grundrechte der betroffenen Person vorliegen. Es muss berücksichtigt werden, dass zwischen dem in den jeweiligen Vertragsländern des Protokolls geltenden Recht, unter anderem in Bezug auf die Zulässigkeit von in einem anderen Land gesammelten Beweismaterialien und darauf, was eine Straftat darstellt, Diskrepanzen bestehen können. Bedingungen für das Ergehen einer Anordnung sind in Bezug auf die Sache auf internationaler Ebene nicht harmonisiert, und gegen die Anerkennung und Vollstreckung einer solchen Anordnung können wichtige Einwände bestehen[63]. Ferner besteht die Möglichkeit, dass Unternehmen nicht dahingehend ausgerüstet sind, die erforderliche Beurteilung durchzuführen. Es darf nicht vergessen werden, und dies ist von ausschlaggebender Bedeutung, dass Diensteanbieter nur die Empfänger von Anordnungen sind; ihre Rechte auf Schutz der Privatsphäre und auf Schutz personenbezogener Daten werden durch die Anordnung nicht eingeschränkt.

52. EU-Mitgliedstaaten haben bei der Implementierung von EU-Recht die rechtliche Verpflichtung, die Grundrechte zu beachten[64]. Diesbezüglich erinnert die Agentur der Europäischen Union für Grundrechte im Zusammenhang mit den Verhandlungen über den Richtlinienentwurf über die Europäische Ermittlungsanordnung[65] daran, dass „***der vollstreckende Staat unter Instrumenten wie der EMRK in die Verantwortung genommen wird, wenn die angemessene Einhaltung der Grundrechte bei der Vollstreckung einer Europäischen Ermittlungsanordnung nicht gewährleistet wird***“[66].

53. **Nach Ansicht des EDSB erfordert der wirksame Schutz der Grundrechte in diesem Zusammenhang ein bestimmtes Maß an Beteiligung der Behörden der ersuchenden Vertragspartei an dem geplanten Abkommen.** Dies ist außerdem eine zusätzliche Garantie in Fällen, bei denen der Aufenthaltsort der betroffenen Person nicht bekannt ist oder sich die betroffene Person in einem Drittland befindet, das kein Unterzeichnerstaat des Protokolls ist. **Er empfiehlt somit die Aufnahme der Verpflichtung der zuständigen Behörden der Unterzeichnerstaaten des Protokolls, die vom Vollstreckungsland bezeichneten justiziellen Behörden so früh wie möglich in das Verfahren zum Sammeln elektronischer Beweismittel einzubeziehen, damit diese Behörden die Möglichkeit erhalten, wirksam zu prüfen, ob die Grundrechte durch die Anordnungen eingehalten werden, und unter Umständen Verweigerungsgründe auf der Grundlage hinreichender Informationen und innerhalb realistischer Fristen vorzubringen, als spezifische Garantie in die Verhandlungsrichtlinien.** Eine solche Einbeziehung stünde auch mehr im Einklang mit Artikel 82 Absatz 1 AEUV (falls diese Rechtsgrundlage als eine der Rechtsgrundlagen des Beschlusses des Rates aufgenommen wird)[67].

d) Einspruchsmöglichkeit für Diensteanbieter

54. Diensteanbieter, bei denen eine Anordnung in Bezug auf elektronisches Beweismaterial von zuständigen Behörden eines Drittlandes, das zu den Unterzeichnerstaaten des Protokolls gehört, eingeht, können sich mit kollidierenden rechtlichen Verpflichtungen gemäß EU-Recht und dem Recht des Drittlandes konfrontiert sehen. Der EDSB begrüßt **Absatz c** der Verhandlungsrichtlinien, nach dem das Protokoll Rechtskollisionen verhindern sollte.

55. Nach Ansicht des EDSB sollte ein Diensteanbieter, dem eine Anordnung über elektronisches Beweismaterial zugestellt wurde, unter Nennung spezifischer, in dem geplanten Protokoll definierter Gründe wie fehlende oder falsche Informationen oder Grundrechtserwägungen Einspruch dagegen einlegen können[68]. Diese Gründe sollten klar definiert sein, damit Anbieter nicht die Möglichkeit haben, von Fall zu Fall zu entscheiden, ob und wie sie kooperieren. **Der EDSB empfiehlt** daher, **dass in den Verhandlungsrichtlinien spezifiziert wird, dass in dem Protokoll ein Mechanismus vorgesehen werden sollte, nach dem ein Diensteanbieter das Recht hat, auf der Basis von spezifischen, darin definierten Gründen Einspruch gegen eine Anordnung einzulegen**.

4.11. Aussetzung des Protokolls, wenn ein Land gegen das Protokoll verstoßen hat, und Prüfung

56. In **Abschnitt 3** des Anhangs, so merkt der EDSB an, wird die Möglichkeit der Kündigung des Protokolls in Anlehnung an die Bestimmungen des Übereinkommens über Computerkriminalität vorgesehen. Ähnlich vorliegenden Angemessenheitsentscheidungen auf der Grundlage von Artikel 45 DSGVO und Artikel 36 Absatz 5 der Richtlinie zum Datenschutz bei der Strafverfolgung **ist der EDSB der Ansicht, dass es** bei Angemessenheitsentscheidungen zu Strafverfolgungszwecken **von ausschlaggebender Bedeutung ist, eine Klausel in die Verhandlungsrichtlinien aufzunehmen, nach der die Aussetzung des Protokolls mit einem Drittland gestattet ist, wenn dieses Land gegen die Bestimmungen des Protokolls verstoßen hat**.

57. Ferner **empfiehlt der EDSB, dass in den Verhandlungsrichtlinien die Forderung der Einführung einer Klausel vorgesehen wird, in der die obligatorische Überprüfung der praktischen Funktion des Protokolls in regelmäßigen Abständen niedergelegt wird.** Zur Sicherstellung einer sinnvollen Überprüfung sollte diese spätestens ein Jahr nach dem Inkrafttreten des Protokolls 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 Protokolls, sondern auch auf die Beurteilung seiner Notwendigkeit und seiner Verhältnismäßigkeit konzentrieren. Für die Zwecke einer solchen Überprüfung sollte vorgesehen sein, dass die Vertragsparteien beim Sammeln von Informationen, einschließlich Statistiken und Rechtsprechung, über die praktische Funktion des Übereinkommens mit dem T-CY zusammenarbeiten. Zu den Überprüfungsteams sollten Datenschutzexperten gehören, und EU-Datenschutzbehörden sollten involviert sein.

5. SCHLUSSFOLGERUNGEN

58. Der EDSB ist sich der Tatsache bewusst, dass Strafverfolgungsbehörden elektronische Beweismittel schnell und effizient sichern und erlangen müssen. Zur Erlangung des grenzüberschreitenden Zugriffs auf elektronisches Beweismaterial bevorzugt er die Verwendung von innovativen Ansätzen und die Ermittlung einer EU-Lösung für bestehende Probleme in diesem Zusammenhang. Ein auf EU-Ebene ausgehandeltes Zweites Zusatzprotokoll wäre im Gegensatz zu einzelnen, von Mitgliedstaaten bilateral abgeschlossenen Vereinbarungen eine bessere Garantie für die Wahrung des vom EU-Datenschutzrahmen gewährten Schutzniveaus und würde ein einheitliches Maß an EU-

weitem Schutz gewährleisten. Daher bezweckt diese Stellungnahme, die Organe der EU konstruktiv und objektiv zu beraten, wenn die Kommission beim Rat um Genehmigung zur Teilnahme an den Verhandlungen zu diesem Protokoll nachsucht.

59. Der EDSB begrüßt es, dass das Mandat darauf abzielt, zu gewährleisten, dass das Protokoll angemessene Garantien für den Datenschutz enthält.

60. Der EDSB hat drei wesentliche Verbesserungen ermittelt, deren Umsetzung er für das geplante Protokoll empfiehlt, um eine Übereinstimmung mit der Charta und Artikel 16 AEUV zu gewährleisten. Gemäß der Empfehlung des EDSB sollten die Verhandlungsrichtlinien auf Folgendes ausgerichtet sein:
    - Gewährleistung, dass das geplante Protokoll verbindlich ist,
    - Einführung detaillierter Garantien wie etwa des Grundsatzes der Zweckbindung aufgrund der verschiedenen potenziellen Unterzeichnerstaaten, von denen nicht alle das Übereinkommen Nr. 108 oder eine dem EU-US-Rahmenabkommen entsprechende Vereinbarung unterzeichnet haben,
    - Ablehnung jeglicher Bestimmungen über den direkten Zugriff auf Daten.

61. Zusätzlich zu diesen allgemeinen Empfehlungen beziehen sich die Empfehlungen und Anmerkungen des EDSB in der vorliegenden Stellungnahme auf die folgenden spezifischen Aspekte:

    - die Rechtsgrundlage des Beschlusses des Rats;
    - die Weiterübermittlung durch zuständige Behörden von Drittländern;
    - die Recht von betroffenen Personen, insbesondere das Recht auf Belehrung und Unterrichtung und das Recht auf Auskunft;
    - die Überwachung durch eine unabhängige Behörde;
    - Rechtsmittel und administrative Rechtsbehelfe;
    - die Straftaten, die von dem geplanten Protokoll abgedeckt werden, und Kategorien personenbezogener Daten;
    - die spezifischen Garantien zur Sicherstellung eines angemessenen Sicherheitsniveaus für die übermittelten Daten;
    - die spezifischen Garantien für durch Vorrechte und Immunitäten geschützte Daten;
    - die Rechtshilfe in Notfällen;
    - im Falle von unmittelbarer Zusammenarbeit, Übermittlung von personenbezogenen Daten, Definition und Datenarten, Beteiligung anderer Behörden, Möglichkeit, dass Diensteanbieter, denen eine Anordnung in Bezug auf elektronisches Beweismaterial zugestellt worden ist, auf der Basis von spezifischen Gründen Einspruch einlegen können;
    - die Möglichkeit, das Protokoll bei Verstößen gegen seine Bestimmungen auszusetzen und es zu überprüfen.

62. Abschließend weist der EDSB darauf hin, dass er der Kommission, dem Rat und dem Europäischen Parlament in den weiteren Phasen dieses Prozesses zur Konsultation zur Verfügung steht. Die Anmerkungen in dieser Stellungnahme sind vorbehaltlich etwaiger zusätzlicher Anmerkungen, die der EDSB anfügen könnte, da sich weitere Problematiken ergeben können, die dann angegangen werden würden, sobald weitere Informationen verfügbar sind. Er geht davon aus, später vor der abschließenden Bearbeitung über die Bestimmungen des Protokollentwurfs konsultiert zu werden.

Brüssel, 2. April 2019

Giovanni Buttarelli

Europäischer Datenschutzbeauftragter

ANMERKUNGEN

[1] ABl. L 119 vom 4.5.2016, S. 1 (nachstehend „DSGVO“).
[2] ABl. L 295 vom 21.11.2018, S. 39.
[3] ABl. L 119 vom 4.5.2016, S. 89 (nachstehend „Richtlinie zum Datenschutz bei der Strafverfolgung“).
[4] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, COM(2018) 225 final.
[5] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafsachen, COM(2018)226 final.
[6] Der Rat hat seinen allgemeinen Standpunkt zu der vorgeschlagenen Verordnung am 7. Dezember 2018 festgelegt, abrufbar unter https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/#. Der Rat hat seinen allgemeinen Standpunkt zu der vorgeschlagenen Verordnung am 8. März 2018 festgelegt, abrufbar unter https://www.consilium.europa.eu/en/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/.
[7] Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen, COM(2019) 70 final.
[8] Empfehlung für einen Beschluss des Rates zur Genehmigung der Teilnahme an Verhandlungen über ein Zweites Zusatzprotokoll zum Übereinkommen des Europarats über Computerkriminalität (SEV Nr. 185), COM(2019) 71 final.
[9] EDSB-Stellungnahme 2/2019 zu dem Verhandlungsmandat einer EU-US-Vereinbarung über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln.
[10] Übereinkommen über die verstärkte internationale Zusammenarbeit bei Computerkriminalität und elektronischen Beweismitteln, Budapest, 23. November 2001, SEV Nr. 185.
[11] 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/-/conventions/treaty/185/signatures?p_auth=ZZawh58m
[12] T-CY-Leitfaden # 3 Grenzüberschreitender Zugriff auf Daten (Artikel 32) T-CY (2013)7 E , S. 3, abrufbar unter:
https://rm.coe.int/16802e726a
[13] Siehe die Europarat-Webpage, abrufbar unter: https://rm.coe.int/t-cy-pd-pubsummary/168076316e.
[14] Dies betrifft Fälle, in denen Behörden Direktersuchen bezüglich Datensicherung und Datenherausgabe an Diensteanbieter im Hoheitsgebiet eines anderen Mitgliedstaats stellen.
[15] Dies betrifft Fälle, in denen Behörden selbst grenzüberschreitend direkt und ohne Vermittlung auf Daten zugreifen.
[16] Mandat für die Ausarbeitung eines Entwurfs für das 2. Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität, Juni 2017, abrufbar unter: https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b.
[17] Siehe Factsheet der Europäische Kommission, abrufbar unter: http://europa.eu/rapid/press-release_MEMO-19-865_en.htm
[18] Nachträgliche Hervorhebung.
[19] Siehe Vorl. Dok. Nr. 10 vom Dezember 2008 – Die Verbindlichkeit / Unverbindlichkeit des Übereinkommens über die Beweisaufnahme im Ausland [in Zivil- oder Handelssachen]: https://assets.hcch.net/upload/wop/2008pd10e.pdf.
[20] S. 7.
[21] Verbundene Rechtssachen C-402/05 P und C-415/05 P, Kadi / Rat, ECLI:EU:C:2008:461, Rn. 285 [nachträgliche Hervorhebung].
[22] Rechtssache C-362/14, Maximillian Schrems / Data Protection Commissioner, ECLI:EU:C:2015:650, Rn. 95.
[23] Siehe insbesondere Absatz b, c, m und o des Anhangs.
[24] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592.
[25] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 214; siehe ferner Rn. 93 des Gutachtens 1/15.
[26] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Straßburg, 28. Januar 1981, SEV Nr. 108 (im Weiteren „Übereinkommen 108“).

[27] Siehe diesbezüglich Art. 29 WP Stellungnahme 4/2001 über den Entwurf des Europarats eines Übereinkommens über Computerkriminalität vom 22. März 2001 (5001/01/EN/ Final WP 41), S. 6: „Unterzeichnerstaaten sollten aufgefordert werden, das Übereinkommen 108 des Europarats zu unterzeichnen".
[28] Insbesondere hat sich herausgestellt, dass nicht alle Drittländervertragsparteien des Übereinkommens über Computerkriminalität auch Vertragsparteien des Übereinkommens 108 oder der Europäischen Menschenrechtskonvention sind und dass einige von ihnen Vertragsparteien des Übereinkommens über IT-Sicherheit und den Schutz personenbezogener Daten der Afrikanischen Union sind. Das Protokoll zur Änderung des Übereinkommens 108, das sogenannte Übereinkommen 108+, ist noch nicht wirksam geworden. Es ist zwar von vielen Mitgliedstaaten unterzeichnet worden, ist aber noch nicht ratifiziert — siehe Unterschriften und Ratifikationsstand des Übereinkommens 108+: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures
[29] Begründung, S. 6.
[30] Arbeitsdokument der Kommissionsdienststellen: Folgenabschätzung, SWD(2018) 118 final (im Weiteren „Folgenabschätzung für den e-Beweismittel-Vorschlag"), abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN, S. 33: „Erweiterter Zugriff, d. h. Verwendung eines als Teil einer Ermittlung (z. B. mit einem Durchsuchungs- und Beschlagnahmebefehl) beschlagnahmten Geräts eines Verdächtigen oder eines Zeugen zum Zugriff auf Daten, auf die von dem Gerät (das die Cloud einschließen kann) aus zugegriffen werden kann. In den meisten Mitgliedstaaten ist den Behörden die Durchführung dieser Art von direktem Zugriff gestattet".
[31] Begründung, S. 6.
[32] Folgenabschätzung für den e-Beweismittel-Vorschlag, S. 11: „Nach nationalem Recht in mindestens 20 Mitgliedstaaten sind die Behörden vorbehaltlich richterlicher Genehmigung bevollmächtigt, ein Gerät sowie räumlich entfernt gespeicherte Daten, auf die von diesem Gerät aus zugegriffen werden kann, zu beschlagnahmen und zu durchsuchen oder Benutzerrechte für ein Konto zu benutzen, um auf Daten, die unter diesem Konto gespeichert sind, zuzugreifen und zu durchsuchen. Dieses Werkzeug wird stärker relevant, weil Daten jetzt üblicherweise nicht auf dem örtlichen Gerät, sondern auf Servern an einem anderen Ort gespeichert werden, der möglicherweise außerhalb des betreffenden Mitgliedstaats oder sogar außerhalb der EU liegt.
Den Strafverfolgungsbehörden ist der Ort dieser Daten oft nicht bekannt („loss of knowledge of location", d. h. der territoriale Speicherort ist unklar oder nicht bestimmbar) und kann praktisch nicht bestimmbar sein, wie etwa in Fällen, in denen Daten auf Darknet-Servern gehostet werden, die auf mehrschichtige IP-Relays zurückgreifen, um ihren Ort zu verschleiern. Daher kann die Bestimmung, ob derartige Durchsuchungen eine grenzüberschreitende Komponente haben, problematisch sein.
Mitgliedstaaten haben unterschiedliche Ansätze für den direkten Zugriff und den Ort der Datenspeicherung".
[33] Kommentar vom 5. Dezember 2013, abrufbar unter https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf
Die Artikel-29-Datenschutzgruppe wies auf die Risiken im Zusammenhang mit einem möglichen Zusatzprotokoll hin, durch das ein direkter Zugriff von Strafverfolgungsbehörden einer Vertragspartei auf Daten legitimisiert würde, die im Rechtsraum einer anderen Vertragspartei gespeichert sind. Die Artikel-29-Datenschutzgruppe betont, dass durch die Anwendung eines derartigen Grundsatzes, unabhängig von der Art der Durchführung dieser Anwendung (z. B. durch Anwendung des Rechts oder der Definitionen von Zustimmung der durchsuchenden Vertragspartei), wesentliche Datenschutzregeln verletzt würden und diese Anwendung „Grundrechte" von betroffenen Personen beeinträchtigen würde". Sie fügte hinzu: „Ein Zusatzprotokoll zu einem internationalen Übereinkommen, das den Zugriff auf Daten, die auf Computern im Ausland gespeichert sind, unter Anwendung des Rechts (oder der Definitionen von Zustimmung) der durchsuchenden Vertragspartei zu gestatten scheint, würde gegen den Besitzstand der EU im Bereich des Datenschutzes verstoßen." Sie betonte ferner, dass „grenzüberschreitende Datenübermittlungen im Bereich der Strafverfolgung pauschalen/grenzüberschreitenden Massenzugriff, Erhebung oder Übermittlung an/von Daten, was mit der Charta der Grundrechte der Europäischen Union und der Europäischen Menschenrechtskonvention unvereinbar ist, ausschließen muss."
[34] S. 6.
[35] Siehe EuGH-Rechtssache C-687/15, Europäische Kommission gegen Rat der Europäischen Union, ECLI:EU:C:2017:803, Rn. 48 ff.
[36] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 232.
[37] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 214.
[38] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 220 [nachträgliche Hervorhebung].
[39] Siehe Rechtssache C-518/07 Kommission / Deutschland, EU:C:2010:125, Rn. 25; Rechtssache C-614/10 Kommission / Österreich, EU:C:2012:631, Rn. 36 und 37; Rechtssache C-288/12 Kommission / Ungarn, EU:C:2014:237, Rn. 48; Rechtssache C-362/14 Maximilian Schrems / Data Protection Commissioner, ECLI:EU:C:2015:650, Rn. 41.
[40] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 230.
[41] Rechtssache C-362/14, Maximillian Schrems / Data Protection Commissioner, ECLI:EU:C:2015:650, Rn. 95.

[42] Rechtssache C-362/14, Maximillian Schrems / Data Protection Commissioner, ECLI:EU:C:2015:650, Rn. 95 [nachträgliche Hervorhebung].
[43] Rechtssache C-362/14, Maximillian Schrems / Data Protection Commissioner, ECLI:EU:C:2015:650, Rn. 56 bis 58.
[44] Rechtssache C-207/16, Ministerio fiscal, ECLI:EU:C:2018:788, Rn. 54, siehe auch Rn. 56.
[45] EuGH, Rechtssache C-207/16, Ministerio fiscal, ECLI:EU:C:2018:788, Rn. 62 [nachträgliche Hervorhebung].
[46] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger, ECLI:EU:C:2014:238, Rn. 39.
[47] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger, ECLI:EU:C:2014:238, Rn. 27.
[48] EuGH, verbundene Rechtssachen C-203/15 und C-698/15, Tele2 Sverige und Watson, ECLI:EU:C:2016:970, Rn. 99.
[49] Siehe Stellungnahme 23/2018 des Europäischen Datenschutzausschusses vom 26. September 2018 zu den Vorschlägen der Kommission über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (im Weiteren „EDSA-Stellungnahme 23/2018“), abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf, S. 12: „Tatsächlich erscheinen die vier vorgeschlagenen Kategorien nicht klar abgegrenzt, und die Definition von „Zugangsdaten“ bleibt im Vergleich zu den anderen Kategorien weiterhin unklar“.
[50] Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (Grundsatz der „Integrität und Vertraulichkeit“ nach Artikel 5 Absatz 1 Buchstabe f DSGVO und Artikel 4 Absatz 1 Buchstabe f der Richtlinie zum Datenschutz bei der Strafverfolgung). Die Verarbeitungssicherheit deckt insbesondere die Fähigkeit ab, die fortlaufende Vertraulichkeit und Integrität von Verarbeitungssystemen sicherzustellen.
[51] In dem Entwurf des Erläuternden Berichts, Absatz 2, S. 6, heißt es wie folgt: „[b]ei Notfällen, in denen das Leben oder die Sicherheit einer Person in großer und unmittelbarer Gefahr steht, geht es oft um Geiselnahmen, bei denen ein glaubhaftes Risiko besteht, dass das Opfer in unmittelbarer Todesgefahr schwebt oder ihm schwere Verletzungen oder anderer Schaden drohen, und der Verdächtige per E-Mail oder auf Sozialen Medien um Lösegeld verhandelt, so dass der Aufenthaltsort des Opfers durch beim Diensteanbieter gespeicherte Daten bestimmt werden kann, um den sexuellen Missbrauch eines Kindes durch Nachweis der Aufdeckung von zeitnah hergestellten Materialien über die sexuelle Ausbeutung von Kindern oder den sexuellen Missbrauch von Kindern oder anderen Missbrauchhinweisen, um Szenarien unmittelbar nach Terroranschlägen, in denen Behörden feststellen wollen, mit wem die Angreifer kommunizierten, um zu bestimmen, ob weitere Anschläge bevorstehen, und um Drohungen gegen die Sicherheit von kritischer Infrastruktur, bei denen das Leben oder die Sicherheit einer natürlichen Person in großer und unmittelbarer Gefahr schwebt“.
[52] https://rm.coe.int/t-cy-2018-23rev-protoprov-pub-text-v4/16808ff490
[53] Siehe Art. 29 WP Stellungnahme 4/2001 über den Entwurf des Europarats eines Übereinkommens über Computerkriminalität vom 22. März 2001 (5001/01/EN/ Final WP 41), S. 5 ff.
Siehe auch die von der Fachabteilung Bürgerrechte und konstitutionelle Angelegenheiten des Europäischen Parlaments in Auftrag gegebene Studie „Das Strafprozessrecht in den Ländern der Europäischen Union – Eine vergleichende Analyse ausgewählter Hauptunterschiede und ihrer Auswirkungen auf die Entwicklung des EU-Rechts“, PE 604.977, S. 30.
Siehe auch Agentur der Europäischen Union für Grundrechte, Gutachten zu dem Richtlinienentwurf über die Europäische Ermittlungsanordnung, 14. Februar 2011, S. 11: *„[ein] Verweigerungsgrund auf der Basis der Grundrechte könnte als angemessenes Werkzeug dafür dienen, während grenzüberschreitender Ermittlungen auftretende Grundrechtsverstöße zu verhindern. Gleichzeitig wäre es erforderlich, dass der Vollstreckungsstaat nicht nur mit den Strafrechtsbestimmungen und -verfahren des Anordnungsstaats, sondern auch mit den Einzelheiten der vorliegenden Sache vertraut ist. Eine vollumfängliche Grundrechtsbeurteilung für jeden Fall wäre somit nicht nur mit dem Konzept der gegenseitigen Anerkennung unvereinbar, sondern würde auch aufgrund komplexer und langwieriger Verfahren manche der in Abschnitt 2.2 festgelegten Grundrechtsnormen unterminieren. Aus diesem Grund sollte die Festlegung eines Verweigerungsgrunds auf der Basis der Grundrechte in der Richtlinie idealerweise durch explizite Parameter ergänzt werden. Durch derartige Parameter könnte der Verweigerungsgrund auf Umstände begrenzt werden, in denen ein EU-Mitgliedstaat begründeten Anlass zu der Befürchtung hat, dass die Vollstreckung einer EEA zu einer Verletzung der Grundrechte der betreffenden Person führen würde. Auf diese Weise könnte ein Verweigerungsgrund auf der Basis der Grundrechte als „Sicherheitsventil“ dienen, das die Einhaltung von sich aus EU-Primärrecht ergebenden Grundrechtsverpflichtungen durch die EU-Mitgliedstaaten erleichtert, ohne dass die Mitgliedstaaten von EU-Sekundärrecht abweichen müssen*“.

[54] 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/JHA des Rates, ABl. L 119 vom 4.5.2016, S. 89.

[55] Dies ist eine spezifische Ausnahme von Artikel 35 Absatz 1 Buchstabe b der Richtlinie zum Datenschutz bei der Strafverfolgung, dass personenbezogene Daten von Strafverfolgungsbehörden in den EU-Mitgliedstaaten an einen Verantwortlichen in einem Drittland oder eine internationale Organisation, die ebenfalls eine Strafverfolgungsbehörde ist, übermittelt werden.

[56] Die zusätzlichen Bedingungen sind wie folgt:
„1 (...) (a) die Übermittlung ist für die Ausübung einer Aufgabe der übermittelnden zuständigen Behörde gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten für die in Artikel 1 Absatz 1 genannten Zwecke unbedingt erforderlich;
(b) die übermittelnde zuständige Behörde stellt fest, dass im konkreten Fall keine Grundrechte und Grundfreiheiten der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen;
(c) die übermittelnde zuständige Behörde hält die Übermittlung an eine für die in Artikel 1 Absatz 1 genannten Zwecke zuständige Behörde in dem Drittland für wirkungslos oder ungeeignet, insbesondere weil die Übermittlung nicht rechtzeitig durchgeführt werden kann;
(d) die für die in Artikel 1 Absatz 1 genannten Zwecke zuständige Behörde in dem Drittland wird unverzüglich unterrichtet, es sei denn, dies ist wirkungslos oder ungeeignet;
(e) die übermittelnde zuständige Behörde teilt dem Empfänger den festgelegten Zweck oder die festgelegten Zwecke mit, für die die personenbezogenen Daten nur dann durch diesen verarbeitet werden dürfen, wenn eine derartige Verarbeitung erforderlich ist. (...)
3. Die übermittelnde zuständige Behörde unterrichtet die Aufsichtsbehörde über die Übermittlungen gemäß diesem Artikel.
4. Übermittlungen gemäß Absatz 1 werden dokumentiert“.

[57] Siehe EDSB, Stellungnahme 23/2018, S. 9.

[58] Bestandsdaten werden gemäß dem Übereinkommen in Artikel 18 Absatz 3 definiert: „alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Diensteanbieter über Teilnehmer seiner Dienste vorliegen, mit Ausnahme von Verkehrsdaten oder inhaltsbezogenen Daten, und durch die Folgendes festgestellt werden kann: (a) die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Maßnahmen und die Dauer des Dienstes; (b) die Identität des Teilnehmers, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen; (c) andere Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen“. Siehe auch der erläuternde Bericht des Übereinkommens über Computerkriminalität Absatz 177 ff.

[59] In Absatz l heißt es wie folgt: „Hinsichtlich der Bestimmungen über „internationale Herausgabeanordnungen“ sollte die Europäische Union nicht die Aufnahme von zusätzlichen Garantien und Verweigerungsgründen in das Zweite Zusatzprotokoll ablehnen, die über die Vorschläge der Kommission zu elektronischen Beweismitteln – einschließlich in ihrer durch die gesetzgebenden Organe im Rahmen des Gesetzgebungsverfahrens weiterentwickelten Form und schließlich in ihrer endgültigen (angenommenen) Form – hinausgehen, wie beispielsweise eine Mitteilung und Zustimmung des Staates des Diensteanbieters und eine vorherige Überprüfung durch ein Gericht oder eine unabhängige Verwaltungsstelle, sofern dies die Wirksamkeit des Rechtsinstruments nach dem Zweiten Zusatzprotokoll (beispielsweise in hinreichend begründeten Eilfällen) nicht unverhältnismäßig verringert. Zusätzliche Garantien und Verweigerungsgründe dürfen die Funktionsfähigkeit der Vorschläge der EU zu elektronischen Beweismitteln im Verhältnis der Mitgliedstaaten untereinander nicht beeinträchtigen“.

[60] Siehe EDSA, Stellungnahme 23/2018, S. 16.

[61] Siehe EDSA, Stellungnahme 23/2018, S. 17.

[62] Siehe Fußnote 34 der allgemeinen Ausrichtung des Rates: „*Die Tschechische Republik, Finnland, Deutschland, Griechenland, Ungarn und Lettland haben Vorbehalte zum Notifizierungsverfahren und plädieren für ein Verfahren von größerer Tragweite, das auch Transaktionsdaten einschließt, sowie für eine Grundrechteklausel, d. h. für die Nennung von Gründen, wenn eine notifizierte Behörde abgewiesen wird; außerdem sollte die Bestimmung, in der dargelegt wird, was als "nationaler Fall" gilt, rückgängig gemacht werden; und schließlich sollte aus Sicht Deutschlands nicht das Zertifikat, sondern die Anordnung selbst übermittelt werden, während die Tschechische Republik die Ansicht vertritt, dass beide – Anordnung und Zertifikat – übermittelt werden sollten*“.

[63] Siehe die Liste der unter Artikel 14 des e-Beweismittel-Vorschlags genannten Ablehnungsgründe sowie die Rechtsprechung des EuGH im Zusammenhang mit dem Europäischen Haftbefehl (EuGH, Rechtssache C-404/15, Pál Aranyosi und Robert Căldăraru / Generalstaatsanwaltschaft Bremen, ECLI:EU:C:2016:198, Rn. 82 ff.).

[64] Siehe Artikel 6 EUV und Artikel 67 Absatz 1 AEUV. Siehe auch Agentur der Europäischen Union für Grundrechte, Gutachten zu dem Richtlinienentwurf über die Europäische Ermittlungsanordnung, 14. Februar 2011, Fußnote 56: „*[i]n diesem Zusammenhang sollte an den Grundsatz der extraterritorialen Haftung unter der EMRK erinnert werden. Gemäß der EMRK haften EU-Mitgliedstaaten für in einem anderen Staatsgebiet begangene Verstöße gegen die Menschenrechte, wenn jemand aufgrund ihrer Handlungen in diese Lage gebracht wurde; siehe EGMR, Soering / Vereinigtes Königreich, Nr. 14038/88, 7. Juli 1989. Siehe auch EGMR, Bosphorus / Irland, Nr. 45036/98, 30. Juni 2005, Rn. 156 „wird davon ausgegangen, dass ein Staat nicht von den Erfordernissen der Konvention abgewichen ist, wenn er nicht mehr tut, als rechtliche Verpflichtungen aus seiner Mitgliedschaft in der [EU] umzusetzen." Diese Annahme galt als zurückweisbar*".

[65] Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen, ABl. L 130 vom 1.5.2014, S. 1.

[66] Siehe Agentur der Europäischen Union für Grundrechte, Gutachten zu dem Richtlinienentwurf über die Europäische Ermittlungsanordnung, 14. Februar 2011, Fußnote 61, Verweis auf EGMR-Sache, MSS / Belgien und Griechenland, Nr. 30696/09, 21. Januar 2011.

[67] Siehe Erwägungsgrund 6 der Empfehlung.

[68] See EDSA, Stellungnahme 23/2018, S. 17, in der der EDSA empfiehlt, dass der e-Beweismittel-Vorschlag „*zumindest die klassische Mindestabweichung vorsehen sollte, wonach beim Vorliegen substanzieller Gründe für die Annahme, dass die Vollstreckung einer Verordnung zu einer Verletzung eines Grundrechts der betreffenden Person führen würde und dass der Vollstreckungsstaat seine Verpflichtungen zum Schutz der in der Charta anerkannten Grundrechte missachten würde, die Vollstreckung der Verordnung verweigert werden sollte*".