EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

20. Januar 2022

Stellungnahme 1/2022

zu zwei Vorschlägen für Beschlüsse des Rates zur Ermächtigung der Mitgliedstaaten, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials zu unterzeichnen und zu ratifizieren

edps.europa.eu

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 Wiewiorówski 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 sicherzustellen, dass Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union sowie Artikel 16 AEUV eingehalten werden.

Zusammenfassung

Am 25. November 2021 nahm die Kommission, gestützt auf Artikel 16, Artikel 82 Absatz 1 und Artikel 218 Absätze 5 und 6 des Vertrags über die Arbeitsweise der Europäischen Union zwei Vorschläge für Beschlüsse des Rates an, die die Mitgliedstaaten ermächtigen, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität zu unterzeichnen bzw. zu ratifizieren. Der Anhang der Vorschläge enthält jeweils die Direktiven des Rates für Vorbehalte, Erklärungen und Mitteilungen bei der Unterzeichnung und Ratifizierung des Protokolls.

Die Untersuchung und Verfolgung von Straftaten ist ein legitimes politisches Ziel, und die internationale Zusammenarbeit einschließlich des Austauschs von Informationen ist heute wichtiger denn je. Der EDSB ist schon lange der Ansicht, 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 in Einklang stehen. Selbst bei Ermittlungen in Inlandsfällen sind Strafverfolgungsbehörden immer häufiger mit „grenzüberschreitenden Situationen“ konfrontiert, weil Informationen elektronisch in Drittländern gespeichert werden. Bestehende Kooperationsmodelle wie Rechtshilfeabkommen geraten an ihre Grenzen, zum einen, weil die Zahl der Ersuchen steigt, zum anderen wegen der Volatilität digitaler Informationen. Der EDSB versteht, dass die Behörden bei der Dateneinholung für ihre Ermittlungen unter hohem zeitlichen Druck stehen, und er unterstützt die Bemühungen um die Entwicklung neuer Modelle für die Zusammenarbeit, auch für die Zusammenarbeit mit Drittländern.

Das Protokoll zielt darauf ab, die traditionellen Wege der Zusammenarbeit zu verbessern, unter anderem durch Bestimmungen, die die direkte Zusammenarbeit zwischen Strafverfolgungsbehörden und Dienstleistern im grenzüberschreitenden Kontext verbessern sollen. Insbesondere würde das Protokoll die Zusammenarbeit im Bereich der Computerkriminalität und bei der Sammlung von Beweismitteln in elektronischer Form für strafrechtliche Ermittlungen oder Verfahren verstärken.

Der EDSB erkennt an, dass es nicht möglich ist, die Terminologie und Definitionen des Unionsrechts in einer multilateralen internationalen Übereinkunft vollständig zu replizieren, betont jedoch, dass der Schutz des Einzelnen eindeutig und wirksam garantiert sein muss, um dem Unionsrecht vollumfänglich zu genügen.

Die Datenschutzgrundsätze, die die Verarbeitung nach Treu und Glauben, Richtigkeit und Relevanz der Informationen, unabhängige Aufsicht und Individualrechte natürlicher Personen umfassen, sind für öffentlich-rechtliche Stellen genauso relevant wie für privatrechtliche Organisationen. Diese Grundsätze sind umso wichtiger, wenn man die Sensibilität der für strafrechtliche Ermittlungen erforderlichen Daten bedenkt.

Diese Stellungnahme will eine objektive Analyse vornehmen und den Organen der Union jetzt, da der Rat die Vorschläge der Kommission zur Unterzeichnung und Ratifizierung des Protokolls prüft, und noch bevor das Europäische Parlament aufgerufen ist, seine Zustimmung zum Abschluss dieses Protokolls zu erteilen, konstruktiven Rat erteilen.

Der EDSB begrüßt, dass die endgültige Fassung des Protokolls keine Bestimmung über den direkten Datenzugang für Strafverfolgungsbehörden enthält. Er begrüßt auch, dass das Protokoll einen eigenen Artikel über den Schutz personenbezogener Daten enthält. Des Weiteren nimmt der EDSB die zahlreichen Garantien, die in das Protokoll aufgenommen wurden, positiv zur Kenntnis.

Der EDSB versteht es so, dass bestätigt ist, dass das Rahmenabkommen zwischen der EU und den USA auf Übermittlungen aus der EU in die Vereinigten Staaten von Amerika, die im Rahmen der im Protokoll enthaltenen Vorschriften über die behördliche Zusammenarbeit erfolgen, Anwendung fände. Der EDSB bedauert dieses Ergebnis.

Für den Fall, dass ein Beschluss des Rates angenommen werden sollte, der die Mitgliedstaaten ermächtigt, das Protokoll im Interesse der Union zu unterzeichnen und zu ratifizieren, begrüßt der EDSB die Vorschläge der Kommission, dass die Mitgliedstaaten im Interesse der Union die Erklärung, Notifikation und Mitteilung gemäß Artikel 7 Absätze 2 Buchstabe b sowie Artikel 5 Buchstaben a und e des Protokolls abgeben. Die Vorschläge stellen sicher, dass Diensteanbieter in der Union nur dann um die Übermittlung personenbezogener Daten ersucht werden können, wenn das Ersuchen auf einer Anordnung beruht, die im ersuchenden Drittland, das Vertragspartei des Protokolls ist, durch eine Staatsanwältin beziehungsweise durch einen Staatsanwalt oder eine andere Justizbehörde oder unter staatsanwaltlicher Aufsicht oder unter Aufsicht einer anderen Justizbehörde oder anderweitig unter unabhängiger Aufsicht erlassen wurde.

Der EDSB hält es auch für positiv, dass den Mitgliedstaaten vorgeschlagen wird, die Erklärung gemäß Artikel 8 Absatz 4 des Protokolls (über die Zusammenarbeit zuständiger Behörden zur Erfüllung von Herausgabeanordnungen in Bezug auf Bestandsdaten und Verkehrsdaten) abzugeben, um sicherzustellen, dass für die Erfüllung auf Grundlage dieser Vorschrift ergangener Anordnungen zusätzliche begleitende Angaben verlangt werden.

Darüber hinaus gibt der EDSB für den Fall, dass das Protokoll von den Mitgliedstaaten im Interesse der Union unterzeichnet und ratifiziert werden sollte, folgende Empfehlungen für künftige Beschlüsse des Rates:

- Gewisse Daten, die unter die Kategorie „Bestandsdaten“ im Sinne des Übereinkommens über Computerkriminalität fallen, gelten nach Unionsrecht unter Umständen als Verkehrsdaten, deren Übermittlung einen schweren Eingriff in die Grundrechte des Betroffenen darstellt, weshalb der Zugang zu diesen Daten nur zur Bekämpfung von schwerer Kriminalität gerechtfertigt sein kann. Der EDSB empfiehlt den Mitgliedstaaten deshalb, sich – entgegen dem Vorschlag der Kommission – das Recht auf Nichtanwendung von Artikel 7 des Protokolls vorzubehalten, da Artikel 7 Absatz 9 Buchstabe b für bestimmte Arten von Zugangsnummern die direkte Weitergabe von Bestandsdaten von Diensteanbietern an zuständige Behörden eines anderen Landes vorsieht.

- Die Mitgliedstaaten sollten gemäß Artikel 7 Absatz 5 Buchstabe e des Protokolls eine Justiz- oder sonstige unabhängige Behörde bestimmen.

- Die vorgeschlagene Mitteilung, die die Mitgliedstaaten bei Unterzeichnung oder bei Hinterlegung der Ratifikations-, Annahme- oder Genehmigungsurkunde an die Behörden der Vereinigten Staaten bezüglich des Rahmenabkommens zwischen der EU und den USA übermitteln, sollte klarer formuliert werden.

- Die vorgeschlagene Erwägung in Bezug auf sonstige Vereinbarungen oder Verträge gemäß Artikel 14 Absatz 1 Buchstabe c des Protokolls, die die Datenschutzbestimmung des Protokolls (Artikel 14) ersetzen könnten, sollte abgeändert werden.

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 (EG) Nr. 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 Union, zum freien Datenverkehr[2], insbesondere auf 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. Im Juni 2017 genehmigte der Ausschuss für das Übereinkommen über Computerkriminalität des Europarats das Mandat für die Ausarbeitung des Zweiten Zusatzprotokolls im Zeitraum September 2017 bis Dezember 2019[4].

2. Am 5. Februar 2019 nahm die Kommission eine Empfehlung[5] für einen Beschluss des Rates an, mit dem die Kommission ermächtigt wird, im Namen der Europäischen Union an den Verhandlungen über ein Zweites Zusatzprotokoll (im Folgenden „Protokoll")[6] zum Übereinkommen des Europarats über Computerkriminalität über eine verstärkte internationale Zusammenarbeit und elektronisches Beweismaterial (im Folgenden „Übereinkommen über Computerkriminalität") teilzunehmen (SEV Nr. 185)[7].

3. Am 2. April 2019 nahm der Europäische Datenschutzbeauftragte (im Folgenden „EDSB") eine Stellungnahme zu der Empfehlung[8] an. Mit Beschluss vom 6. Juni 2019 ermächtigte der Rat der Europäischen Union die Kommission, im Namen der Europäischen Union an den Verhandlungen über das Protokoll teilzunehmen[9].

4. Der Ausschuss für das Übereinkommen über Computerkriminalität verlängerte das Mandat zweimal, zunächst bis Dezember 2020 und später bis Mai 2021. Das Protokoll wurde im Zeitraum September 2017 bis Mai 2021 vom Ausschuss für das Übereinkommen über Computerkriminalität erstellt. In diesem Zeitraum fanden neunzig Sitzungen des Redaktionsplenums des Ausschusses für das Übereinkommen über Computerkriminalität, des

Redaktionsausschusses und der Untergruppen sowie sechs Konsultationen der Interessenträger statt.

5. Der Europäische Datenschutzausschuss leistete am 13. November 2019, 2. Februar 2021 und 4. Mai 2021 Beiträge zu den öffentlichen Konsultationen zum Entwurf des Protokolls[10].

6. Das Europäische Parlament wies 2021 in seiner Entschließung zu der Cybersicherheitsstrategie der EU für die digitale Dekade darauf hin, dass die Arbeit am Protokoll abgeschlossen werden muss[11].

7. Am 17. November 2021 wurde das Protokoll vom Ministerkomitee des Europarats angenommen. Es soll im Mai 2022 zur Unterzeichnung aufgelegt werden. Änderungen des Protokolls können deshalb nur von einer Vertragspartei des Protokolls vorgeschlagen und vom Ministerkomitee angenommen werden. Nach dem Protokoll treten Änderungen nur in Kraft, wenn sie von sämtlichen Vertragsparteien angenommen werden[12].

8. Die Europäische Union kann nicht Vertragspartei des Protokolls werden, da sowohl das Protokoll als auch das Übereinkommen über Computerkriminalität nur Staaten offensteht[13].

9. Am 25. November 2021 nahm die Kommission auf Grundlage von Artikel 16, Artikel 82 Absatz 1 und Artikel 218 Absätze 5 und 6 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) zwei Vorschläge für Beschlüsse des Rates an[14]

10. Laut den Vorschlägen[15] gehören die Bestimmungen des Protokolls zu einem Bereich, der weitgehend Gegenstand gemeinsamer Vorschriften im Sinne von Artikel 3 Absatz 2 AEUV ist. Mit diesen Vorschlägen will die Kommission zwei Beschlüsse des Rates erwirken, mit denen die Mitgliedstaaten ermächtigt werden, das Protokoll im Interesse der Europäischen Union zu unterzeichnen bzw. zu ratifizieren. Beiden Vorschlägen ist jeweils ein Anhang (im Folgenden „Anhang“) beigefügt, der an die Mitgliedstaaten gerichtete Anweisungen enthält hinsichtlich der Vorbehalte, Erklärungen, Notifikationen oder Mitteilungen und sonstigen Erwägungen, die bei der Unterzeichnung und Ratifizierung des Protokolls im Interesse der Europäischen Union vorzulegen sind. Dem Vorschlag bezüglich der Ratifizierung ist auch der Text des Protokolls im Anhang beigefügt.

11. Damit die Vereinbarung, falls der Rat die Mitgliedstaaten zu deren Unterzeichnung im Interesse der Union zu ermächtigen beschließt, abgeschlossen werden kann, sollte der Rat einen Beschluss annehmen, der die Mitgliedstaaten ermächtigt, die Vereinbarung im Interesse der Union zu ratifizieren, nachdem die Zustimmung des Europäischen Parlaments eingeholt wurde. Das Protokoll tritt am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag folgt, an dem fünf Vertragsparteien des Übereinkommens nach Artikel 16 Absätze 1 und 2 ihre Zustimmung ausgedrückt haben, durch dieses Protokoll gebunden zu sein[16].

12. Der EDSB ist nach der Annahme der beiden Vorschläge von der Europäischen Kommission gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 konsultiert worden. Auf diese Stellungnahme wird in den Erwägungsgründen 12 und 13 der Vorschläge bezüglich der Ratifizierung bzw. Unterzeichnung des Protokolls Bezug genommen. Der EDSB wünscht hervorzuheben, dass die vorliegende Stellungnahme unbeschadet etwaiger zusätzlicher Anmerkungen ergeht, die der EDSB auf der Grundlage weiterer, künftig verfügbarer Informationen abgeben kann.

2. Ziele des zweiten Zusatzprotokolls

13. Das Übereinkommen über Computerkriminalität steht Mitgliedern des Europarats wie auch Nicht-Mitgliedern (auf Einladung) offen. Derzeit sind 66 Länder Vertragsparteien des Übereinkommens, darunter 26 Mitgliedstaaten der Europäischen Union (im Folgenden „Mitgliedstaaten“)[17] und andere Drittländer-Mitgliedstaaten des Europarats wie Armenien, Aserbaidschan, und die Türkei sowie Nicht-Mitglieder des Europarats wie Australien, Kanada, Ghana, Israel, Japan, Marokko, Paraguay, die Philippinen, Senegal, Sri Lanka, Tonga und die USA[18].

14. Das Übereinkommen über Computerkriminalität ist eine verbindliche internationale Übereinkunft, mit der sich die Vertragsparteien 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. Das Übereinkommen enthält Mindestanforderungen an die in Ermittlungsverfahren zur Verfügung stehenden Ermittlungsbefugnisse und fördert die internationale Zusammenarbeit zwischen den Vertragsparteien. Insbesondere in seinem Kapitel III über internationale Zusammenarbeit[19] enthält es allgemeine Bestimmungen über die internationale Zusammenarbeit, die auch in anderen Verträgen über die Zusammenarbeit in Strafsachen zu finden sind, sowie spezifische Bestimmungen zur Erhebung von Beweismaterial in elektronischer Form.

15. Das Protokoll zielt darauf ab, zusätzliche Instrumente vorzusehen, unter anderem für die Zusammenarbeit in Notfällen; darauf wird weiter unten genauer eingegangen. Dem Protokoll ist ein erläuternder Bericht[20] beigefügt, aus dem das Verständnis der Verfasser hervorgeht. Der erläuternde Bericht stellt kein Instrument dar, das eine verbindliche Auslegung des Protokolls bietet, sondern soll die Vertragsparteien bei der Anwendung des Protokolls „anleiten und unterstützen“[21].

16. Das Protokoll umfasst:

- Bestimmungen zur **Gestattung der direkten Zusammenarbeit zwischen zuständigen Behörden** in einer Vertragspartei auf der einen Seite, und **Stellen, die Domänennamenregistrierungsdienste erbringen, oder Diensteanbietern** in einer anderen Vertragspartei auf der anderen Seite, in Bezug auf die Weitergabe von **Domainnamenregistrierungsdaten oder Bestandsdaten**[22] (Artikel 6 und 7).

- Bestimmungen zur **Verstärkung der internationalen Zusammenarbeit zwischen Behörden**:

  - Durchführung von **Anordnungen einer anderen Vertragspartei auf umgehende Herausgabe von Bestandsdaten und Verkehrsdaten**[23] (Artikel 8);

  - **nicht rechtlich bindende Ersuchen** um **umgehende Weitergabe gespeicherter Computerdaten**[24] **im Notfall** (Artikel 9);

  - **Rechtshilfe in Notfällen** (Artikel 10[25]);

  - Videokonferenzen (Artikel 11)

- Gemeinsame Ermittlungsgruppen und gemeinsame Ermittlungen (Artikel 12);

- **Garantien** (Artikel 13 und 14), **einschließlich Datenschutzanforderungen**. Bestandteil der spezifischen Kooperationsmaßnahmen sind auch spezifische Bedingungen und Garantien.

17. Ersuchen um Registrierungsinformationen zu Domänennamen (Artikel 6) im Rahmen der direkten Zusammenarbeit wie auch Ersuchen um umgehende Weitergabe gespeicherter Computerdaten im Notfall (Artikel 9) sind *nicht rechtlich bindende* Ersuchen[26].

18. Das Protokoll sieht die **Möglichkeit vor, dass sich eine Vertragspartei *das Recht auf Nichtanwendung vorbehält***, und zwar in Bezug auf:

    – Artikel 7 (direkte Zusammenarbeit bei der Weitergabe von Bestandsdaten), diesen Artikel insgesamt nicht anzuwenden, oder, falls die Weitergabe bestimmter Arten von Zugangsnummern nach diesem Artikel mit den Grundprinzipien der innerstaatlichen Rechtsordnung unvereinbar sein sollte, diesen Artikel nicht auf solche Nummern anzuwenden (Artikel 7 Absatz 9)[27].

    – Artikel 8 (Verstärkung der internationalen Zusammenarbeit zwischen Behörden zur Durchführung von Anordnungen einer anderen Vertragspartei auf umgehende Herausgabe von Bestandsdaten und Verkehrsdaten) in Bezug auf Verkehrsdaten (Artikel 8 Absatz 13)[28].

19. Im Protokoll vorgesehen ist auch die **Möglichkeit, dass eine Vertragspartei *gewisse Erklärungen abgeben kann***, unter anderem folgende Erklärungen:

    – zu Artikel 7 (direkte Zusammenarbeit bezüglich der Weitergabe von Bestandsdaten), eine Erklärung, die der ersuchten Vertragspartei gestattet, wenn eine Anordnung gegen einen Diensteanbieter in ihrem Hoheitsgebiet erlassen wird, zu verlangen:

        o dass die Anordnung durch eine Staatsanwältin beziehungsweise durch einen Staatsanwalt oder eine andere Justizbehörde oder unter staatsanwaltlicher Aufsicht oder unter Aufsicht einer anderen Justizbehörde oder anderweitig unter unabhängiger Aufsicht erlassen werden muss (Absatz 2 Buchstabe b);

        o dass, wenn eine Anordnung nach Absatz 1 an einen Diensteanbieter in ihrem Hoheitsgebiet gerichtet wird, zeitgleich die Benachrichtigung über die Anordnung, die ergänzenden Angaben und eine Zusammenfassung des mit den Ermittlungen oder dem Verfahren in Zusammenhang stehenden Sachverhalts an eine Behörde erfolgt, die den Diensteanbieter anweisen kann, die Bestandsdaten nicht weiterzugeben, falls bestimmte Bedingungen oder Ablehnungsgründe gegeben sind (Absatz 5 Buchstaben a und e);

    – zu Artikel 8 (Umgehende Herausgabe von Bestandsdaten und Verkehrsdaten), wonach die ersuchte Vertragspartei erklären kann, dass für die Erfüllung einer Anordnung zusätzliche begleitende Angaben erforderlich sind (Absatz 4).

20. In den Vorschlägen für die Beschlüsse des Rates schlägt die Kommission vor, die Mitgliedstaaten zu ermächtigen, das Protokoll im Interesse der Europäischen Union gemeinsam zu unterzeichnen und zu ratifizieren, und zwar mit einigen Vorbehalten und Erklärungen. Insbesondere **werden die Mitgliedstaaten angewiesen, davon abzusehen, sich das Recht, Artikel 7 nicht anzuwenden, vorzubehalten,** und zwar sowohl, was die volle Nichtanwendung angeht, als auch was die Nichtanwendung in Bezug auf bestimmte Arten von Zugangsnummern angeht[29]; außerdem werden sie aufgefordert, davon abzusehen, sich das Recht vorzubehalten, Artikel 8 (Durchführung von Anordnungen einer anderen

Vertragspartei) nach Artikel 8 Absatz 13 nicht auf Verkehrsdaten anzuwenden. Der vorgeschlagene Beschluss des Rates **weist die Mitgliedstaaten jedoch an, von den vorgenannten Erklärungen zu den Artikeln 7 und 8 Gebrauch zu machen, damit die darin enthaltenen zusätzlichen Garantien Anwendung finden**[30].

3. Allgemeine Anmerkungen

21. Der EDSB versteht, dass die Behörden bei der Dateneinholung für ihre Ermittlungen unter hohem zeitlichen Druck stehen, und er unterstützt die Bemühungen um die Entwicklung neuer Modelle für die Zusammenarbeit, auch für die Zusammenarbeit mit Drittländern. Diesbezüglich erinnert er daran, dass er gemeinsam mit dem EDSA dazu aufgerufen hat, eine neue Generation von Rechtshilfeabkommen abzuschließen, die in der Praxis eine schnellere und sicherere Bearbeitung der Ersuchen ermöglichen[31].

22. Die von der Union geschlossenen internationalen Übereinkünfte „*binden die Organe der Union und die Mitgliedstaaten*", wie in Artikel 216 Absatz 2 AEUV eindeutig geregelt ist. Darüber hinaus bilden internationale Übereinkünfte gemäß der ständigen Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) ab ihrem Inkrafttreten „*einen integrierenden Bestandteil der Gemeinschaftsrechtsordnung*"[32] und haben Vorrang vor den Bestimmungen des abgeleiteten Unionsrechts[33].

23. Im Hinblick darauf, dass das Übereinkommen über Computerkriminalität, wie auch seine Zusatzprotokolle bindende internationale Übereinkünfte sind, 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*"[34]. Es ist daher unerlässlich, sicherzustellen, dass die sich aus dem Protokoll ergebenden Verpflichtungen diese Grundsätze, was den Datenschutz angeht, nicht beeinträchtigen würden.

24. Nach dem Protokoll, dessen Unterzeichnung und Ratifizierung die Kommission vorschlägt, wäre es u. a. gestattet, dass personenbezogene Daten von zuständigen Behörden[35] oder auch von Stellen des Privatsektors in den Mitgliedstaaten[36] übermittelt und diese Daten dann von Behörden eines Drittlands, das Vertragspartei des Protokolls ist, oder auch von Stellen des Privatsektors in dem betreffenden Land verarbeitet würden.

25. Dazu heißt es jeweils im achten Erwägungsgrund der beiden Vorschläge: „*Da das Protokoll geeignete Garantien vorsieht, die den Anforderungen für internationale Übermittlungen personenbezogener Daten nach der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 entsprechen, wird sein Inkrafttreten zur weltweiten Verbreitung der Datenschutzstandards der Union beitragen, den Datenverkehr zwischen den Vertragsparteien des Protokolls, die EU-Mitgliedstaaten sind, und denen, die keine EU-Mitgliedstaaten sind, erleichtern, und die Erfüllung der Verpflichtungen der EU-Mitgliedstaaten aus den Datenschutzvorschriften der Union gewährleisten.*"

3.1. Zur Verarbeitung aufgrund des Protokolls empfangener personenbezogener Daten durch eine Behörde eines Mitgliedstaats oder eine Stelle des Privatsektors[37]

26. Artikel 14 des Protokolls betrifft den Schutz personenbezogener Daten. In Absatz 1 Buchstabe e dieser Bestimmung heißt es, dass „*[d]ieser Artikel ... eine Vertragspartei nicht daran [hindert], auf die Verarbeitung von nach diesem Protokoll empfangenen personenbezogenen Daten durch ihre eigenen Behörden strengere Garantien anzuwenden*". Es wäre den Mitgliedstaaten daher gestattet, vorzusehen, dass für die Verarbeitung personenbezogener Daten, sei es durch ihre Behörden oder durch eine Stelle des Privatsektors in ihrem Hoheitsgebiet, eigene strengere Garantien gelten.

3.2. Zu den Übermittlungen an Drittländer-Vertragsparteien des Protokolls

27. Der EDSB stellt fest, dass es nach den Artikeln 6 und 7 des Protokolls möglich ist, dass personenbezogene Daten von Stellen des Privatsektors übermittelt werden, sofern dies einem Strafverfolgungsziel dient, wobei dieses Ziel ein anderes ist als das, für das die Daten erhoben wurden.

28. Vorab merkt der EDSB an, dass jeder Eingriff in die Grundrechte – die in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta") garantierten Grundrechte auf die Achtung des Privat- und Familienlebens und den Schutz personenbezogener Daten – den in Artikel 52 Absatz 1 der Charta genannten Anforderungen genügen muss.

29. Übermittlungen von einer Strafverfolgungsbehörde an einen Diensteanbieter oder eine Stelle, die in einer anderen Vertragspartei Domänennamenregistrierungsdienste erbringt, müssen den in der Richtlinie (EU) 2016/680 (Strafverfolgungsrichtlinie) niedergelegten Datenschutzgrundsätzen genügen, insbesondere den in Kapitel V der Richtlinie genannten, damit sichergestellt ist, dass das Schutzniveau, das das Unionsrecht natürlichen Personen bietet, nicht untergraben wird[38]

30. Gemäß Artikel 44 der Verordnung (EU) 2016/679 („DSGVO")[39] ist zu prüfen, ob das Protokoll sicherstellt, dass Übermittlungen durch Stellen des Privatsektors, die im Zusammenhang mit den Artikeln 6 und 7 des Protokolls erfolgen, so stattfinden können, dass die in Kapitel V der DSGVO genannten Bedingungen und die sonstigen Bestimmungen der Verordnung (siehe Abschnitt 4) erfüllt sind.

31. Hinsichtlich der Übermittlung von Daten, die für ein Urteil oder eine Entscheidung einer Behörde in einem Drittland gebraucht werden, durch Stellen des Privatsektors in der EU, ergibt sich aus Artikel 48 DSGVO, dass solche Urteile oder Entscheidungen „*unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel jedenfalls nur dann anerkannt oder vollstreckbar werden [dürfen], wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind*".

32. Im Juli 2017 legte der EuGH das Gutachten 1/15[40] über ein geplantes Abkommen zwischen der EU und Kanada über die Übermittlung von Fluggastdatensätzen („PNR-Daten") nach Kanada vor, in dem die Bedingungen festgelegt werden, unter denen ein internationales Abkommen eine Rechtsgrundlage für die Übermittlung personenbezogener Daten im Sinne der Richtlinie 95/46/EG (inzwischen durch die DSGVO ersetzt) bilden kann. Der EuGH hat entschieden, *„dass eine Weitergabe personenbezogener Daten aus der Union in ein Drittland nur zulässig ist, wenn*

das Drittland ein Schutzniveau der Grundfreiheiten und Grundrechte gewährleistet, das dem in der Union garantierten Niveau der Sache nach gleichwertig ist"[41]. **Aus dem Gutachten 1/15 folgt also, dass das Schutzniveau, das sich aus dem Protokoll über den Austausch personenbezogener Daten mit Drittländern ergibt, der Sache nach dem Schutzniveau im Unionsrecht gleichwertig sein muss.** Diesbezüglich weist der EDSB darauf hin, dass gemäß der Rechtsprechung des EuGH sowohl Artikel 7 als auch Artikel 8 der Charta in Verbindung mit **dem Recht auf einen wirksamen Rechtsbehelf gemäß Artikel 47 der Charta** zu beurteilen sind[42].

33. Was die Rechtsgrundlage angeht, so bilden gemäß Artikel 6 des Protokolls gestellte Ersuchen um Registrierungsinformationen zu Domänennamen die Grundlage für eine freiwillige Zusammenarbeit, weshalb sie gemäß dem Protokoll für die ersuchte Stelle nicht bindend sind. Nach dem Protokoll bleibt es den Vertragsparteien überlassen, die Form der Durchführung festzulegen[43]. In Bezug auf Anordnungen gemäß Artikel 7 schreibt das Protokoll vor, dass die Vertragsparteien die gesetzgeberischen und anderen Maßnahmen treffen, die erforderlich sind, damit Diensteanbieter in ihrem Hoheitsgebiet einer Anordnung, die von einer zuständigen Behörde in einer anderen Vertragspartei erlassen wurde, Folge leisten. Im erläuternden Bericht heißt es dazu, dass „*[d]ie Form der Durchführung von den jeweiligen rechtlichen und politischen Erwägungen der Vertragsparteien abhängt*"[44].

34. Laut dem erläuternden Bericht würde dies für Mitgliedstaaten bedeuten, „*eine klare Grundlage für die Verarbeitung personenbezogener Daten anzugeben. Wegen der zusätzlichen Anforderungen an die Bewilligung, die nach den Datenschutzgesetzen zu beachten sind, wenn ggf. im Zuge der Beantwortung Bestandsdaten international übermittelt werden, berücksichtigt das Protokoll das wichtige öffentliche Interesse an dieser Maßnahme der direkten Zusammenarbeit und sieht in Artikel 14 diesbezügliche Garantien vor*". Die DSGVO bietet einige Rechtsgrundlagen, die in solche Fällen in Betracht kommen[45], und das Protokoll hindert nicht daran, im innerstaatlichen Recht weitere Rechtsgrundlagen für Übermittlungen vorzusehen, sofern die im Protokoll vorgesehene Zusammenarbeit noch möglich bleibt[46].

4. Zu den Garantien in Bezug auf internationale Datenübermittlungen und die Achtung der Grundrechte

4.1. Status des Protokolls in Bezug auf den Datenschutz

35. Während alle Mitgliedstaaten Vertragsparteien des Übereinkommens Nr. 108[47] des Europarats sind, das für den Bereich der Strafverfolgung gilt, sind nicht alle Drittländer-Vertragsparteien des Übereinkommens über Computerkriminalität auch Vertragsparteien des Übereinkommens Nr. 108[48]; nur für eine Minderheit gibt es einen Angemessenheitsbeschluss im Sinne der DSGVO[49], und nur für eines (das Vereinigte Königreich) gibt es einen Angemessenheitsbeschluss im Sinne der Strafverfolgungsrichtlinie.

36. In Anbetracht des Strafverfolgungskontexts und der potenziellen Risiken, die solche Datenübermittlungen für betroffene Personen bedeuten können, sollten die Garantien, die in diesem Protokoll mit Drittländern vorgesehen sind, diesen Risiken auf zufriedenstellende Weise entgegenwirken und sie mindern.

37. **Artikel 14** des Protokolls über den Schutz personenbezogener Daten bietet Garantien **für aufgrund des Protokolls empfangene Daten**, auch für Daten, die Teil von auf das Protokoll gestützten Anordnungen oder Ersuchen sind, um „*den Vertragsparteien zu ermöglichen, die [Datenschutz-] Anforderungen zu erfüllen*“, wenn personenbezogene Daten für die Zwecke des Protokolls übermittelt werden[50]. Dazu merkt der EDSB positiv an, dass der Begriff der personenbezogenen Daten, so wie er in Artikel 3 des Protokolls definiert ist, mit dem Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 223) (Übereinkommen Nr. 108+) und dem Unionsrecht in Einklang steht.

38. Es wäre Sache der Strafverfolgungsbehörden der Mitgliedstaaten, die Verhältnismäßigkeit ihrer aufgrund des Protokolls erlassenen Ersuchen oder Anordnungen zu überprüfen[51]. Gleichermaßen wäre es Sache dieser Behörden, zu prüfen, ob ihre Ersuchen oder Anordnungen bezüglich der Herausgabe personenbezogener Daten an eine Drittland-Vertragspartei des Protokolls den unionsrechtlichen Anforderungen genügen, bevor sie das Ersuchen oder die Anordnung absenden.

39. Nach Artikel 14 Absatz 1 Buchstabe d geht „[j]ede Vertragspartei ... davon aus, dass die Verarbeitung personenbezogener Daten nach [Artikel 14 Absätze 2 bis 15] die Anforderungen ihres Rechtsrahmens im Bereich des Schutzes personenbezogener Daten **für internationale Übermittlungen personenbezogener Daten** erfüllt; einer weiteren Genehmigung der Übermittlung nach diesem Rechtsrahmen bedarf es nicht. *Eine Vertragspartei darf die Übermittlung von Daten an eine andere Vertragspartei nach diesem Protokoll nur dann aus Gründen des Datenschutzes unter den in Absatz 15 festgelegten Bedingungen ablehnen oder untersagen ...*“[52].

40. Dies bedeutet, dass Mitgliedstaaten, wenn sie Vertragspartei des Protokolls sind, anerkennen, dass das Protokoll angemessene Schutzvorkehrungen für die Übermittlung personenbezogener Daten bietet. Es muss deshalb geprüft werden, ob für Übermittlungen, die von Strafverfolgungsbehörden oder Stellen des Privatsektors in einem Mitgliedstaat vorgenommen werden, im Kontext dieses Protokolls geeignete Garantien vorgesehen sind.

41. Diesbezüglich versteht der EDSB Artikel 14 Absatz 1 Buchstabe d dahin, dass es Mitgliedstaaten – selbst in einem Einzelfall – untersagt ist, die Übermittlung angeforderter Daten aus Gründen, die sich aus der Anwendung ihres eigenen **rechtlichen Rahmens für die internationale Übermittlung personenbezogener Daten** ergeben, abzulehnen oder zu verhindern. Mit anderen Worten: Man kann sich nicht auf zusätzliche besondere Voraussetzungen für die Übermittlung personenbezogener Daten berufen, um eine Übermittlung an eine Vertragspartei des Protokolls abzulehnen oder zu verhindern. Allerdings bietet das Protokoll für den Fall, dass im Einzelfall zusätzliche Garantien erforderlich sein sollten, in Kapitel II (Maßnahmen für eine verstärkte Zusammenarbeit) Möglichkeiten, zusätzliche Garantien sicherzustellen (vgl. Abschnitt 4.4). Abschließend ist hervorzuheben, dass nur ein rechtsgültiges Ersuchen im Sinne des Protokolls, das unter anderem die in den Artikeln 13 und 14 genannten Anforderungen erfüllt, die Verpflichtung begründen kann, der ersuchenden Vertragspartei zu helfen und die Daten zu übermitteln.

4.2. Grundsatz der Verhältnismäßigkeit

42. Nach **Artikel 13** des Protokolls muss – in Einklang mit Artikel 15 des Übereinkommens über Computerkriminalität[53], in dem ausdrücklich auf den Grundsatz der Verhältnismäßigkeit Bezug genommen wird – „*jede Vertragspartei [sicherstellen], dass für die Schaffung, Umsetzung und Anwendung der in diesem Protokoll vorgesehenen Befugnisse und Verfahren Bedingungen und*

Garantien ihres innerstaatlichen Rechts gelten, die einen angemessenen Schutz der Menschenrechte und Freiheiten vorsehen". Dies gilt für alle Bestimmungen des Protokolls.

43. Der EDSB merkt auch positiv an, dass **Artikel 14 Absatz 2 Buchstabe b** vorsieht, dass bei der Einholung und Verarbeitung personenbezogener Daten[54] „*[d]ie empfangende Vertragspartei ... in ihrem innerstaatlichen Recht [sicherstellt], dass angeforderte und verarbeitete personenbezogene Daten für den Verarbeitungszweck erheblich sind und nicht darüber hinausgehen*".[55] Das Protokoll enthält zwar keine genaueren Angaben dazu, was mit „erheblich ... und nicht darüber hinausgehen[d]" gemeint ist, doch Nummer 231 des erläuternden Berichts stellt klar, dass diesem Erfordernis durch die „*Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit*" Rechnung getragen werden kann.

44. Außerdem heißt es in **Artikel 14 Absatz 2 Buchstabe a**, dass „*[d]ie Vertragspartei, die personenbezogene Daten empfangen hat, ... diese für die in Artikel 2 bezeichneten Zwecke [verarbeitet][56]. Sie darf die personenbezogenen Daten nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeiten und die Daten nicht weiterverarbeiten, wenn dies nach ihrem innerstaatlichen Recht nicht zulässig ist.*" Insbesondere aus Artikel 2 des Protokolls ergibt sich, wie im erläuternden Bericht eingehender erklärt wird, dass die Bestimmungen des Protokolls nicht dafür verwendet werden dürfen, Daten in Massen oder Mengen zu produzieren[57].

45. Überdies sind, wie bereits erwähnt, in Kapitel II des Protokolls (Maßnahmen für eine verstärkte Zusammenarbeit) zusätzliche Möglichkeiten für die Umsetzung des Verhältnismäßigkeitsgrundsatzes vorgesehen.

46. Der EDSB ist der Meinung, dass sich die Anwendung dieses Grundsatzes[58] und die Möglichkeit, die Ausführung eines gemäß dem Protokolls gestellten Ersuchens aus Gründen der Verhältnismäßigkeit zum Teil oder ganz ablehnen zu können, ebenfalls aus diesem Kapitel ergeben, das nicht nur die Möglichkeit vorsieht, die Lieferung der angeforderten Informationen an Bedingungen zu knüpfen[59], sondern in den Artikeln 7, 8 und 10 auch Ablehnungsgründe vorsieht, wie etwa Artikel 27 Absatz 4 des Übereinkommens über Computerkriminalität[60].

4.3. Schutz personenbezogener Daten

47. In Artikel 14 Absätze 2 bis 15 sind die grundlegenden Datenschutzgrundsätze niedergelegt, die für alle Formen der im Protokoll vorgesehenen Zusammenarbeit gelten.

48. Diese Grundsätze decken die in der DSGVO und der Strafverfolgungsrichtlinie vorgesehenen ab: Zweckbindung, Datenminimierung, Richtigkeit, Sicherheit und Integrität, sensible Daten, Verantwortlichen auferlegte Verpflichtungen (in Bezug auf Speicherung und Speicherbegrenzung, automatisierte Entscheidungsfindung, Aufzeichnungen und Protokollierung, sowie in Bezug auf Informationsweitergabe und Weiterübermittlung), Individualrechte (auf Transparenz und Information, Auskunft, Berichtigung, einschließlich Löschung) sowie gerichtliche und außergerichtliche Rechtsbehelfe und unabhängige und wirksame Beaufsichtigung durch eine oder mehrere Behörden (vgl. Abschnitt 5).

4.3.1. Grundsätze der Zweckbindung und Datenminimierung

49. Wie bereits erwähnt, ist die **Übermittlung personenbezogener Daten durch Strafverfolgungsbehörden eines Mitgliedstaats** an ein Drittland zulässig, wenn dies zum Zwecke der Ermittlung, Aufdeckung oder Verfolgung von Straftaten erforderlich ist.

50. Dabei finden gemäß **Artikel 2** des Protokolls die im Protokoll genannten Maßnahmen Anwendung „*auf **spezifische** strafrechtliche Ermittlungen oder Verfahren in Bezug auf Straftaten*

in Zusammenhang mit Computersystemen und -daten und auf die Erhebung von Beweismaterial in elektronischer Form für eine Straftat … und zwischen den Vertragsparteien des Ersten Zusatzprotokolls, die Vertragsparteien des vorliegenden Protokolls sind, auf ***spezifische*** *strafrechtliche Ermittlungen oder Verfahren in Bezug auf Straftaten nach dem Ersten Zusatzprotokoll*"[61].

51. Dieses Ziel fällt unter die in der Strafverfolgungsrichtlinie genannten Zwecke[62]

52. Der EDSB begrüßt, dass gemäß **Artikel 14 Absatz 2 Buchstabe a die Verarbeitung von personenbezogenen Daten, die gemäß dem Protokoll empfangen wurden,**[63] **auf den Anwendungsbereich des Protokolls zu beschränken ist**.

53. **Was die weitere Verarbeitung empfangener Daten angeht,**[64] begrüßt der EDSB das **in Artikel 14 Absatz 2 vorgesehene Verbot der Weiterverarbeitung der personenbezogenen Daten, wenn die Weiterverarbeitung einem nicht zu vereinbarenden Zweck dient**[65] bzw. **wenn sie nach dem innerstaatlichen Recht der Vertragspartei nicht zulässig ist**. Diesbezüglich merkt der EDSB positiv an, dass die zuständigen Behörden im erläuternden Bericht angehalten werden, eine Gesamtbetrachtung der spezifischen Umstände vorzunehmen, etwa*„(i) wie sich der ursprüngliche zum weiteren Zweck verhält (zum Beispiel, ob es einen objektiven Zusammenhang gibt); (ii) die (potenziellen) Folgen der beabsichtigten weiteren Verwendung für die betroffenen natürlichen Personen, unter Berücksichtigung der Art der personenbezogenen Daten (zum Beispiel deren Sensibilität); (iii) alle angemessenen Erwartungen der betroffenen natürlichen Personen hinsichtlich des Zwecks der weiteren Verwendung und der Stellen, von denen die Daten verarbeitet werden könnten; sowie (iv) die Art und Weise, wie die Daten verarbeitet und vor nicht ordnungsgemäßer Verwendung geschützt werden*"[66].

54. Wie bereits erwähnt, ist es nach dem Protokoll nur insoweit gestattet, personenbezogene Daten, die gemäß dem Protokoll empfangen wurden, zu einem zu vereinbarenden Zweck weiterzuverarbeiten, als dies mit Artikel 13, so wie er von der Vertragspartei im Einklang mit den Grundsätzen ihres innerstaatlichen Rechts umgesetzt wurde, vereinbar ist[67].

55. Der EDSB merkt des Weiteren positiv an, dass **Artikel 14 Absatz 2 Buchstabe b** vorsieht, dass die empfangende Vertragspartei in ihrem innerstaatlichen Recht sicherstellt, dass angeforderte und verarbeitete personenbezogene Daten für den Verarbeitungszweck erheblich sind und nicht darüber hinausgehen[68].

56. Darüber hinaus wird in **Artikel 14 Absatz 2 Buchstabe a** festgelegt, dass „*[d]ieser Artikel … nicht die Möglichkeit der übermittelnden Vertragspartei*[69] *[berührt], in einem bestimmten Fall zusätzliche Bedingungen nach diesem Protokoll vorzusehen, jedoch dürfen diese Bedingungen keine allgemeinen Datenschutzbedingungen einschließen*"[70]; eine solche Bedingung wäre etwa die Anforderung, dass die ersuchende Vertragspartei eine spezielle Datenschutzbehörde haben muss, obwohl gemäß Artikel 14 verschiedene Aufsichtssysteme akzeptabel sind[71]. Laut dem erläuternden Bericht[72] ist die Auferlegung solcher Bedingungen möglich, soweit dies in Kapitel II des Protokolls vorgesehen ist.

57. Der EDSB versteht dies daher so, dass für den Fall, dass die empfangende Behörde nicht in der Lage wäre, sämtliche oder einen Teil dieser zusätzlichen Bedingungen zu erfüllen, es nicht dem letzteren Verbot unterläge, wenn im betreffenden Einzelfall die Datenübermittlung verweigert, verhindert oder reduziert würde, weil dies ja seinen Grund in den konkreten Umständen des Einzelfalls hätte.

58. In Bezug auf die **Daten, die als Teil der jeweiligen Ersuchen oder Anordnungen übermittelt werden,** enthält Kapitel II des Protokolls spezifische Bestimmungen, die es der ersuchenden Vertragspartei gestatten, besondere Verfahrensanweisungen in ihr Ersuchen oder ihre Anordnung aufzunehmen, etwa Vorgaben hinsichtlich der Vertraulichkeit oder der Nichtweitergabe der personenbezogenen Daten an den Domäneninhaber, den Dienstteilnehmer oder sonstige Dritte[73]. Es ist jedoch zu beachten, dass das Protokoll lediglich eine Möglichkeit der Zusammenarbeit eröffnet, jedoch keine Verpflichtung begründet, gemäß dem Protokoll um Rechtshilfe zu ersuchen. Sollte also die ersuchende Behörde die geforderten zusätzlichen Garantien nicht geben, lässt das Protokoll den Vertragsparteien die Möglichkeit, von anderen ihnen zur Verfügung stehenden Wegen der Zusammenarbeit Gebrauch zu machen (Artikel 5 Absatz 7). Der EDSB versteht dies so, dass, was die Mitgliedstaaten angeht, von solchen anderen Möglichkeiten der Zusammenarbeit Gebrauch gemacht werden könnte, sofern diese unionsrechtskonform sind.

59. Was **die angeforderten Daten** angeht, nimmt der EDSB positiv zur Kenntnis, dass Artikel 6 die Verpflichtung enthält, die Informationen nur für die spezifischen strafrechtlichen Ermittlungen oder Verfahren zu verwenden, für die die Daten angefordert werden. Gemäß Artikel 7 Absatz 5 Buchstabe c Ziffer ii (der nach dem Vorschlag der Kommission in den Mitgliedstaaten anwendbar wäre) sowie Artikel 8 und Artikel 10 des Protokolls kann die ersuchte Vertragspartei die Lieferung der Informationen oder Materialien, um die ersucht wird, an die Bedingung knüpfen, dass diese nicht für andere Untersuchungen oder Verfahren als die im Ersuchen angegebenen verwendet werden[74]. Gemäß Artikel 9 Absatz 6 des Protokolls kann die ersuchte Vertragspartei Bedingungen angeben, unter denen sie die Daten zur Verfügung stellen würde; dabei kann es sich um eine Beschränkung oder sonstige Bedingung hinsichtlich der weiteren Verwendung der Daten handeln, zum Beispiel die Bedingung, über die weitere Verwendung informiert zu werden. Dass die Möglichkeit besteht, die Verwendung auf Grundlage des Protokolls empfangener Daten zu beschränken, bestätigt auch der erläuternde Bericht, der weitere Klarstellungen zu den Ausnahmen von dieser Möglichkeit enthält[75].

60. Hinsichtlich der Übermittlungen gemäß Artikel 7 stellt der erläuternde Bericht[76] klar, dass das Verfahren gemäß Absatz 5 Buchstabe d[77] „auch Gelegenheit bieten kann, Aspekte der Vertraulichkeit der angeforderten Informationen sowie der Beschränkung der Verwendung, die von der die Daten anfordernden Behörde beabsichtigt wird, zu klären".

61. Zwar bedauert der EDSB, dass im Protokoll kein allgemeiner Mechanismus vorgesehen ist, nach dem die zuständigen Behörden der betroffenen Mitgliedstaaten über die Weiterverarbeitung informiert werden, er merkt jedoch an, dass das Protokoll einen Rahmen bietet, der es der Vertragspartei, die die Daten übermittelt, ermöglicht, Beschränkungen hinsichtlich der weiteren Verwendung der Daten aufzuerlegen, und dass die Vertragsparteien davon Gebrauch machen könnten, um gegebenenfalls über die Weiterverarbeitung auf dem Laufenden gehalten zu werden. Dazu heißt es im erläuternden Bericht, dass „das Material für einen anderen Zweck verwendet werden darf, sofern dies mit vorheriger Einwilligung der übermittelnden Vertragspartei geschieht"[78]. Mit Inkrafttreten des Protokolls bestünde ein günstiges Umfeld, in dem die Vertragsparteien weitere Transparenzmaßnahmen (wie etwa Verwendungsbeschränkungen (Handling Codes)) im Einzelfall bilateral vereinbaren könnten.

4.3.2. Grundsätze der Speicherbegrenzung und Datenspeicherung

62. In Artikel 14 Absatz 5 sieht das Protokoll die Verpflichtung vor, die personenbezogenen Daten lediglich so lange zu speichern, wie es für die Zwecke der Verarbeitung der Daten nach Artikel 2 des Protokolls notwendig und verhältnismäßig ist. Die Daten können also für die Dauer der Ermittlungen und des anschließenden Verfahrens sowie für weitere Verarbeitungen, die nicht

mit dem ursprünglichen Zweck unvereinbar sind, gespeichert werden. Zur Erfüllung dieser Verpflichtung müssen die Vertragsparteien in ihren innerstaatlichen Rechtsrahmen genaue Speicherfristen und/oder genaue Abstände, in denen die Erforderlichkeit der weiteren Speicherung zu überprüfen ist, vorschreiben. Laut dem erläuternden Bericht sollten die Vertragsparteien „*in ihrem Rechtsrahmen sicherstellen, dass die zuständigen Behörden interne Vorschriften und/oder Verfahren für die Umsetzung der spezifischen Aufbewahrungsfristen und/oder regelmäßigen Überprüfungen der Erforderlichkeit der weiteren Speicherung ausarbeiten. Ist die Speicherfrist abgelaufen oder hat die Vertragspartei bei der regelmäßigen Überprüfung festgestellt, dass die weitere Speicherung der Daten nicht mehr erforderlich ist, sind die Daten zu löschen oder zu anonymisieren*“[79].

4.3.3. Grundsatz der Richtigkeit

63. Nach Artikel 14 Absatz 3 des Protokolls muss jede Vertragspartei angemessene Maßnahmen ergreifen, um sicherzustellen, dass personenbezogene Daten mit der für ihre rechtmäßige Verarbeitung notwendigen und angemessenen Richtigkeit, Vollständigkeit und Aktualität aufbewahrt werden, wobei die Zwecke, für die sie verarbeitet werden, Berücksichtigung finden. Laut dem erläuternden Bericht werden die *Vertragsparteien angehalten, angemessene Maßnahmen zu ergreifen, um für den Fall, dass die Daten, die einer anderen Behörde geliefert oder die von einer anderen Behörde empfangen wurden, unrichtig oder veraltet sind, sicherzustellen, dass die andere Behörde so bald wie praktisch möglich unterrichtet wird, um, soweit dies für die Zwecke der Verarbeitung erforderlich und angemessen ist, Berichtigungen vorzunehmen*“[80].

4.3.4. Grundsätze der Sicherheit, Integrität und Vertraulichkeit

64. Das Protokoll schneidet wichtige Fragen hinsichtlich der Sicherheit der übermittelten Daten an. Der EDSB möchte hervorheben, dass der Schutz personenbezogener Daten nicht nur eine eindeutige Anforderung nach dem Unionsrecht[81] ist, sondern vom EuGH auch in Bezug auf das Wesen des Grundrechts auf Datenschutz berücksichtigt wird. Auch bei der Gewährleistung der Vertraulichkeit von Ermittlungen und Strafverfahren ist Datensicherheit wesentlich.

65. Der EDSB begrüßt deshalb Artikel 14 Absatz 7, der den Vertragsparteien die Pflicht auferlegt, sicherzustellen, dass sie über geeignete technische, physische und organisatorische Maßnahmen zum Schutz personenbezogener Daten verfügen, sowie bei einem Sicherheitsvorfall, „*von dem eine erhebliche Gefahr eines körperlichen oder anderen Schadens für Personen oder die andere Vertragspartei ausgeht*“, umgehend geeignete Schadensbegrenzungsmaßnahmen zu ergreifen, wobei diese Maßnahmen die Benachrichtigung der übermittelnden Behörde und der betroffenen Person einschließen.

66. Der EDSB nimmt auch die Erklärung, die dafür im erläuternden Bericht gegeben wird, positiv zur Kenntnis[82].

67. Darüber hinaus ist in Kapitel II des Protokolls ausdrücklich vorgesehen, dass bei der Vorlage von Ersuchen in elektronischer Form, die Einhaltung angemessener Sicherheits- und Authentifizierungsstandards verlangt werden kann[83].

4.3.5. Führung von Aufzeichnungen oder Protokollierung (Grundsatz der Rechenschaftspflicht)

68. Der EDSB begrüßt die in Artikel 14 Absatz 8 vorgesehene Verpflichtung, Aufzeichnungen zu führen oder über andere geeignete Mittel, wie etwa die Protokollierung[84], zu verfügen, um

nachzuweisen, wie in einem bestimmten Fall auf die personenbezogenen Daten einer Person zugegriffen wird, wie diese verwendet und wie sie weitergegeben werden. Er bedauert jedoch, dass diese Verpflichtung keine genaueren Vorgaben dazu vorsieht, welche Angaben enthalten sein müssen. Ihm missfällt, dass diese Verpflichtung nur für bestimmte Verarbeitungstätigkeiten (Zugang, Verwendung und Weitergabe) gilt und nicht für andere Verarbeitungstätigkeiten wie etwa die Speicherung.

4.3.6. Sensible Daten

69. Nach der Rechtsprechung des Gerichtshofs sind Garantien insbesondere erforderlich, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht[85].

70. Hinsichtlich der Frage, **welche Datenkategorien besondere Kategorien personenbezogener Daten im Sinne des Protokolls** sind, merkt der EDSB positiv an, dass in Artikel 14 Absatz 4 des Protokolls die Verarbeitung von „personenbezogenen Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder sonstige Überzeugungen oder eine Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, von biometrischen Daten, *die angesichts der damit verbundenen Gefahren als sensibel angesehen werden*, oder von die Gesundheit oder das Sexualleben betreffenden personenbezogenen Daten“ erwähnt ist[86]. Nach dieser Vorschrift ist die Verarbeitung solcher sensiblen Daten nur „unter Wahrung angemessener Garantien zum Schutz vor *ungerechtfertigten nachteiligen Auswirkungen der Verwendung solcher Daten*, insbesondere vor unrechtmäßiger Diskriminierung“ gestattet [87]

71. Dazu ist anzumerken, dass Artikel 14 Absatz 2 Buchstabe b – der in Verbindung mit Artikel 13 zu lesen ist – vorschreibt, dass insbesondere sicherzustellen ist, dass „*angeforderte und verarbeitete personenbezogene Daten für den Verarbeitungszweck erheblich sind und nicht darüber hinausgehen*“[88] und dass es im Falle automatisierter Entscheidungen geeignete Garantien geben muss (Artikel 14 Absatz 6, siehe unten).

72. Was die **Verarbeitung personenbezogener Daten** – sei es im Ersuchen enthaltene Daten oder angeforderte Daten – betrifft, ist anzumerken, dass der erläuternde Bericht die Vertragsparteien in Bezug auf den im Protokoll verankerten Grundsatz der Datensicherheit (siehe oben) dazu anregt, Maßnahmen zu entwickeln und umzusetzen, die die Sensibilität der Daten berücksichtigen[89]. Darüber hinaus sind die Daten im Fall der Weitergabe innerhalb einer Vertragspartei gemäß Artikel 14 zu verarbeiten, wobei jede Weiterübermittlung von der übermittelnden Behörde autorisiert sein muss (Artikel 14 Absätze 9 und 10, siehe unten).

73. Bei der **Übermittlung von Daten in Erledigung von Ersuchen oder Anordnungen**, die aufgrund des Protokolls erlassen wurden, kann die übermittelnde Behörde im Einzelfall, soweit dies in Kapitel II des Protokolls (Maßnahmen für eine verstärkte Zusammenarbeit) vorgesehen ist, zusätzliche Bedingungen für die Verwendung der Daten vorsehen (Artikel 14 Absatz 2 Buchstabe a) Nach Kapitel II gibt es verschiedene Möglichkeiten – auf der einen Seite ein nicht bindendes Ersuchen mit der Möglichkeit, es an Bedingungen nach nationalem Recht zu knüpfen, bei denen es sich folglich um spezifische Bedingungen für die besondere Datenkategorie, um die es geht, handeln könnte, oder, auf der andere Seite, die Zusammenarbeit gemäß den Artikeln 7, 8 und 10 mit der Möglichkeit, spezifische Bedingungen hinzuzufügen, bei denen es sich folglich um spezifische Bedingungen für die besondere Datenkategorie, um die es geht, handeln könnte[90], oder aber die Übermittlung der angeforderten Daten zu verweigern, falls die Anordnung, trotz der Garantien, denen die Anordnung gemäß dem Protokoll unterliegt[91], wesentliche Interessen der ersuchten Vertragspartei beeinträchtigt (Artikel 27 Absatz 4 des Übereinkommens über

Computerkriminalität) oder die Voraussetzungen des Artikels 25 Absatz 4 des Übereinkommens über Computerkriminalität erfüllt sind[92].

74. In Bezug auf **Daten, die Teil der jeweiligen Ersuchen oder Anordnungen sind,** enthält Kapitel II des Protokolls spezifische Bestimmungen, die es der ersuchenden Vertragspartei gestatten, besondere Verfahrensanweisungen in ihr Ersuchen oder ihre Anordnung aufzunehmen, etwa Vorgaben hinsichtlich der Vertraulichkeit oder der Nichtweitergabe der personenbezogenen Daten an den Domäneninhaber, Dienstteilnehmer oder an sonstige Dritte[93].

75. Der EDSB ist deshalb der Ansicht, dass es einer Behörde möglich wäre, im Einzelfall zusätzliche Garantien für die Verarbeitung biometrischer Daten in der empfangenen Vertragspartei zu verlangen, selbst wenn die biometrischen Daten von der empfangenden Vertragspartei nicht als sensible Daten im Sinne von Absatz 4 angesehen werden.

4.3.7. Automatisierte Entscheidungen

76. Nach der Rechtsprechung des EuGH ist „*[d]as Erfordernis, über solche Garantien zu verfügen, … umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden. Dies gilt insbesondere, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht*“[94].

77. Der EDSB begrüßt, dass Artikel 14 Absatz 6 automatisierte Entscheidungen, die „ausschließlich auf eine automatisierte Verarbeitung von personenbezogenen Daten gestützt“ sind, verbietet, wenn sie „die rechtmäßigen Interessen [der betroffenen Person] erheblich beeinträchtigen, es sei denn, dies ist nach innerstaatlichem Recht zulässig und es gibt geeignete Garantien“. Zu den Garantien gegen eine erhebliche Beeinträchtigung der rechtmäßigen Interessen des Betroffenen zählt die „*Möglichkeit, das Eingreifen eines Menschen zu erwirken*“. So wird sichergestellt, dass automatisierte Entscheidungen, die auf gemäß dem Protokoll empfangenen Daten beruhen, nur ergehen, wenn die Möglichkeit besteht, dass ein Mensch eingreift, und wenn es geeignete Garantien gibt. Dies ist im Bereich der Strafverfolgung besonders wichtig, da hier die Folgen einer Erstellung von Profilen natürlicher Personen noch gravierender sein können.

78. Es ist auch anzumerken, dass es im erläuternden Bericht heißt, dass „*geeignete Garantien für die Minderung der potenziellen Beeinträchtigung der rechtmäßigen Interessen der Person, auf die sich die personenbezogenen Daten beziehen, von entscheidender Bedeutung sind*“[95]. Dies ist in Verbindung mit Artikel 13 zu lesen, der bestimmt, dass für die im Protokoll vorgesehenen Befugnisse und Verfahren die „*Bedingungen und Garantien ihres innerstaatlichen Rechts gelten, die einen angemessenen Schutz der Menschenrechte und Freiheiten vorsehen*“.

79. Darüber hinaus sieht das Protokoll für **besondere Kategorien personenbezogener Daten**, die von einer Strafverfolgungsbehörde gemäß dem Protokoll empfangen und verarbeitet werden, vor, dass die Verarbeitung sensibler Daten „*nur unter Wahrung angemessener Garantien zum Schutz vor ungerechtfertigten nachteiligen Auswirkungen der Verwendung solcher Daten*“[96], insbesondere vor unrechtmäßiger Diskriminierung erfolgen darf (Artikel 14 Absatz 6 in Verbindung mit Artikel 14 Absatz 4).

80. Abschließend sei darauf hingewiesen, dass Artikel 14 Absatz 2 Buchstabe b des Protokolls, wie bereits oben im Abschnitt über Zweckbindung und Datenminimierung erwähnt, der ersuchenden Vertragspartei die Verpflichtung auferlegt, sicherzustellen, dass angeforderte und verarbeitete personenbezogene Daten für den Verarbeitungszweck erheblich sind und nicht darüber hinausgehen. Außerdem sieht das Protokoll für die übermittelnde Vertragspartei die Möglichkeit vor, zusätzliche Bedingungen für die anschließende Verwendung vorzusehen (Artikel 14 Absatz 2 Buchstabe a in Verbindung mit Kapitel II – Maßnahmen für eine verstärkte Zusammenarbeit –

siehe oben). Der EDSB versteht dies so, dass zum Beispiel die übermittelnde Behörde eines Mitgliedstaats im Einzelfall jede spezifische Maßnahme ergreifen kann, um die Rechte und Freiheiten sowie die rechtmäßigen Interessen der betroffenen Person zu schützen. Umso wichtiger ist es deshalb, dass die Mitgliedstaaten, wie von der Kommission vorgeschlagen, von der in Artikel 7 Absatz 5 vorgesehenen Erklärung Gebrauch machen, damit im ersuchten Mitgliedstaat stets eine Behörde eingeschaltet ist; dies gilt für den Fall, dass der Rat die Mitgliedstaaten ermächtigt, das Protokoll im Interesse der Europäischen Union zu unterzeichnen bzw. zu ratifizieren, ohne sich das Recht, Artikel 7 nicht anzuwenden, vorzubehalten[97].

4.3.8. Weitergabe innerhalb einer Vertragspartei

81. Der EDSB begrüßt die Bestimmungen in Artikel 14 Absatz 9 über die Weitergabe innerhalb einer Vertragspartei und merkt positiv an, dass die Verarbeitung der aufgrund des Protokolls empfangenen Daten durch die andere Behörde der empfangenden Vertragspartei gemäß Artikel 14 erfolgt. Der erläuternde Bericht[98] stellt klar, dass das in Artikel 7 Absatz 5 Buchstabe d vorgesehene Verfahren – welches nach den Vorschlägen der Kommission in den Mitgliedstaaten anwendbar wäre (siehe unten) – auch die Möglichkeit vorsieht, Aspekte der Vertraulichkeit der ersuchten Informationen sowie der beabsichtigten Beschränkung der Verwendung durch die die Daten anfordernden Behörde zu klären. Außerdem ist es der ersuchenden Behörde gemäß Kapitel II des Protokolls möglich, besondere Anweisungen zu erteilen, die die Weitergabe des Ersuchens an Dienstteilnehmer oder andere Dritte untersagen[99].

4.3.9. Weiterübermittlung an andere Staaten oder internationale Organisationen

82. Der EDSB begrüßt die in Artikel 14 Absatz 10 vorgesehene Bestimmung, nach der die empfangende Vertragspartei für die Übermittlung an einen anderen Staat oder eine internationale Organisation der vorherigen Genehmigung der übermittelnden Behörde bedarf.

4.3.10. Konsultation und Aussetzung

83. Der EDSB begrüßt, dass das Protokoll in Artikel 14 Absatz 15 eine spezifische Bestimmung vorsieht, nach der die Übermittlung personenbezogener Daten an eine andere Vertragspartei des Protokolls ausgesetzt werden kann, wenn „*systematisch oder schwerwiegend gegen diesen Artikel [verstoßen wird] oder ... ein schwerwiegender Verstoß unmittelbar bevorsteht*“.

84. Insbesondere im Hinblick darauf, dass Artikel 14 Absatz 1 Buchstabe d eine weitere Genehmigung der Übermittlung untersagt, möchte der EDSB daran erinnern, dass die Einrichtung unabhängiger nationaler Aufsichtsbehörden in den Mitgliedstaaten ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten darstellt[100]. Die nationalen Kontrollstellen sind für die Überwachung der Einhaltung des Datenschutzrechts der Union gemäß Artikel 8 Absatz 3 der Charta verantwortlich, wobei jede Behörde ermächtigt ist, zu prüfen, ob die Übermittlung personenbezogener Daten aus dem eigenen Mitgliedstaat an ein Drittland dem geltenden Datenschutzrecht genügt, auch wenn das Rechtssystem des betreffenden Drittlands für angemessen befunden wurde oder eine Konformitätsvermutung auf der Grundlage eines Abkommens besteht.

4.3.11. Überprüfung

85. Der EDSB begrüßt, dass in Artikel 23 ein Verfahren eingeführt wird, nach dem die wirksame Anwendung und Durchführung des Protokolls in regelmäßigen Abständen bewertet wird, sowie die Klarstellung im erläuternden Bericht[101], dass „*die Vertragsparteien im Hinblick auf die*

Fachkenntnisse, die für die Bewertung der Anwendung und Durchführung einiger der Bestimmungen dieses Protokolls, einschließlich des Artikels 14 über Datenschutz, erforderlich sind, in Betracht ziehen könnten, ihre Experten für diese Materie in die Bewertungen einzubeziehen".

4.4. Maßnahmen für eine verstärkte Zusammenarbeit

4.4.1. Allgemeine Anmerkungen

86. Der EDSB möchte zunächst daran erinnern, dass der Verantwortliche gemäß Erwägungsgrund 71 der Strafverfolgungsrichtlinie bei Übermittlungen, die nicht auf der Grundlage eines Angemessenheitsbeschlusses erfolgen, berücksichtigen muss, 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. Er begrüßt es deshalb, dass die im Protokoll in den Artikeln 7, 8 und 10 vorgesehenen Bestimmungen über die Zusammenarbeit, indem sie Artikel 27 Absatz 4 des Übereinkommens über Computerkriminalität als Grund für die Ablehnung der Übermittlung einführen, es der übermittelnden Vertragspartei gestatten, dieses Risiko zu berücksichtigen und die Datenübermittlung aus diesem Grund abzulehnen.

87. Darüber hinaus können, so wie es der EDSB versteht, **Sonderrechte und Immunitäten** nicht nur von einer ersuchten Vertragspartei geltend gemacht werden, um im Einzelfall Herausgabeanordnungen gemäß Artikel 25 Absatz 4 und Artikel 27 Absatz 4 des Übereinkommens über Computerkriminalität abzulehnen[102], sondern auch von einer Vertragspartei als Teil der angemessenen Bedingungen des innerstaatlichen Rechts bezüglich nicht bindender Ersuchen gemäß den Artikeln 6 und 9 hinzugefügt werden[103].

88. Abschließend begrüßt der EDSB, dass in die endgültige Fassung des Protokolls keine Bestimmung über den **direkten Datenzugang für Strafverfolgungsbehörden** aufgenommen wurde.

4.4.2. Weitergabe von Bestandsdaten – direkt von Diensteanbietern an zuständige Behörden einer anderen Vertragspartei (Artikel 7)

4.4.2.1. Von der ersuchten Vertragspartei vorgenommene Beschränkung im Hinblick auf den Status der ersuchenden Behörden

89. Der EDSB begrüßt, dass die Mitgliedstaaten im Anhang angewiesen werden, die Erklärung gemäß Artikel 7 Absatz 2 Buchstabe b abzugeben, nach der Anordnungen an Diensteanbieter in ihrem Hoheitsgebiet durch eine Staatsanwältin beziehungsweise durch einen Staatsanwalt oder eine andere Justizbehörde oder unter staatsanwaltlicher Aufsicht oder unter Aufsicht einer anderen Justizbehörde oder anderweitig unter unabhängiger Aufsicht erlassen werden müssen.

4.4.2.2. Systematische Einschaltung einer Justizbehörde der ersuchten Vertragspartei

90. Der EDSB begrüßt, dass die Mitgliedstaaten im Anhang angewiesen werden, gemäß Artikel 7 Absatz 5 Buchstabe a des Protokolls zu notifizieren, dass sie, wenn eine Anordnung nach Artikel 7 Absatz 1 an einen Diensteanbieter in ihrem Hoheitsgebiet gerichtet wird, eine zeitgleiche Benachrichtigung ihrer Behörden über die Anordnung, die ergänzenden Angaben und eine Zusammenfassung des mit den Ermittlungen oder dem Verfahren in Zusammenhang stehenden Sachverhalts verlangen. Diese Behörden sind befugt, die Diensteanbieter anzuweisen, die Bestandsdaten nicht weiterzugeben, falls:

i. die Weitergabe strafrechtliche Ermittlungen oder Verfahren in der betreffenden Vertragspartei beeinträchtigen könnte; oder

ii. wenn, falls die Bestandsdaten im Wege der Rechtshilfe angefordert worden wären, in Artikel 25 Absatz 4 bzw. Artikel 27 Absatz 4 des Übereinkommens über Computerkriminalität[104] genannte Voraussetzungen oder Gründe für die Verweigerung gegeben gewesen wären.

91. Diesbezüglich sieht Artikel 7 Absatz 5 Buchstabe e vor, dass die Vertragsparteien eine einzige Behörde bestimmen, die solche Benachrichtigungen empfängt. Allerdings ist die Art der Behörde weder im Artikel noch im Anhang genau angegeben. Da es sich bei der zuständigen Behörde, die die Weitergabe der Informationen anordnet, unter Umständen nicht um eine Justizbehörde oder sonstige unabhängige Behörde handelt[105], empfiehlt der EDSB, **die Mitgliedstaaten anzuweisen, eine Justizbehörde oder sonstige unabhängige Behörde als Benachrichtigungsempfänger zu bestimmen**, damit diese Behörden in der Lage sind, wirksam zu überprüfen, dass die Anordnungen dem Übereinkommen über Computerkriminalität genügen, sowie die in Absatz 5 Buchstaben b, c und d genannten Maßnahmen zu ergreifen. Eine solche Einbeziehung stünde auch eher mit Artikel 82 Absatz 1 AEUV in Einklang.

92. Diesbezüglich erinnert der EDSB daran, dass der **EuGH** in seiner Rechtsprechung über den Zugang zu Kommunikationsdaten für Strafverfolgungszwecke **die Möglichkeit, solchen Zugang zu gewähren, von mehreren Voraussetzungen abhängig macht, unter anderem, und *„außer in hinreichend begründeten Eilfällen“*[106], von *„einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle“***, „*im Anschluss an einen mit Gründen versehenen Antrag der [zuständigen nationalen] Behörden[, der] im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten ergeht*“[107]. Die systematische Einbeziehung von Justizbehörden in den ersuchten Vertragsparteien ist auch von wesentlicher Bedeutung für die Wahrung des Grundsatzes der beiderseitigen Strafbarkeit[108] im Bereich der justiziellen Zusammenarbeit, da sie die Überprüfung der zur Anwendung dieses Grundsatzes führenden Umstände durch eine angemessene und geeignete Behörde ermöglicht. Der EDSB erinnert daran, dass der Grundsatz der beiderseitigen Strafbarkeit eine zusätzliche Garantie geben soll, um zu gewährleisten, dass es einem Staat nicht möglich ist, die Unterstützung eines anderen Staates in Anspruch zu nehmen, um eine strafrechtliche Sanktion anzuwenden, die das Recht des anderen Staates nicht kennt.

4.4.2.3. Definitionen und Datenarten

93. Der EDSB bemerkt, dass unter die Definition der Bestandsdaten in Artikel 18 Absatz 3 des Übereinkommens über Computerkriminalität auch Informationen fallen können, die nach dem Unionsrecht Verkehrsdaten sind. So können insbesondere Informationen zum Zwecke der Erkennung eines Dienstteilnehmers bestimmte Informationen zur Internet Protokoll (IP) Adresse enthalten – zum Beispiel die zum Zeitpunkt der Kontoeröffnung verwendete IP-Adresse, die IP-Adresse, von der zuletzt eingeloggt wurde oder die zu einem bestimmten Zeitpunkt zum Einloggen verwendeten IP-Adressen; nach dem Unionsrecht handelt es sich dabei um Verkehrsdaten bezüglich der Übertragung einer Kommunikation[109].

94. Überdies kommt es nach der einschlägigen Rechtsprechung des EuGH für die Feststellung eines Eingriffs in das Grundrecht auf Privatsphäre nicht darauf an, ob die betreffenden Informationen über die Privatsphäre sensibel sind oder ob die betroffenen Personen dadurch in irgendeiner Weise beeinträchtigt worden sind. In seinem Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 Tele2 Sverige AB hat der EuGH des Weiteren ausgeführt,

dass es anhand von Metadaten (wie z. B. Verkehrsdaten) möglich ist, ein Profil der betreffenden Personen zu erstellen, das im Hinblick auf das Recht auf Achtung der Privatsphäre eine genauso sensible Information darstellt wie der Inhalt der Kommunikationen selbst[110].

95. Im Hinblick darauf, dass eine Abwägung zwischen den Arten von Straftaten, derentwegen eine Anordnung erlassen werden kann, und den Kategorien der betroffenen Daten vorzunehmen ist, um den Erlass von Anordnungen der Herausgabe von Daten, die als Verkehrsdaten anzusehen sein könnten, in Grenzen zu halten, da der Zugang zu diesen nur zur Bekämpfung schwerer Straftaten gerechtfertigt ist, **empfiehlt der EDSB den Mitgliedstaaten – entgegen der von der Kommission im Anhang erteilten Anweisung -, sich das Recht, Artikel 7 nicht auf bestimmte Arten von Zugangsnummern anzuwenden, gemäß Artikel 7 Absatz 9 Buchstabe b vorzubehalten**, um eine stärkere Einbeziehung der Behörden im ersuchten Staat sicherzustellen. Dazu merkt er an, dass das Protokoll in Artikel 8 eine alternative Möglichkeit für eine umgehende Herausgabe von Daten zwischen den zuständigen Behörden der betreffenden Vertragsparteien vorsieht.

4.4.3. Durchführung von Anordnungen einer anderen Vertragspartei auf umgehende Herausgabe von Bestandsdaten und Verkehrsdaten (Artikel 8)

96. Der EDSB begrüßt, dass die Kommission die Mitgliedstaaten anweist, gemäß Artikel 8 Absatz 4 zu erklären, dass für die Erfüllung einer Anordnung nach Artikel 8 Absatz 1 zusätzliche begleitende Angaben erforderlich sind, die jeweils von den Umständen der Anordnung und den dazugehörigen Ermittlungen oder Verfahren abhängig sind; dies ist von besonderer Wichtigkeit dafür, die Behörden in die Lage zu versetzen, eine angemessene Entscheidung gemäß Artikel 8 Absatz 8 des Protokolls zu treffen.

97. Der EDSB nimmt des Weiteren die von der Kommission gegebene Anweisung zur Kenntnis, dass die „*Mitgliedstaaten, die sich an der Verstärkten Zusammenarbeit nach der Verordnung (EU) 2017/1939 zur Durchführung einer Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft (EUStA) beteiligen, … die EUStA bei der Ausübung ihrer Zuständigkeiten nach den Artikeln 22, 23 und 25 der Verordnung (EU) 2017/1939 in die Liste der Behörden [aufnehmen], die nach Artikel 8 Absatz 10 Buchstaben a und b mitgeteilt werden*“, d. h. in die Liste der Behörden, die nach Artikel 8 Absatz 10 Buchstabe a für die Vorlage einer Anordnung und nach Artikel 8 Absatz 10 Buchstabe b für die Entgegennahme einer Anordnung auf umgehende Herausgabe von Bestandsdaten und Verkehrsdaten benannt sind.

98. Der EDSB wiederholt, dass nach der Rechtsprechung des Europäischen Gerichtshofs die Möglichkeit, solchen Zugang zu gewähren, „grundsätzlich – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird[111]“ (siehe oben Nummer 92). Er betont deshalb, dass es einer Staatsanwalt eines Mitgliedstaates und folglich der EUStA möglich sollte, eine Anordnung vorzulegen oder auf eine gemäß dieser Bestimmung erlassene Anordnung einer anderen Vertragspartei hin Daten zu übermitteln, wenn sichergestellt ist, dass dies einer Überprüfung durch eine Justizbehörde oder eine unabhängige Stelle im Sinne der Rechtsprechung des EuGH unterliegt[112].

5. Durchsetzbare Rechte der betroffenen Person und wirksame Rechtsbehelfe für betroffene Personen

5.1. Recht auf Unterrichtung, Recht auf Auskunft, Recht auf Berichtigung und Löschung

99. Der EDSB erinnert daran, dass das Recht auf Auskunft und das Recht auf Berichtigung als wesentliche Elemente des Rechts auf den Schutz personenbezogener Daten in Artikel 8 Absatz 2 der Charta festgeschrieben sind. Auch wenn die Ausübung der Rechte betroffener Personen im Kontext der Strafverfolgung in der Regel eingeschränkt ist, um laufende Ermittlungen nicht zu gefährden, sollte für betroffene Personen die Möglichkeit der Ausübung ihrer Rechte in der Praxis tatsächlich bestehen und nicht rein theoretischer Natur sein, selbst wenn dies in Situationen, in denen die Ausübung dieser Rechte zum Schutz sensibler strafrechtlicher Informationen verweigert wird, eingeschränkt ist oder durch eine Behörde erfolgt.

100. Das Protokoll enthält Bestimmungen über das Recht auf Unterrichtung (Artikel 14 Absatz 11 („Transparenz und Information")), das Recht auf Auskunft (in Artikel 14 Absatz 12 Buchstabe a Ziffer i als „Zugang" bezeichnet) und das Recht auf Berichtigung, das auch Löschung und Sperrung einschließt (Artikel 14 Absatz 12 Buchstabe a Ziffer ii), sowie das Recht, keinen automatisierten Entscheidungen unterworfen zu sein (Artikel 14 Absatz 6 – siehe oben).

101. Dem **Recht auf Unterrichtung** kommt allergrößte Bedeutung zu, da es die Ausübung anderer Datenschutzrechte, etwa des Rechts auf Rechtsbehelf, ermöglicht und eine Verarbeitung der Daten nach Treu und Glauben gewährleistet[113]. In der Regel ist den betroffenen Personen die Tatsache, dass ihre Daten für Strafverfolgungszwecke verarbeitet (oder übermittelt) werden, nicht bekannt. Der EDSB erinnert daran, dass der EuGH in seinem Gutachten 1/15 in Bezug auf Übermittlungen durch Stellen des Privatsektors festgestellt hat, 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*", da „*[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 Absatz 1 der Charta bei einem Gericht einen wirksamen Rechtsbehelf einzulegen, ausüben können*"[114].

102. Der EDSB begrüßt deshalb, dass in Artikel 14 Absatz 11 aufgenommen wurde, dass jede Vertragspartei zur Unterrichtung verpflichtet ist, sei es durch Veröffentlichung allgemeiner Informationen oder durch persönliche Information der betroffenen Person. Man mag zwar bedauern, dass diese Verpflichtung nicht die Verpflichtung beinhaltet, die Kontaktangaben des Verantwortlichen mitzuteilen, doch der EDSB nimmt zur Kenntnis, dass das Protokoll jedenfalls zur Mitteilung der Rechtsgrundlage und Zwecke der Verarbeitung; etwaiger Speicher- und Überprüfungsfristen, soweit einschlägig; der Auskunfts-, Berichtigungs- und Rechtsbehelfsmöglichkeiten sowie der Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, verpflichtet.

103. Das Recht auf Unterrichtung findet auch Anwendung, wenn Daten zum Zwecke der Weiterverarbeitung innerhalb einer Vertragspartei weitergegeben werden (Artikel 14 Absatz 9).

104. Das Protokoll stellt überdies sicher, dass die betroffene Person, soweit das Recht der übermittelnden Vertragspartei dies verlangt, persönlich unterrichtet wird. Hat die andere Vertragspartei darum ersucht, die Bereitstellung der Daten, soweit die in Absatz 12 Buchstabe a

Ziffer i genannten Bedingungen für Beschränkungen gelten, vertraulich zu behandeln, erfolgt die persönliche Unterrichtung erst, wenn die Beschränkungen nicht mehr gelten[115]. Die Beschränkung der persönlichen Unterrichtung ist unter denselben Voraussetzungen möglich wie die Beschränkung des Rechts auf Auskunft (siehe unten).

105. Das **Recht auf Auskunft und das Recht auf Berichtigung** sind als wesentliche Elemente des Rechts auf Datenschutz in Artikel 8 Absatz 2 der Charta festgeschrieben. Des Weiteren hat der Gerichtshof zu Artikel 7 der Charta entschieden, „dass das darin niedergelegte Grundrecht auf Achtung des Privatlebens voraussetzt, dass sich die betroffene Person vergewissern kann, dass ihre personenbezogenen Daten fehlerfrei verarbeitet werden und die Verarbeitung zulässig ist. *Sie muss, um die nötigen Nachprüfungen durchführen zu können, ein Auskunftsrecht hinsichtlich der sie betreffenden Daten haben, die Gegenstand einer Verarbeitung sind*"[116].

106. Der EDSB begrüßt deshalb die Aufnahme eines **Rechts auf Auskunft und Berichtigung, welches das Recht auf Löschung einschließt**, in Artikel 14 Absatz 12 („Zugang und Berichtigung").

107. Das Protokoll sieht vor, dass das Recht auf Auskunft Beschränkungen unterliegen kann (Buchstabe a). 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. Diesbezüglich merkt der EDSB positiv an, dass im Protokoll ausdrücklich vorgesehen ist, dass die Beschränkungen verhältnismäßig und zum Schutz der Rechte und Freiheiten anderer oder wichtiger Ziele des allgemeinen öffentlichen Interesses erforderlich sein und die berechtigten Interessen der betroffenen Person angemessen berücksichtigen müssen. Er bedauert jedoch, dass es nach dem Protokoll nicht erforderlich ist, dass der innerstaatliche Rechtsrahmen der Vertragsparteien sicherstellt, dass die Möglichkeit, Auskunft über ihre eigenen Daten zu verlangen, für die betroffenen Personen tatschlich besteht, und sei es in beschränkter Form oder in Form der Ausübung durch eine Behörde.

108. Der EDSB bedauert, dass es nach dem Protokoll zulässig ist, eine Gebühr für die Auskunft („Zugangsgewährung") zu erheben (Buchstabe b). Er merkt jedoch an, dass solche Gebühren auf ein angemessenes und nicht überzogenes Maß beschränkt werden sollten, was laut dem erläuternden Bericht „im Hinblick auf die aufgewendeten Ressourcen" zu beurteilen ist, „um nicht von der Wahrnehmung des Rechts auf Auskunft abzuhalten oder abzuschrecken"[117]. Der EDSB versteht das Protokoll dahin, dass für die Ausübung des Rechts auf Berichtigung, einschließlich des Rechts auf Löschung, keine solche Gebühr erhoben werden darf.

5.2. Gerichtliche und administrative Rechtsbehelfe

109. Der EDSB erinnert daran, dass der EuGH in einem anderen Kontext, nämlich in Bezug auf eine Angemessenheitsfeststellung (Safe-Harbor-Entscheidung) festgestellt hat[118], dass der Wesensgehalt von Artikel 47 der Charta, der das Recht auf wirksamen gerichtlichen Rechtsschutz vorsieht, verletzt ist, wenn personenbezogene Daten an ein Drittland übermittelt werden, ohne dass es einen wirksamen gerichtlichen Rechtsbehelf gibt. In diesem Zusammenhang hat der EuGH ausgeführt, 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 dass „*[n]ach Art. 47 Abs. 1 der Charta … nämlich jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht [hat], nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht* ***einen wirksamen Rechtsbehelf*** *einzulegen*"[119].

110. Der EuGH hat ferner betont, dass es unerlässlich ist, dass es natürlichen Personen möglich sein muss, Beschwerden bei unabhängigen Kontrollstellen vorzubringen[120] und somit einen administrativen Rechtsbehelf einzulegen.

111. Der EDSB begrüßt deshalb, dass Artikel 14 Absatz 13 vorsieht, dass jede Vertragspartei über wirksame gerichtliche und außergerichtliche Rechtsbehelf verfügt, um Verstößen gegen diesen Artikel abzuhelfen.

5.3. Beaufsichtigung: Überwachung durch eine unabhängige Behörde

112. 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 Stelle vor. Auch wenn jeder Mitgliedstaat eine unabhängige Behörde benennt, die für die Aufsicht über die Verarbeitungstätigkeiten einschließlich der Datenübermittlungen an Drittländer zuständig ist, bedarf es doch nach erfolgter Übermittlung der Daten auch einer wirksamen, unabhängigen Aufsicht in den empfangenden Drittländern.

113. Der EDSB erinnert daran, dass nach der Rechtsprechung des EuGH[121] eine unabhängige Kontrollstelle im Sinne von Artikel 8 Absatz 3 der Charta eine Behörde ist, die ihre Entscheidungen ohne jede unmittelbare oder mittelbare Einflussnahme von außen erlassen kann. Eine solche Kontrollstelle muss nicht nur von den von ihr kontrollierten Stellen unabhängig sein, sondern sie sollte zudem nicht ihrerseits „*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*".[122]

114. Der EDSB begrüßt Artikel 14 Absatz 14 über Beaufsichtigung, der vorsieht, dass jede Vertragspartei über eine unabhängige Kontrollstelle verfügen muss, und die Befugnisse aufführt, die (eine) solche Behörde(n) gegenüber den Behörden hat, an die personenbezogene Daten gemäß dem Protokoll übermittelt werden. Aus dem erläuternden Bericht geht hervor, dass „*[d]ie Behörden in der Wahrnehmung ihrer Aufgaben und Ausübung ihrer Befugnisse unabhängig sein müssen; dass sie in der Lage sein müssen, frei von jeder Einflussnahme von außen, die in die unabhängige Ausübung ihrer Befugnisse und Funktionen eingreifen könnte, zu handeln; dass die betreffenden Behörden keinerlei Weisungen im Einzelfall unterliegen sollten, und zwar weder hinsichtlich der Ausübung ihrer Ermittlungsbefugnisse noch hinsichtlich der Vornahme von Korrekturmaßnahmen; und, als Letztes, dass es wichtig ist, dass die Behörden über die Fertigkeiten, Kenntnisse und das Fachwissen verfügen, die zur Wahrnehmung ihrer Pflichten erforderlich sind, und dass sie mit angemessenen finanziellen, technischen und personellen Mitteln zur wirksamen Ausübung ihrer Funktionen ausgestattet werden*"[123]. Der EDSB betont, dass es den Mitgliedstaaten für den Fall, dass in der Praxis festgestellt werden sollte, dass eine andere Vertragspartei über keine unabhängige Kontrollstelle verfügt, die den Unionsstandards im Wesentlichen gleichwertig ist, gestattet sein sollte, von der Aussetzungsbestimmung in Artikel 14 Absatz 15 Gebrauch zu machen, wenn es sich um einen Fall des systematischen oder wesentlichen Verstoßes gegen Artikel 14 handelt.

115. Auch wenn das Protokoll keinen spezifischen Mechanismus für die Zusammenarbeit zwischen den jeweiligen Kontrollstellen vorsieht und die Vertragsparteien nicht gehalten sind, ihre Kontrollstelle zu notifizieren, hält der EDSB es für positiv, dass im erläuternden Bericht angeregt wird, dass die Vertragsparteien die Zusammenarbeit zwischen ihren jeweiligen Kontrollstellen fördern. „*Die jeweiligen Behörden der Vertragsparteien können einander, soweit angemessen, im Zuge der Wahrnehmung ihrer Aufsichtsfunktionen gegenseitig konsultieren. Dies kann auch den Austausch von Informationen und bewährten Verfahren beinhalten*"[124].

6. Verhältnis der Datenschutzbestimmung (Artikel 14) des Protokolls zu anderen Übereinkünften

116. Wegen des multilateralen Charakters des Protokolls ist es Vertragsparteien, die Parteien bilateraler Übereinkünfte sind, nach Artikel 14 Absatz 1 Buchstaben b und c des Protokolls unter bestimmten Voraussetzungen gestattet, den Schutz der aufgrund des Protokolls übermittelten personenbezogenen Daten auf andere Weise sicherzustellen.

6.1. Verhältnis zwischen der Union und den USA

117. Während die Garantien in Artikel 14 Absätze 2 bis 15 für Vertragsparteien, die personenbezogene Daten empfangen, automatisch gelten, gilt gemäß Artikel 14 Absatz 1 Buchstabe b: „*Sind die übermittelnde Vertragspartei und die empfangende Vertragspartei zum Zeitpunkt des Empfangs personenbezogener Daten nach diesem Protokoll wechselseitig durch eine völkerrechtliche Übereinkunft gebunden, die zwischen diesen Vertragsparteien einen umfassenden Rahmen für den Schutz personenbezogener Daten schafft, der auf die Übermittlung personenbezogener Daten für den Zweck der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Straftaten Anwendung findet und der vorsieht, dass die Verarbeitung personenbezogener Daten nach dieser Übereinkunft den in den Datenschutzgesetzen der betreffenden Vertragsparteien niedergelegten Anforderungen entspricht, so finden bei Maßnahmen, die in den Geltungsbereich einer solchen Übereinkunft fallen, auf nach dem Protokoll empfangene personenbezogene Daten anstelle der Absätze 2 bis 15 die Vorgaben der Übereinkunft Anwendung, sofern die betreffenden Vertragsparteien nichts anderes vereinbart haben.*“

118. Der EDSB merkt an, dass im erläuternden Bericht[125] das Rahmenabkommen zwischen der EU und den USA [126]als Beispiel für eine solche Übereinkunft angeführt wird; im erläuternden Bericht heißt es, dass „*hinsichtlich der Maßnahmen, die Gegenstand solcher Übereinkünfte sind, die Bestimmungen der Übereinkünfte anstelle der Absätze 2 bis 15 Anwendung finden*“.

119. Diesbezüglich begrüßt der EDSB, dass die Kommission den Mitgliedstaaten vorschlägt, den Behörden der Vereinigten Staaten von Amerika die Sichtweise der EU in dieser Frage mitzuteilen.

120. Der EDSB versteht die Lage so, dass feststeht, dass auf Übermittlungen aus der EU in die Vereinigten Staaten von Amerika, die im Rahmen der im Protokoll enthaltenen Vorschriften über die **behördliche Zusammenarbeit** erfolgen, das Rahmenabkommen Anwendung fände. Der EDSB bedauert dieses Ergebnis.

121. Was die **Vorschriften des Protokolls über die direkte Zusammenarbeit** (Artikel 6 und 7) angeht, möchte der EDSB daran erinnern, dass das Rahmenabkommen nicht anwendbar wäre[127]. Eine Anwendbarkeit käme nur in Betracht, wenn es durch ein Abkommen zwischen der Union und den Vereinigten Staaten, das zusätzliche Garantien enthielte, abgeändert würde. Insoweit verweist er auf seine Stellungnahme zur Empfehlung der Europäischen Kommission für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein internationales Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln[128]. Der EDSB geht deshalb davon aus, dass, solange kein solches Abkommen angenommen wurde und im Verhältnis der beiden Vertragsparteien in Kraft getreten ist, die Garantien in Artikel 14 des Protokolls auf die Verarbeitung personenbezogener Daten, die eine Vertragspartei gemäß den Bestimmungen des Protokolls über die direkte Zusammenarbeit empfängt, Anwendung finden.

122. Der EDSB versteht dies so, dass die von der Kommission vorgeschlagene Mitteilung darauf abzielt, genauer klarzustellen, dass das Rahmenabkommen, was die im Protokoll vorgesehene direkte Zusammenarbeit angeht, im Verhältnis zwischen der Union und den USA nicht anstelle von Artikel 14 Absätze 2 bis 15 des Protokolls anwendbar wäre. In der Tat ergibt sich aus Artikel 14 Absatz 1 Buchstabe b des Protokolls in Verbindung mit den im Unionsrecht niedergelegten Anforderungen, dass nur ein rechtliches bindendes Instrument, das von der Union und den Vereinigten Staaten in Form eines internationalen Abkommens abgeschlossen wird, um das Rahmenabkommen zu ändern und die erforderlichen zusätzlichen Garantien vorzusehen, die in Artikel 14 Absatz 1 Buchstabe b des Protokolls genannten Voraussetzungen erfüllen könnte, die erfüllt sein müssen, damit seine Datenschutzbestimmungen anstelle von Artikel 14 Absätze 2 bis 15 des Protokolls Anwendung finden. Der EDSB **würde deshalb für den Fall, dass der Rat beschließt, die Mitgliedstaaten zur Unterzeichnung und Ratifizierung des Protokolls zu ermächtigen, empfehlen, die vorgeschlagene Mitteilung, in der zurzeit von „einer spezifischen Übermittlungsvereinbarung" die Rede ist, noch klarer zu formulieren.**

6.2. Verhältnis zwischen der Union und anderen Drittländer-Vertragsparteien des Protokolls

123. Artikel 14 Absatz 1 Buchstabe c des Protokolls lautet: „*Sind die übermittelnde Vertragspartei und die empfangende Vertragspartei nicht durch eine unter Buchstabe b bezeichnete Übereinkunft wechselseitig gebunden, können sie einvernehmlich bestimmen, dass die Übermittlung personenbezogener Daten nach diesem Protokoll statt auf der Grundlage der Absätze 2 bis 15 auf der Grundlage anderer Übereinkünfte oder Vereinbarungen zwischen den betreffenden Vertragsparteien erfolgen kann.*"[129]

124. Der EDSB begrüßt die aus ihren Erwägungen ersichtliche Absicht der Kommission, klarzustellen, dass die Mitgliedstaaten bei der Entscheidung, ob sie von den Bestimmungen in Artikel 14 Absatz 1 Buchstabe c des Protokolls Gebrauch machen könnten (um anstelle von Artikel 14 Absätze 2 bis 15 des Protokolls andere zwischen den Vertragsparteien vereinbarte Datenschutzbestimmungen auf die Übermittlung personenbezogener Daten auf Grundlage des Protokolls anzuwenden), an den unionsrechtlichen Rahmen gebunden sind, so wie sich dieser aus Kapitel V der DSGVO und der Strafverfolgungsrichtlinie ergibt.

125. Der EDSB würde jedoch **für den Fall, dass der Rat beschließt, die Mitgliedstaaten zur Unterzeichnung und Ratifizierung des Protokolls zu ermächtigen, empfehlen, diese Erwägung noch klarer zu formulieren**.

126. Insbesondere möchte er hervorheben, dass derartige Abkommen die Voraussetzungen erfüllen müssen, die jeweils in Kapitel V sowohl der DSGVO **als auch** der Strafverfolgungsrichtlinie niedergelegt sind.

127. In den Erwägungen ist unter anderem von der „*Übereinkunft oder Vereinbarung[, die] geeignete Datenschutzgarantien nach Artikel 46 der Datenschutz-Grundverordnung ... bietet*", die Rede.

128. Der EDSB möchte des Weiteren betonen, dass es ein wichtiges Ziel des Protokolls ist, in einer rechtlich bindenden völkerrechtlichen Übereinkunft angemessene Datenschutzgarantien vorzusehen, die für Diensteanbieter in der Union gelten, wenn sie auf Ersuchen von Behörden in Drittländern Daten übermitteln. Da im Protokoll die Formulierung „Übereinkünfte oder Vereinbarungen zwischen den betreffenden Vertragsparteien" verwendet wird, bittet der EDSB die Kommission um Erklärung, welche Übereinkünfte oder Vereinbarungen angemessene Datenschutzgarantien nach Artikel 46 der DSGVO vorsehen könnten, die für in

der Union ansässige Diensteanbieter oder Stellen, die Domänennamenregistrierungsdienste erbringen, gelten, wenn sie Übermittlungen an Behörden von Drittländer-Vertragsparteien des Protokolls vornehmen.

7. Schlussfolgerungen

129. Angesichts der starken Zunahme der Computerkriminalität und der zunehmenden Bedeutung elektronischen Beweismaterials für strafrechtliche Ermittlungen und im Hinblick auf die Komplexität der Einholung solchen Beweismaterials, wenn sich dieses nicht im Zuständigkeitsbereich des Mitgliedstaats befindet, hat der EDSB Verständnis dafür, dass es für die Strafverfolgungsbehörden zur Sicherstellung der wirksamen Kriminalitätsbekämpfung notwendig ist, elektronisches Beweismaterial schnell und wirksam einholen zu können.

130. Der EDSB spricht sich deshalb für ein internationales Vorgehen aus, das geeignete Garantien bezüglich der in diesem Zusammenhang bestehenden Problempunkte vorsieht.

131. Das Protokoll zielt darauf ab, sowohl die traditionellen Wege der Zusammenarbeit zu verbessern als auch die direkte Zusammenarbeit zwischen Strafverfolgungsbehörden und Dienstleistern im grenzüberschreitenden Kontext zu ermöglichen. Seine Bestimmungen sehen keinen direkten Zugang der Strafverfolgungsbehörden zu Daten vor, was der EDSB begrüßt.

132. Der EDSB erkennt an, dass es nicht möglich ist, die Terminologie und Definitionen des Unionsrechts in einer mehrseitigen internationalen Übereinkunft vollständig zu replizieren, betont jedoch, dass angemessene Datenschutzgarantien für natürliche Personen sichergestellt sein müssen, um dem Unionsrecht in vollem Umfang zu genügen.

133. Der EDSB hat sich davon überzeugt, dass das Protokoll einen eigenen Artikel über den Schutz personenbezogener Daten enthält. Des Weiteren nimmt er die zahlreichen Garantien, die in das Protokoll aufgenommen wurden, positiv zur Kenntnis.

134. Der EDSB versteht die Lage so, dass feststeht, dass auf Übermittlungen aus der EU in die Vereinigten Staaten von Amerika, die im Rahmen der im Protokoll enthaltenen Vorschriften über die behördliche Zusammenarbeit erfolgen, das Rahmenabkommen Anwendung fände. Der EDSB bedauert dies.

135. Für den Fall, dass ein Beschluss des Rates angenommen werden sollte, der die Mitgliedstaaten ermächtigt, das Protokoll im Interesse der Union zu unterzeichnen und zu ratifizieren, begrüßt der EDSB die Vorschläge der Kommission, dass die Mitgliedstaaten im Interesse der Union die Erklärung, Notifikation und Mitteilung gemäß Artikel 7 Absätze 2 Buchstabe b sowie Artikel 5 Buchstaben a und e des Protokolls abgeben. Diese Vorschläge stellen sicher, dass Diensteanbieter in der Union nur um die Übermittlung personenbezogener Daten ersucht werden können, wenn das Ersuchen auf einer Anordnung beruht, die im ersuchenden Drittland, das Vertragspartei des Protokolls ist, durch eine Staatsanwältin beziehungsweise durch einen Staatsanwalt oder eine andere Justizbehörde oder unter staatsanwaltlicher Aufsicht oder unter Aufsicht einer anderen Justizbehörde oder anderweitig unter unabhängiger Aufsicht erlassen wurde.

136. Er begrüßt es auch, dass den Mitgliedstaaten vorgeschlagen wird, die Erklärung gemäß Artikel 8 Absatz 4 des Protokolls (über die Zusammenarbeit zuständiger Behörden zur Erfüllung von Herausgabeanordnungen in Bezug auf Bestandsdaten und Verkehrsdaten)

abzugeben, um sicherzustellen, dass für die Erfüllung einer Anordnung nach dieser Vorschrift zusätzliche begleitende Angaben erforderlich sind.

137. Darüber hinaus gibt der EDSB für den Fall, dass das Protokoll von den Mitgliedstaaten im Interesse der Union unterzeichnet und ratifiziert werden sollte, folgende Empfehlungen für künftige Beschlüsse des Rates:

- Gewisse Daten, die unter die Kategorie „Bestandsdaten" im Sinne des Übereinkommens über Computerkriminalität fallen, gelten nach Unionsrecht unter Umständen als Verkehrsdaten, bei denen ein schwerer Eingriff in die Grundrechte des Betroffenen gegeben sein kann, weshalb der Zugang zu diesen Daten nur zur Bekämpfung von schwerer Kriminalität gerechtfertigt sein kann. Der EDSB empfiehlt den Mitgliedstaaten deshalb, sich – entgegen den Vorschlägen der Kommission – das Recht auf Nichtanwendung von Artikel 7 des Protokolls vorzubehalten, der in Artikel 7 Absatz 9 Buchstabe b für bestimmte Arten von Zugangsnummern die direkte Weitergabe von Bestandsdaten von Diensteanbietern an zuständige Behörden eines anderen Landes vorsieht.

- Die Mitgliedstaaten sollten gemäß Artikel 7 Absatz 5 Buchstabe e des Protokolls eine Justiz- oder sonstigen unabhängige Behörde benennen.

- Die vorgeschlagene Mitteilung, die die Mitgliedstaaten bei Unterzeichnung oder bei Hinterlegung der Ratifikations-, Annahme- oder Genehmigungsurkunde an die Behörden der Vereinigten Staaten bezüglich des Rahmenabkommens zwischen der EU und den USA übermitteln, sollte klarer formuliert werden.

- Die vorgeschlagene Erwägung in Bezug auf sonstige Vereinbarungen oder Verträge gemäß Artikel 14 Absatz 1 Buchstabe c des Protokolls, die die Datenschutzbestimmung des Protokolls (Artikel 14) ersetzen könnten, sollte abgeändert werden.

138. Abschließend hebt der EDSB hervor, dass es einer Staatsanwaltschaft eines Mitgliedstaats und somit auch der EUStA nur dann möglich sein sollte, eine Anordnung zu erlassen oder Daten auf Anordnung einer anderen Vertragspartei gemäß Artikel 8 zu übermitteln, wenn sichergestellt ist, dass die betreffende Anordnung der Überprüfung durch eine Justizbehörde oder eine unabhängige Stelle im Sinne der Rechtsprechung des EuGH unterliegt.

139. Der EDSB steht der Kommission, dem Rat und dem Europäischen Parlament in den weiteren Phasen dieses Verfahrens weiterhin beratend zur Verfügung. Diese Stellungnahme lässt etwaige zusätzliche Anmerkungen, die der EDSB auf der Grundlage weiterer, in Zukunft verfügbarer Informationen abgeben könnte, unberührt.

Brüssel, den 20. Januar 2022

[elektronisch unterzeichnet]
Wojciech Rafał WIEWIÓROWSKI

Endnoten

[1] ABl. L 119 vom 4.5.2016, S. 1.
[2] ABl. L 295 vom 21.11.2018, S. 39.
[3] ABl. L 119 vom 4.5.2016, S. 89.
[4] https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690
[5] 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.
[6] https://rm.coe.int/1680a49dab (vom Ministerkomitee genehmigte vorläufige Fassung).
[7] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561
[8] Stellungnahme 3/2019 des EDSB vom 2. April 2019 zu der Teilnahme an den Verhandlungen mit Blick auf ein Zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität.
[9] Beschluss des Rates vom 6. Juni 2019 zur Genehmigung der Teilnahme der Europäischen Kommission an Verhandlungen über ein Zweites Zusatzprotokoll zum Übereinkommen des Europarats über Computerkriminalität (SEV Nr. 185).
[10] „EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) of 13. November 2019"; „Stellungnahme 02/2021 zum neuen Entwurf von Bestimmungen des Zweiten Zusatzprotokolls zum Übereinkommen des Europarats über Computerkriminalität (Budapester Übereinkommen), angenommen am 2. Februar 2021"; „EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime" vom 4. Mai 2021.
[11] Entschließung des Europäischen Parlaments vom 10. Juni 2021 zu der Cybersicherheitsstrategie der EU für die digitale Dekade.
[12] Artikel 21 des Protokolls.
[13] Erwägungsgrund 10 der Vorschläge für einen Beschluss des Rates zur Ermächtigung der Mitgliedstaaten, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials zu unterzeichnen bzw. zu ratifizieren.
[14] Vorschlag für einen Beschluss des Rates zur Ermächtigung der Mitgliedstaaten, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials zu unterzeichnen (COM(2021)718 final).
Vorschlag für einen Beschluss des Rates zur Ermächtigung der Mitgliedstaaten, im Interesse der Europäischen Union das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität über eine verstärkte Zusammenarbeit und die Weitergabe elektronischen Beweismaterials zu ratifizieren (COM(2021)719 final).
Aus den Erwägungsgründen 14 und 15 des Vorschlags bezüglich der Unterzeichnung und den Erwägungsgründen 13 und 14 des Vorschlags bezüglich der Ratifizierung geht hervor, dass Irland die Option hat, sich an der Annahme und Anwendung des Beschlusses zu beteiligen, und dass sich Dänemark nicht an der Annahme dieses Beschlusses beteiligt, der daher weder für Dänemark bindend noch Dänemark gegenüber anwendbar ist.
[15] Erwägungsgrund 3 des Vorschlags.
[16] Artikel 16 Absatz 1: „... [die Vertragsparteien] können ihre Zustimmung, gebunden zu sein, ausdrücken,
a. indem sie es ohne Vorbehalt der Ratifikation, Annahme oder Genehmigung unterzeichnen oder
b. indem sie es vorbehaltlich der Ratifikation, Annahme oder Genehmigung unterzeichnen und später ratifizieren, annehmen oder genehmigen".
2. Die Ratifikations-, Annahme- oder Genehmigungsurkunden werden bei der Generalsekretärin beziehungsweise dem Generalsekretär des Europarats hinterlegt.
[17] Alle außer der Republik Irland, die das Übereinkommen zwar unterzeichnet, aber nicht ratifiziert hat, jedoch entschlossen ist, den Beitritt zu verfolgen.
[18] 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
[19] Vgl. Artikel 23 bis 35 des Übereinkommens über Computerkriminalität.
[20] https://rm.coe.int/1680a49c9d, so wie vom Ministerkomitee am 17. November 2021 mitgeteilt.
[21] Vgl. Nummer 2 des erläuternden Berichts zum Protokoll.
[22] Der Begriff „Bestandsdaten" im Sinne von Artikel 18 Absatz 3 des Übereinkommens über Computerkriminalität bezeichnet „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".

[23] Nach dem Übereinkommen über Computerkriminalität sind „Verkehrsdaten" alle Computerdaten in Zusammenhang mit einer Kommunikation, unter Nutzung eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette ist, erzeugt wurden und aus denen der Ursprung, das Ziel, der Leitweg, die Uhrzeit, das Datum, der Umfang oder die Dauer der Kommunikation oder die Art des für die Kommunikation benutzten Dienstes hervorgeht.

[24] Nach dem Übereinkommen über Computerkriminalität bezeichnet der Begriff „Computerdaten" jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form einschließlich eines Programms, das die Ausführung einer Funktion durch ein Computersystem auslösen kann;

[25] Nummer 172 des erläuternden Berichts: „Weil Artikel 10 dieses Protokolls auf Notfälle beschränkt ist, in denen solche umgehenden Eilmaßnahmen gerechtfertigt sind, unterscheidet er sich von Artikel 25 Absatz 3 des Übereinkommens, der in dringenden Fällen, die jedoch nicht den Tatbestand eines Notfalls im Sinne der Definition erfüllen, die Übersendung von Rechtshilfeersuchen durch schnelle Kommunikationsmittel gestattet. Anders gesagt, ist Artikel 25 Absatz 3 insofern weiter gefasst als Artikel 10 dieses Protokolls, als er auch Situationen erfasst, die nicht unter Artikel 10 fallen; etwa bestehende, jedoch nicht unmittelbar drohende Gefahren für das Leben oder die Sicherheit von Personen, die Gefahr der Beweisvernichtung im Falle des Verzugs, das unmittelbare Bevorstehen von Verhandlungsterminen oder andere Arten von Eilfällen. Während die in Artikel 25 Absatz 3 getroffene Regelung schnellere Mittel für die Übersendung und Beantwortung von Ersuchen vorsieht, sind die Verpflichtungen in einem Notfall gemäß Artikel 10 dieses Protokolls bedeutend größer; das heißt, dass das Verfahren in Fällen erheblicher und unmittelbarer Gefahr für das Leben oder die Sicherheit einer natürlichen Person noch schleuniger sein sollte (vgl. die in Nummer 42 dieses erläuternden Berichts angegebenen Beispiele für Notfälle)."

[26] In den Nummern 77 und 169 des erläuternden Berichts.

[27] „Einer Vertragspartei, die einen Vorbehalt zu diesem Artikel erklärt, ist es nicht gestattet, gemäß Absatz 1 Diensteanbietern in Hoheitsgebieten anderer Vertragsparteien vorzulegende Anordnungen zu erlassen", erläuternder Bericht, Nummern 122 und 123.

[28] „Einer Vertragspartei, die einen Vorbehalt zu diesem Artikel erklärt, ist es nicht gestattet, gemäß Absatz 1 anderen Vertragsparteien vorzulegende Anordnungen in Bezug auf Verkehrsdaten zu erlassen", erläuternder Bericht, Nummer 147.

[29] Anhang, Abschnitt 1.

[30] Anhang, Abschnitte 2 und 3.

[31] EDSA-EDSB, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, 10. Juli 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[32] EuGH, Rechtssache C-181/73, Haegemann / Belgischer Staat, ECLI:EU:C:1974:41, Rn. 5.

[33] EuGH, Rechtssache C-308/06, Intertanko u.a., ECLI:EU:C:2008:312, Rn. 42.

[34] Verbundene Rechtssachen C-402/05 P und C-415/05 P, Kadi / Rat und Kommission, ECLI:EU:C:2008:461, Rn. 285.

[35] Entweder als Teil von Ersuchen und Anordnungen der Mitgliedstaaten oder in Erledigung derartiger Ersuchen und Anordnungen.

[36] Zur Erledigung von Ersuchen oder Anordnungen gemäß den Artikeln 6 und 7 des Protokolls.

[37] Nummer 99 des erläuternden Berichts stellt klar, dass „in Artikel 7 der Begriff ‚Diensteanbieter im Hoheitsgebiet einer anderen Vertragspartei' voraussetzt, dass der Diensteanbieter über eine physische Präsenz in der anderen Vertragspartei verfügt. Nach diesem Artikel würde der bloße Umstand, dass ein Diensteanbieter zum Beispiel in einem Vertragsverhältnis zu einer Gesellschaft in einer Vertragspartei steht, ohne dass jedoch der Diensteanbieter selbst physisch in der Vertragspartei präsent wäre, nicht bedeuten, dass der Diensteanbieter „im Hoheitsgebiet einer anderen Vertragspartei" wäre. Absatz 1 erfordert darüber hinaus, dass sich die Daten im Besitz oder unter der Kontrolle des Diensteanbieters befinden." Vgl. auch Nummer 77 des erläuternden Berichts zu Artikel 6.

[38] 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).

[39] 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, ABl. L 119 vom 4.5.2016, S. 1.

[40] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592.

[41] Ebd., Nummer 214.

[42] Rechtssache C-362/14, Schrems, ECLI:EU:C:2015:650, Rn. 95.

[43] Siehe Nummer 76 des erläuternden Berichts: „Artikel 6 hat das Ziel, einen wirksamen und effizienten Rahmen für die Einholung von Informationen zur Identifizierung oder zum Kontaktieren des Domaininhabers vorzugeben. Die Form der Durchführung hängt von den jeweiligen rechtlichen und politischen Erwägungen der Vertragsparteien ab. Dieser Artikel soll die derzeitigen und künftigen Politiken und Praktiken im Bereich der Internet-Governance ergänzen."

[44] Nummer 100.
[45] Vgl. z. B., wenngleich es an einer internationalen Übereinkunft fehlt, EDSA-EDSB, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, 10. Juli 2019.
[46] Artikel 6 Absatz 2 des Protokolls und Nummer 82 des erläuternden Berichts; Artikel 7 Absatz 1 des Protokolls und Nummer 100 des erläuternden Berichts.
[47] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Straßburg, 28. Januar 1981, SEV Nr. 108 (im Folgenden „Übereinkommen Nr. 108").
[48] Siehe diesbezüglich Artikel 29 – Datenschutzgruppe, Stellungnahme 4/2001 zum Entwurf einer Konvention des Europarats über Cyberkriminalität vom 22. März 2001 (5001/01/DE/ endg. WP 41), S. 6: „Zudem sollte von den Unterzeichnern verlangt werden, dass sie der Konvention 108 des Europarats beitreten …" Insbesondere hat sich herausgestellt, dass nicht alle Drittländer-Vertragsparteien des Übereinkommens über Computerkriminalität auch Vertragsparteien des Übereinkommens Nr. 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 Nr. 108, das so genannte Übereinkommen Nr. 108+, ist noch nicht wirksam geworden. Es ist von 26 Mitgliedstaaten unterzeichnet und von 11 Mitgliedstaaten ratifiziert worden – siehe Unterschriften und Ratifikationsstand des Übereinkommens Nr. 108+: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures
[49] Andorra, Argentinien, Kanada, Israel, Japan, Vereinigtes Königreich und Schweiz.
[50] Nummer 220 des erläuternden Berichts.
[51] Unbeschadet der Bedingungen und Gründe, bei deren Vorliegen die ersuchte Vertragspartei zur Ablehnung berechtigt ist (siehe unten).
[52] Hervorhebung nur hier.
[53] Artikel 15 des Übereinkommens über Computerkriminalität lautet: „Jede Vertragspartei stellt sicher, dass für die Schaffung, Umsetzung und Anwendung der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren Bedingungen und Garantien ihres innerstaatlichen Rechts gelten, die einen angemessenen Schutz der Menschenrechte und Freiheiten einschließlich der Rechte vorsehen, die sich aus ihren Verpflichtungen nach dem Übereinkommen des Europarats von 1950 zum Schutz der Menschenrechte und Grundfreiheiten,
dem Internationalen Pakt der Vereinten Nationen von 1966 über bürgerliche und politische Rechte und anderen anwendbaren völkerrechtlichen Übereinkünften auf dem Gebiet der Menschenrechte ergeben und **zu denen der Grundsatz der Verhältnismäßigkeit gehören muss**.
2 Diese Bedingungen und Garantien umfassen, soweit dies in Anbetracht der Art der betreffenden Befugnis oder des betreffenden Verfahrens angebracht ist, unter anderem eine gerichtliche oder sonstige unabhängige Kontrolle, eine Begründung der Anwendung sowie die Begrenzung des Umfangs und der Dauer der Befugnis oder des Verfahrens.
3 Soweit es mit dem öffentlichen Interesse, insbesondere mit einer geordneten Rechtspflege, vereinbar ist, berücksichtigt jede Vertragspartei die Auswirkungen der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren auf die Rechte, Verantwortlichkeiten und berechtigten Interessen Dritter." (Hervorhebung nur hier)
[54] Nummer 231 des erläuternden Berichts.
[55] Hervorhebung nur hier.
[56] Siehe Ausführungen zu Artikel 2 in Abschnitt 4.3.1.
[57] Siehe Nummer 97 des erläuternden Berichts. Dies ergibt sich auch aus Artikel 7 Absatz 1, wo von „bestimmten" Informationen die Rede ist, sowie Artikel 8 Absatz 1 und Artikel 9 Absatz 1, in denen der Begriff „spezifische" Informationen verwendet wird.
[58] Vgl. z. B. diesbezüglich:
- Artikel 6 Absatz 3 Buchstabe c, Artikel 7 Absatz 1 und Artikel 8 Absatz 1, wo von „benötigten" bzw. „erforderlichen" Informationen die Rede ist, sowie den erläuternden Bericht, insbesondere die Nummern 82, 84 und 97.
- Artikel 8, Nummer 129 des erläuternden Berichts, wo klargestellt wird, dass der Mechanismus, durch den der Diensteanbieter gezwungen wird, die Informationen herauszugeben, den Bestimmungen des Rechts der ersuchten Vertragspartei unterliegt, da sich die Herausgabe nach den Verfahren der ersuchten Vertragspartei richtet. „Deshalb kann die ersuchte Vertragspartei sicherstellen, dass ihr eigenes Recht, einschließlich der sich aus ihrem Verfassungsrecht und den Menschenrechten ergebenden Anforderungen, eingehalten wird, insbesondere in Bezug auf zusätzliche Garantien, einschließlich derjenigen, die für die Herausgabe von Verkehrsdaten erforderlich sind."
[59] Angemessene Bedingungen des innerstaatlichen Rechts der ersuchten Vertragspartei gemäß Artikel 6 Absatz 2 sowie jegliche Bedingungen gemäß Artikel 9 Absatz 6, die auf jeden Fall nicht bindende Ersuchen vorsehen (vgl. auch Nummern 77, 82 und 169 des erläuternden Berichts zum Protokoll). Außerdem kann die ersuchte Vertragspartei gemäß Artikel 8 Absatz 7 angeben, unter welchen Bedingungen sie das Ersuchen erledigen könnte. Vgl. auch in Artikel 8 Absatz 8 und Artikel 10 Absatz 7 des Protokolls die sich aus Artikel 28 Absatz 2 Buchstabe b des Übereinkommens über Computerkriminalität ergebende Bedingung (Bedingung, die Informationen nicht für andere als die in dem Ersuchen genannten Ermittlungen oder Verfahren zu verwenden) sowie in Artikel 7 Absatz 5 Buchstabe c Ziffer ii, Artikel 8 Absätze 8 und 10 des Protokolls (vgl. Nummer 173 des erläuternden Berichts) die sich aus Artikel 25 Absatz 4 des Übereinkommens über Computerkriminalität ergebenden Bedingungen, wonach die Rechtshilfe den im Recht der ersuchten Vertragspartei oder in den anwendbaren Rechtshilfeverträgen vorgesehenen Bedingungen unterliegt.

[60] Nummer 269 des erläuternden Berichts zum Übereinkommen über Computerkriminalität stellt klar, dass nach Artikel 27 Absatz 4 die „Verweigerung der Rechtshilfe aus Datenschutzgründen nur in Ausnahmefällen in Betracht kommt. Eine derartige Situation könnte sich ergeben, wenn nach Abwägung der in einem gegebenen Fall zu berücksichtigenden wichtigen Interessen (zum einen des öffentlichen Interesses, wozu auch eine ordnungsgemäße Rechtspflege gehört, und zum anderen des Interesses des Schutzes der Privatsphäre) die ersuchte Vertragspartei zu der Auffassung gelangt, dass die Übermittlung der von der ersuchenden Vertragspartei angeforderten spezifischen Daten so grundlegende Probleme aufwerfen würde, dass der Tatbestand der Ablehnung wegen Beeinträchtigung wesentlicher Interessen erfüllt ist. Es ist deshalb ausgeschlossen, sich allgemein, kategorisch oder systematisch auf die Datenschutzgrundsätze zu stützen, um die Zusammenarbeit zu verweigern. Folglich stellt der Umstand, dass die Vertragsparteien verschiedene Datenschutzsysteme haben (dass etwa die ersuchende Vertragspartei keine Stelle hat, die einer spezialisierten Datenschutzbehörde gleichwertig ist) oder dass sie personenbezogene Daten auf unterschiedliche Weise schützen (dass etwa die ersuchende Vertragspartei den Schutz der Privatsphäre oder der Richtigkeit der von Strafverfolgungsbehörden empfangenen personenbezogenen Daten auf andere Weise als durch Löschung bewirkt), für sich genommen keinen Ablehnungsgrund dar. Bevor sie die Zusammenarbeit auf ‚wesentliche Interessen' gestützt verweigert, sollte die ersuchte Vertragspartei vielmehr versuchen, Bedingungen anzugeben, unter denen die Übermittlung der Daten möglich wäre" (Hervorhebung nur hier). Solche Ablehnungsgründe sind vorgesehen in:
- Artikel 7 Absatz 5 Buchstabe c Ziffer ii (direkte Zusammenarbeit mit Diensteanbietern bezüglich der Herausgabe von Bestandsdaten), sofern die ersuchte Vertragspartei von der Möglichkeit, ihre Behörde zu konsultieren, Gebrauch gemacht hat – dies ist es, was die Kommission den Mitgliedstaaten im Anhang vorschlägt;
- Artikel 8 Absatz 8 (Zusammenarbeit der Behörden bei der umgehenden Herausgabe von Bestandsdaten und Verkehrsdaten);
- Artikel 10 Absatz 7 (Rechtshilfe in Notfällen)
Vgl. des Weiteren die Ablehnungsgründe in Artikel 7 Absatz 5 Buchstabe c Ziffer ii, Artikel 8 Absätze 8 und 10 des Protokolls (vgl. Nummer 173 des erläuternden Berichts) die sich aus Artikel 25 Absatz 4 des Übereinkommens über Computerkriminalität ergeben, wonach die Rechtshilfe den im Recht der ersuchten Vertragspartei oder in den anwendbaren Rechtshilfeverträgen vorgesehenen Bedingungen unterliegt, einschließlich der Gründe, die die ersuchte Vertragspartei zur Verweigerung der Zusammenarbeit geltend machen kann.
[61] Hervorhebung nur hier.
[62] Zum Grundsatz der Verhältnismäßigkeit siehe Abschnitt 4.2.
[63] Nummer 221 des erläuternden Berichts stellt klar, dass „jede Vertragspartei personenbezogene Daten, die sie gemäß diesem Protokoll empfängt, gemäß den spezifischen Garantien verarbeitet, die in den Absätzen 2 bis 15 niedergelegt sind. Dazu zählen auch personenbezogene Daten, die als Teil auf das Protokoll gestützter Anordnungen oder Ersuchen übermittelt werden."
[64] Hinsichtlich Weitergabe und Weiterübermittlung siehe unten.
[65] Siehe auch die eingehenden Ausführungen unter Nummern 227 ff. im erläuternden Bericht dazu, was einen Zweck darstellen könnte, der nicht vereinbar wäre.
[66] Nummer 228: „Der rechtliche Rahmen einer Vertragspartei kann weitere besondere Beschränkungen hinsichtlich der Zwecke vorsehen, zu denen die Daten verwendet werden dürfen."
[67] Artikel 13 und Nummer 218 des erläuternden Berichts
[68] Siehe oben zur Auslegung „erheblich ... und nicht darüber hinausgehen[d]".
[69] Gemäß Artikel 3 Absatz 1 Buchstabe e des Protokolls bezeichnet „übermittelnde Vertragspartei" die Vertragspartei, die die Daten im Rahmen der Erledigung eines Ersuchens oder einer gemeinsamen Ermittlungsgruppe übermittelt, oder, für die Zwecke von Kapitel II Abschnitt 2, eine Vertragspartei, in deren Hoheitsgebiet sich ein übermittelnder Diensteanbieter oder eine Stelle, die Domänennamenregistrierungsdienste bereitstellt, befindet.
[70] Hervorhebung nur hier.
[71] Erläuternder Bericht, Nummer 230.
[72] Nummer 230.
[73] Artikel 6 Absatz 3 Buchstabe d, Artikel 7 Absatz 4 Buchstabe f, Artikel 8 Absatz 3 und Artikel 9 Absatz 3 Buchstabe g, Nummern 84, 105, 106, 131, 135 und 165 des erläuternden Berichts sowie Artikel 10 Absatz 7 in Verbindung mit Artikel 27 Absatz 3 des Übereinkommens über Computerkriminalität.
[74] Artikel 6 Absatz 3 Buchstabe c, Artikel 8 Absatz 8 und Artikel 10 Absatz 7.
[75] Siehe Nummer 71.
[76] Nummer 111.
[77] Gemäß Artikel 7 Absatz 5 Buchstabe d können die benachrichtigten Behörden des ersuchten Staates für die Zwecke der Anweisung an den Diensteanbieter, die Bestandsdaten nicht weiterzugeben, die Behörde in der ersuchenden Vertragspartei, an die der Diensteanbieter die Bestandsdaten senden oder der er in sonstiger Weise erwidern soll, um zusätzliche Informationen ersuchen, und zusätzliche Informationen, die sie empfangen, dürfen sie ohne die Zustimmung der betreffenden Behörde nicht an den Diensteanbieter weitergeben. Wird der Diensteanbieter angewiesen, die Bestandsdaten nicht weiterzugeben, sind die Behörden des ersuchten Staates auch verpflichtet, die ersuchende Behörde umgehend unter Darlegung der Gründe darüber zu unterrichten.
[78] Nummer 71.

[79] Nummern 241 und 242.
[80] Nummer 234.
[81] Artikel 5 Absatz 1 Buchstabe f DSGVO und Artikel 4 Absatz 1 Buchstabe f der Strafverfolgungsrichtlinie.
[82] Nummer 246-247.
[83] Artikel 6 Absatz 4, Artikel 7 Absatz 6, Artikel 8 Absatz 5, Artikel 9 Absatz 4 und Artikel 10 Absatz 2 sowie die Nummern 86, 116 und 174 des erläuternden Berichts.
[84] Nummer 258.
[85] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 141.
[86] Hervorhebung nur hier.
[87] Hervorhebung nur hier.
[88] Dies ist, was angeforderte Informationen betrifft, in Verbindung mit dem in Kapitel II und Artikel 13 verankerten Grundsatz der Zweckbindung zu lesen: Vgl. insbesondere oben Abschnitt 4.2 über den Grundsatz der Verhältnismäßigkeit und Abschnitt 4.3.1 über Zweckbindung und Datenminimierung.
[89] Nummer 248.
[90] Siehe Fußnote 59.
[91] Vgl. die obigen Abschnitte über den Grundsatz der Verhältnismäßigkeit sowie über Zweckbindung und Datenminimierung.
[92] Vgl. die Abschnitte über den Grundsatz der Verhältnismäßigkeit sowie über Zweckbindung und Datenminimierung, insbesondere Fußnote 60.
[93] Artikel 6 Absatz 3 Buchstabe d, Artikel 7 Absatz 4 Buchstabe f, Artikel 8 Absatz 3 und Artikel 9 Absatz 3 Buchstabe g, Nummern 84, 105, 106, 131, 135 und 165 des erläuternden Berichts sowie Artikel 10 Absatz 7 in Verbindung mit Artikel 27 Absatz 3 des Übereinkommens über Computerkriminalität.
[94] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Nr. 141.
[95] Nummer 245.
[96] Siehe oben Abschnitt 4.3.6.
[97] Siehe unten.
[98] Nummer 111.
[99] Artikel 6 Absatz 3 Buchstabe d, Artikel 7 Absatz 4 Buchstabe f, Artikel 8 Absatz 3 und Artikel 9 Absatz 3 Buchstabe g, Nummern 84, 105, 106, 131, 135 und 165 des erläuternden Berichts sowie Artikel 10 Absatz 7 in Verbindung mit Artikel 27 Absatz 3 des Übereinkommens über Computerkriminalität.
[100] Vgl. Rechtssache C-518/07, Kommission / Deutschland, EU:C:2010:125, Randnummer 25; Rechtssache C-288/12, Kommission / Ungarn, EU:C:2014:237, Randnummer 48.
[101] Nummer 322.
[102] Artikel 7 Absatz 5 Buchstabe c Ziffer ii, Artikel 8 Absatz 8 und Artikel 10 Absatz 7.
[103] Artikel 6 Absatz 2 und Artikel 9 Absatz 6.
[104] Artikel 25 – Allgemeine Grundsätze der Rechtshilfe – Absatz 4: „Soweit in den Artikeln dieses Kapitels nicht ausdrücklich etwas anderes vorgesehen ist, unterliegt die Rechtshilfe den im Recht der ersuchten Vertragspartei oder in den anwendbaren Rechtshilfeverträgen vorgesehenen Bedingungen einschließlich der Gründe, aus denen die ersuchte Vertragspartei die Zusammenarbeit ablehnen kann. Die ersuchte Vertragspartei darf das Recht auf Verweigerung der Rechtshilfe in Bezug auf die in den Artikeln 2 bis 11 bezeichneten Straftaten nicht allein mit der Begründung ausüben, dass das Ersuchen eine Straftat betrifft, die von ihr als fiskalische Straftat angesehen wird.“ Bei den in den Artikeln 2 bis 11 des Übereinkommens aufgeführten Straftaten handelt es sich um Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und Computersystemen, computer- und contentbezogene Straftaten, Straftaten im Zusammenhang mit der Verletzung von Urheberrechten und verwandten Schutzrechten sowie Beihilfe bei oder Anstiftung zu diesen Straftaten und den Versuch der Begehung gewisser anderer im Übereinkommen vorgesehener Straftaten.
Artikel 27 – Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte – Absatz 4: „Zusätzlich zu den Ablehnungsgründen nach Artikel 25 Absatz 4 kann die ersuchte Vertragspartei die Rechtshilfe verweigern, wenn
a das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als politische oder als mit einer solchen zusammenhängende Straftat angesehen wird, oder
b sie der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung (ordre public) oder andere wesentliche Interessen zu beeinträchtigen.“
[105] Gemäß Artikel 3 Absatz 2 Buchstabe b des Protokolls bezeichnet der Begriff „‚zuständige Behörde‘ … eine Justiz-, Verwaltungs- oder sonstige Strafverfolgungsbehörde, die nach innerstaatlichem Recht ermächtigt ist, Maßnahmen im Sinne dieses Protokolls für Zwecke der Erhebung oder Herausgabe von Beweismaterial in Bezug auf spezifische strafrechtliche Ermittlungen oder Verfahren anzuordnen, zu bewilligen oder durchzuführen“.
[106] EuGH, verbundene Rechtssachen C-203/15 und C-698/15, Tele2 Sverige, ECLI:EU:C:2016:970, Rn. 120.
[107] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238, Rn. 62.
[108] Artikel 5 Absatz 6 des Protokolls und Nummer 69 des erläuternden Berichts.
[109] Nummer 93 des erläuternden Berichts zum Protokoll.
[110] EuGH, verbundene Rechtssachen C-203/15 und C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970, Rn 99.

[111] EuGH, verbundene Rechtssachen C-203/15 und C-698/15, Tele2 Sverige, ECLI:EU:C:2016:970, Rn. 120.
[112] Rechtssache C-746/18, Prokuratuur, ECLI:EU:C:2021:152, Urteilstenor: „2. Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte dahin auszulegen, dass er einer nationalen Regelung entgegensteht, wonach die Staatsanwaltschaft, deren Aufgabe darin besteht, das strafrechtliche Ermittlungsverfahren zu leiten und gegebenenfalls in einem späteren Verfahren die öffentliche Klage zu vertreten, dafür zuständig ist, einer Behörde für strafrechtliche Ermittlungen Zugang zu Verkehrs- und Standortdaten zu gewähren."
[113] Rechtssache C-201/14, Bara u. a., ECLI:EU:C:2015:638, Rn. 33: „[Das] Erfordernis einer Unterrichtung der von der Verarbeitung ihrer personenbezogenen Daten betroffenen Personen [ist] umso wichtiger, als es die Voraussetzung dafür schafft, dass sie ihr in Art. 12 der Richtlinie 95/46 festgelegtes Auskunfts- und Berichtigungsrecht in Bezug auf die verarbeiteten Daten und ihr in Art. 14 der Richtlinie geregeltes Recht, der Verarbeitung der Daten zu widersprechen, ausüben können."
[114] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 220 [Hervorhebung nur hier].
[115] Artikel 14 Absatz 11 Buchstabe c des Protokolls.
[116] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 219.
[117] Erläuternder Bericht, Nummer 276.
[118] Rechtssache C-362/14, Schrems, ECLI:EU:C:2015:650, Rn. 95.
[119] Ebd., Randnummer 95 (Hervorhebung nur hier).
[120] Ebd., Randnummern 56 bis 58.
[121] Rechtssache C-518/07, Kommission / Deutschland, ECLI:EU:C:2010:125, Rn. 25; Rechtssache C-614/10, Kommission / Österreich, ECLI:EU:C:2012:631, Rn. 36 und 37; Rechtssache C-288/12, Kommission / Ungarn, Rn. 48.
[122] Gutachten 1/15, EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Randnummern 229 und 230.
[123] Nummer 278 ff.
[124] Nummer 281.
[125] Nummer 222.
[126] Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten, ABl. L 336 vom 10.12.2016, S. 3, (im Folgenden „Rahmenabkommen"). Das am 1. Februar 2017 in Kraft getretene Rahmenabkommen legt den Rahmen für den Schutz personenbezogener Daten fest, die zwischen der EU und den USA für Strafverfolgungszwecke ausgetauscht werden.
[127] Vgl. EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection.
[128] Stellungnahme 7/2019 des EDSB zu den Vorschlägen über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen.
[129] Hervorhebung nur hier.