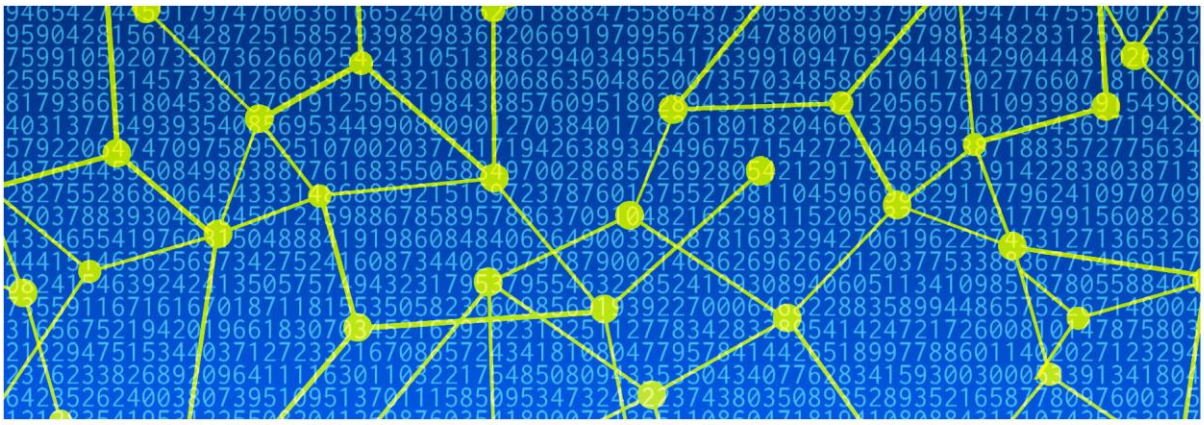

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 7/2019

Stellungnahme des EDSB zu den Vorschlägen über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen

EDPS

6. November 2019

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 52 Absatz 2 der Verordnung 2018/1725 im „Hinblick auf die Verarbeitung personenbezogener Daten [...] sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Datenschutz, von den Organen und Einrichtungen der Union geachtet werden"; er ist gemäß Artikel 52 Absatz 3 „für die Beratung der Organe und Einrichtungen der Union und der betroffenen Personen in allen Fragen der Verarbeitung personenbezogener Daten" zuständig. Nach Artikel 58 Absatz 3 Buchstabe c der Verordnung 2018/1725 hat der EDSB die Befugnis, „zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an die Organe und Einrichtungen der Union sowie an die Öffentlichkeit zu richten".

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

In dieser Stellungnahme geht es um den Auftrag des EDSB, die EU-Organe bezüglich der Datenschutzauswirkungen ihrer Politiken zu beraten und eine verantwortliche Politikgestaltung zu fördern, im Einklang mit Maßnahme 9 der Strategie des EDSB: „Förderung einer verantwortungsvollen und fundierten politischen Entscheidungsfindung". Der EDSB unterstützt das Ziel, den grenzüberschreitenden Zugang zu elektronischen Beweismitteln effizienter zu gestalten, betont aber die Notwendigkeit, die von der Kommission vorgelegten Gesetzgebungsvorschläge zu verbessern, um die Achtung der Grundrechte und die Erfüllung der Datenschutzauflagen zu gewährleisten. Beide Aspekte sind wesentlich, um einen funktionierenden Rahmen für die Europäischen Herausgabe- und Sicherungsanordnungen für das Erheben von elektronischen Beweismitteln in Strafsachen zu schaffen.

Zusammenfassung

Im April 2018 legte die Kommission zwei Vorschläge – einen für eine Verordnung und einen für eine Richtlinie – vor, um einen Rechtsrahmen zu schaffen, der die Sicherung von und den Zugang zu elektronischen Beweismitteln in grenzüberschreitenden Fällen für die Polizei und die Justizbehörden erleichtert und beschleunigt. Seitdem hat der Rat allgemeine Ausrichtungen zu den Vorschlägen festgelegt und das Europäische Parlament hat mehrere Arbeitsunterlagen erarbeitet. Der Europäischer Datenschutzausschuss legte seine Stellungnahme vor. Auf internationaler Ebene haben sich Entwicklungen ergeben, insbesondere durch die Aufnahme von Verhandlungen über ein internationales Übereinkommen mit den Vereinigten Staaten über den Zugang zu elektronischen Beweismitteln auf grenzüberschreitender Ebene und Arbeiten an einem zweiten Zusatzprotokoll zum Übereinkommen über Computerkriminalität. Mit der vorliegenden Stellungnahme beabsichtigt der EDSB, dem Unionsgesetzgeber unter Berücksichtigung der vorstehend aufgeführten Entwicklungen einen neuen Beitrag für die bevorstehenden Arbeiten an den Vorschlägen zur Verfügung zu stellen.

In der heutigen, von neuen Technologien veränderten Welt ist die Zeit oft ein entscheidender Faktor, um diesen Behörden das Einholen von Daten zu ermöglichen, die zur Erfüllung ihrer Aufträge unabdingbar sind. Gleichzeitig finden sich die Strafverfolgungsbehörden auch bei Ermittlungen in nationalen Fällen zunehmend allein deshalb in „grenzüberschreitenden Situationen“ wieder, weil ein ausländischer Diensteanbieter involviert war und die Daten in einem anderen Mitgliedstaat elektronisch gespeichert sind. Der EDSB **unterstützt das Ziel**, sicherzustellen, dass den Strafverfolgungsbehörden wirksame Instrumente zur Verfügung stehen, um Straftaten zu ermitteln und zu verfolgen. Er begrüßt insbesondere das Ziel der Vorschläge, den Zugang zu Daten in grenzüberschreitenden Fällen durch Straffung der Verfahren innerhalb der EU zu beschleunigen und zu erleichtern.

Gleichzeitig möchte der EDSB betonen, dass alle Initiativen auf diesem Gebiet **in vollem Umfang der Charta der Grundrechte der Europäischen Union und dem EU-Datenschutzrahmen Rechnung tragen** müssen und dass **das Bestehen ausreichender Garantien** unbedingt gewährleistet werden muss. Der wirksame Schutz der Grundrechte im Prozess der grenzüberschreitenden Erhebung von elektronischen Beweismitteln erfordert insbesondere **eine stärkere Beteiligung der Justizbehörden im vollstreckenden Mitgliedstaat**. Sie sollten so früh wie möglich an diesem Prozess systematisch beteiligt werden, die Möglichkeit haben, die Vereinbarkeit der Anordnungen mit der Charta zu prüfen, und die Pflicht haben, auf dieser Grundlage Ablehnungsgründe geltend zu machen.

Zudem sollten die **Definitionen der Datenkategorien** im Verordnungsvorschlag präzisiert und ihre Vereinbarkeit mit anderen Definitionen von Datenkategorien im Unionsrecht sollte sichergestellt werden. Er empfiehlt zudem die Neubewertung des Verhältnisses zwischen den **Arten von Straftaten,** bei denen Europäische Herausgabeanordnungen erlassen werden könnten, und den betreffenden **Datenkategorien** im Hinblick auf die einschlägige Rechtsprechung des Europäischen Gerichtshofs.

Darüber hinaus spricht der EDSB konkrete Empfehlungen zu verschiedenen Aspekten der Vorschläge zu elektronischen Beweismitteln aus, für die Verbesserungen erforderlich sind: die **Authentizität und Vertraulichkeit von Anordnungen und übermittelten Daten**, die **begrenzte Sicherung** unter Europäischen Sicherungsanordnungen, der **anwendbare Datenschutzrahmen**, die **Rechte betroffener Personen**, betroffene Personen, die **Immunitäten und Vorrechte** genießen, die **Vertreter**, die **Fristen** zur Einhaltung Europäischer Herausgabeanordnungen und die **Möglichkeit für Diensteanbieter,** Einspruch gegen Anordnungen zu erheben.

Abschließend bittet der EDSB um mehr Klarheit in Bezug auf die Wechselbeziehungen des Verordnungsvorschlags und künftigen internationalen Übereinkommen. Der Verordnungsvorschlag sollte das hohe Maß an Datenschutz in der EU erhalten und bei der Aushandlung internationaler Übereinkommen zu grenzüberschreitendem Zugang zu elektronischen Beweismitteln zu einem Bezugspunkt 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) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG[1], insbesondere auf Artikel 42 Absatz 1, Artikel 57 Absatz 1 Buchstabe g und Artikel 58 Absatz 3 Buchstabe c,

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)[2],

gestützt auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[3] –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG UND HINTERGRUND

1. Am 17. April 2018 legte die Kommission zwei Gesetzgebungsvorschläge (im Folgenden „die Vorschläge“) mit einer Folgenabschätzung[4] vor, und zwar:
   - Vorschlag für eine Verordnung über Europäischen Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen[5] (im Folgenden „der Verordnungsvorschlag“);
   - eines Vorschlags für eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren[6] (im Folgenden „der Richtlinienvorschlag“).

2. Der Verordnungsvorschlag würde parallel zur Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen (im Folgenden „EEA-Richtlinie“)[7] bestehen, die die Erleichterung des Prozesses der Beweiserhebung im Hoheitsgebiet eines anderen Mitgliedstaats zum Ziel hat und jede Art der Beweiserhebung abdeckt, einschließlich elektronischer Daten[8]. Alle Mitgliedstaaten, die sich an der Annahme der EEA-Richtlinie[9] beteiligten, hatten bis Mai 2017 Zeit, sie in einzelstaatliches Recht umzusetzen[10].

3. Am 26. September 2018 nahm der Europäische Datenschutzausschuss[11] (im Folgenden „EDSA“) eine Stellungnahme[12] zu den Vorschlägen an.

4. Am 7. Dezember 2018 und 8. März 2019 legte der Rat seine allgemeine Ausrichtung zum Verordnungsvorschlag[13] und zum Richtlinienvorschlag[14] fest. Das Europäische Parlament veröffentlichte eine Reihe von Arbeitsdokumenten.

5. Der Europäische Datenschutzbeauftragte (im Folgenden „EDSB“) begrüßt, dass er vor der Annahme der Vorschläge von den Dienststellen der Kommission informell konsultiert wurde. Der EDSB begrüßt ferner die Bezugnahmen auf die vorliegende Stellungnahme in Erwägungsgrund 66 des Verordnungsvorschlags und in Erwägungsgrund 24 des Richtlinienvorschlags.

6. Am 5. Februar 2019 nahm die Kommission zwei Empfehlungen für Beschlüsse des Rates an: eine Empfehlung über die Ermächtigung zur Aufnahme von Verhandlungen über ein internationales Abkommen zwischen der Europäischen Union (EU) und den Vereinigten Staaten von Amerika (USA) über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen[15] und eine Empfehlung zur Genehmigung der Teilnahme der Kommission an Verhandlungen über ein Zweites Zusatzprotokoll zum Übereinkommen des Europarats über Computerkriminalität im Namen der EU (SEV Nr. 185) (im Folgenden „das Übereinkommen über Computerkriminalität“)[16]. Die beiden Empfehlungen waren Gegenstand von zwei Stellungnahmen des EDSB[17]. Die Verhandlungen mit den USA und die Verhandlungen im Europarat sind eng miteinander verbunden.

7. Im Februar 2019 richtete der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments ähnliche Schreiben an den EDSB und den EDSA, um eine rechtliche Beurteilung der Auswirkung des US CLOUD Act,[18] der vom US-Kongress im März 2018 verabschiedet wurde, auf den Europäischen Rechtsrahmen für Datenschutz anzufordern. Am 12. Juli 2019 gaben der EDSB und der EDSA eine Gemeinsame Antwort auf diese Anfrage, die auch ihrer ersten Bewertung enthielt[19].

8. Am 3. Oktober 2019 unterzeichneten das Vereinigte Königreich und die Vereinigten Staaten ein bilaterales Abkommen über grenzüberschreitenden Zugang zu elektronischen Beweismitteln zur Bekämpfung von schwerer Kriminalität[20]. Es ist das erste hochrangige Übereinkommen, das es US-Diensteanbietern gestattet, Ersuchen von ausländischen Staaten nach Inhaltsdaten gemäß dem US CLOUD Act zu entsprechen.

9. Diese Stellungnahme behandelt beide Vorschläge, wobei das Hauptaugenmerk allerdings auf dem Verordnungsvorschlag liegt. Im Einklang mit der Aufgabe des EDSB konzentriert sie sich hauptsächlich auf das Recht auf den Schutz der Privatsphäre und das Recht auf den Schutz personenbezogener Daten und hat zum Ziel, einheitlich mit und ergänzend zur Stellungnahme 23/2018 des EDSB zu sein, auch unter Berücksichtigung der allgemeine Ausrichtungen des Rates und der Arbeitsdokumente des Europäischen Parlaments.

2. ZIELE DER VORSCHLÄGE

10. Das übergeordnete Ziel des Verordnungsvorschlags besteht darin, den Prozess der Sicherung und des Erhalts von elektronischen Beweismitteln grenzüberschreitend zu beschleunigen[21]. Zu diesem Zweck würde die Verordnung zwei neue Arten bindender Anordnungen einführen: die Europäische Herausgabeanordnung (im Folgenden „EPO“) zur Herausgabe von Daten durch einen Diensteanbieter und die Europäische Sicherungsanordnung (im Folgenden „EPO-PR“) zur Sicherung von Daten im Hinblick auf

spätere Ersuchen um Herausgabe dieser Daten, die möglicherweise als Beweismittel in Strafverfahren verwendet werden.

11. Die vorgeschlagenen Maßnahmen würden die Verarbeitung personenbezogener Daten und Einschränkungen sowohl des Rechts auf Schutz der Privatsphäre, das durch Artikel 7[22] der Charta gewährleistet wird, als auch des Rechts auf Schutz personenbezogener Daten, das durch Artikel 8[23] der Charta gewährleistet wird, nach sich ziehen. Solche Einschränkungen der Ausübung der durch die Charta geschützten Grundrechte müssen, damit sie rechtmäßig sind, den folgenden, in Artikel 52 Absatz 1 der Charta niedergelegten Bedingungen entsprechen. Dies beinhaltet die Sicherstellung, dass jegliche Einschränkung des Rechts auf Schutz personenbezogener Daten „notwendig" und „verhältnismäßig" ist. Zur Unterstützung des Unionsgesetzgebers bei der Beurteilung der Einhaltung der vorgeschlagenen Rechtsetzungsmaßnahmen im Zusammenhang mit der Verarbeitung personenbezogener Daten veröffentlichte der EDSB ein Instrumentarium zur Beurteilung der Notwendigkeit („Necessity Toolkit"),[24] das sich auf die einschlägige Rechtsprechung und seine früheren Stellungnahmen stützt.
12. Gemäß dem Verordnungsvorschlag würden die Anordnungen nur in grenzüberschreitenden[25] und nicht in innerstaatlichen Situationen erteilt[26]. Herausgabeanordnungen würden nur von einer Justizbehörde eines Mitgliedstaats erteilt oder bestätigt, wenn für die gleiche Straftat in einer vergleichbaren innerstaatlichen Situation im Anordnungsstaat eine ähnliche Maßnahme verfügbar ist. Die Anordnungen würden von der Anordnungsbehörde direkt an die Diensteanbieter gerichtet, die Dienstleistungen in der Europäischen Union (im Folgenden „EU")[27] anbieten und in einem anderen Mitgliedstaat niedergelassen oder über Vertreter vertreten sind. Sie würden den Diensteanbieter über Zertifikate über eine Europäische Herausgabeanordnung (im Folgenden „EPOC") oder über Zertifikate über eine Europäische Sicherungsanordnung (im Folgenden „EPOC-PR") übermittelt. Diese Anordnungen würden direkt im vollstreckenden Mitgliedstaat ohne vorheriges Verfahren auf Anerkennung und Vollstreckung in diesem Mitgliedstaat ausgeführt. Unter bestimmten Bedingungen könnten allerdings eingeschränkte Gründe im vollstreckenden Mitgliedstaat angeführt werden, um die Anerkennung oder Vollstreckung der Anordnungen zu versagen (Artikel 14) oder um im anordnenden Mitgliedstaat die Überprüfung einer Europäischen Herausgabeanordnung („EPO") zu ersuchen (Artikel 15 und 16).

13. Mit dem Richtlinienvorschlag soll eine gemeinsame EU-Lösung zur Identifizierung der Adressaten von EPOC und EPOC-PR[28] geschaffen werden. Zu diesem Zweck führt er für alle Diensteanbieter, die in der Union Dienstleistungen anbieten, eine Verpflichtung ein, einen Vertreter in der EU zu benennen[29], der für den Empfang von EPOC und EPOC-PR und deren zeitnahe und vollständige Ausführung verantwortlich ist[30].

14. Angesichts der Herausforderungen, denen Polizei und Justizbehörden gegenüberstehen, um elektronische Beweismittel in der heutigen digitalen Welt, die keine Grenzen kennt, zu erheben, **unterstützt der EDSB das Ziel, den Strafverfolgungsbehörden wirksame Instrumente zur Verfügung zu stellen, um über Grenzen hinweg schnellen Zugang zu elektronischen Beweismitteln zu erhalten. In vielen Fällen ist die Zeit ein entscheidender Faktor, um diesen Behörden das Einholen von Daten zu ermöglichen, die zur Erfüllung ihrer Aufträge unabdingbar sind.** Auch bei Ermittlungen in nationalen Fällen finden sich die Strafverfolgungsbehörden zunehmend allein deshalb in „grenzüberschreitenden Situationen" wieder, weil ein ausländischer Diensteanbieter involviert war und die Daten in einem anderen Mitgliedstaat elektronisch gespeichert sind.

Daher **begrüßt der EDSB das Ziel der Vorschläge zu elektronischen Beweismitteln, den Zugang in grenzüberschreitenden Fällen zu beschleunigen und zu erleichtern und um die Rechtssicherheit durch Straffung der Verfahren innerhalb der EU zu erhöhen.** Gleichzeitig **besteht er auf die Notwendigkeit, dass die Sicherung von und der Zugang zu elektronischen Beweismitteln der Charta der Grundrechte der EU (im Folgenden „die Charta") und dem Rechtsrahmen für den Datenschutz in vollem Umfang Rechnung tragen**.

15. Der EDSB hält fest, dass die den Vorschlägen beiliegende Folgenabschätzung das in Artikel 6 der Charta verankerte Recht auf Freiheit und Sicherheit als *„Grundrechte von Personen, die Opfer von Straftaten sind oder werden können"*[31] vorsieht. Der EDSB unterstreicht, dass dieses Recht die Freiheit und Sicherheit des Einzelnen gegenüber dem Staat schützen und nicht durch den Staat gewährleisten soll[32].

16. Zur Einhaltung der Bedingungen von Artikel 52 Absatz 1 erinnert der EDSB daran, dass der EuGH festgestellte, dass der Unionsgesetzgeber *„klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen [sollte], sodass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen."*[33] Die Vorschläge stellen die jüngste Maßnahme aus einer Reihe von Rechtsetzungsmaßnahmen dar, in denen der Unionsgesetzgeber aufgefordert wird, ein ausgewogenes Verhältnis zwischen den Rechten natürlicher Personen auf Datenschutz gegenüber dem Allgemeininteresse an der Bekämpfung und Verfolgung von Straftaten zu schaffen. Solche Maßnahmen können offensichtlich mit Datenschutzrechten kollidieren.[34] **Daher müssen diese Vorschläge sehr genau geprüft und dabei besondere Aufmerksamkeit der Frage geschenkt werden, inwiefern alle erforderlichen Garantien gegeben sind.**

3. HAUPTEMPFEHLUNGEN

3.1. Klare Definitionen der Kategorien personenbezogener Daten

17. Der Begriff „elektronische Beweismittel" wird in Artikel 2 Nummer 6 des Verordnungsvorschlags definiert und in die vier Unterkategorien „Teilnehmerdaten", „Zugangsdaten", „Transaktionsdaten" und „Inhaltsdaten" unterteilt, die ihrerseits in Artikel 2 Nummer 7, 8, 9 bzw. 10 definiert werden. Der Schwerpunkt dieser Unterteilung liegt auf der „Sensibilität"[35] jeder Datenkategorie und sieht auf dieser Grundlage verschiedene Anforderungen[36] für den Zugang zu Daten vor, die in diese Kategorien fallen.

3.1.1. Vereinbare Datenkategorie-Definitionen im Unionsrecht

18. Der EDSB betont, wie wichtig es ist, die Kohärenz zwischen den Datenkategorien im Verordnungsvorschlag und anderen Definitionen von Datenkategorien im Unionsrecht sicherzustellen. In dieser Hinsicht hält der EDSB fest, dass der Verordnungsvorschlag die im Zusammenhang mit dem Entwurf der Verordnung über Privatsphäre und elektronische Kommunikation vorgeschlagenen Definitionen berücksichtigt, die die elektronischen Kommunikationsdaten definieren[37] und zwischen den beiden Kategorien elektronischer Kommunikationsinhaltsdaten[38] und elektronischer Kommunikationsmetadaten unterscheiden würden[39].

19. Während die Kategorie der Inhaltsdaten im Verordnungsvorschlag mit der Kategorie der elektronischen Kommunikationsinhaltsdaten im Verordnungsvorschlag über Privatsphäre und elektrische Kommunikation vereinbar zu sein scheint, sind die Kategorien der **Transaktionsdaten und Zugangsdaten im Verordnungsvorschlag neue Datenkategorien**. Sie sind im EU-Datenschutzrecht derzeit nicht definiert. Beide umfassen elektronische Kommunikationsmetadaten gemäß der Definition des Verordnungsvorschlags über Privatsphäre und elektronische Kommunikation, sind aber nicht darauf beschränkt. Die zukünftige Verordnung über Privatsphäre und elektronische Kommunikation würde für die Sicherung und Herausgabe von Daten der elektronischen Kommunikationsdiensteanbieter gemäß dem Verordnungsvorschlag über elektronische Beweismittel gelten. **Nach Ansicht des EDSB muss während des gesamten Gesetzgebungsverfahrens die umfassende Kohärenz zwischen den Definitionen dieser beiden Texte sichergestellt werden. Der EDSB erinnert daran, dass er wiederholt zu einer schnellen Annahme der Verordnung über Privatsphäre und elektronische Kommunikation aufgerufen hat, um Rechtsunsicherheit zu vermeiden[40].**

3.1.2. Mangelnde Klarheit und Überlappung der Datenkategorien

20. Der EDSB betont, wie wichtig es ist, klare und einfache Definitionen für jede Datenkategorie niederzulegen, um Rechtssicherheit für alle beteiligten Akteure zu gewährleisten. Dies ist eines der Hauptziele des Verordnungsvorschlags[41]. Die Wirksamkeit der Anordnungen könnte leicht durch die mangelnde Präzision und Klarheit der Kerndefinitionen des Verordnungsvorschlags untergraben werden.

21. Der Verordnungsvorschlag würde eine neue Kategorie der „Zugangsdaten" einführen, die als „*Daten über den Beginn und die Beendigung der Zugangssitzung eines Nutzers in Bezug auf einen Dienst*" definiert sind. Artikel 2 Absatz 8 definiert Zugangsdaten auch in Verbindung mit dem Verarbeitungszweck solcher Daten, d. h. sie sind „*ausschließlich zum Zweck der Identifizierung des Nutzers des Dienstes unbedingt erforderlich*". Zudem wird festgelegt, dass darin auch elektronische Kommunikationsmetadaten enthalten sind. Die Begründung führt aus, dass es grundlegend ist, diese Kategorie von Zugangsdaten zu erfassen, da sie zusammen mit Teilnehmerdaten oft „*Ausgangspunkt [sind], um bei einer Untersuchung erste Hinweise auf die Identität eines Verdächtigen zu erhalten*"[42]. Der EDSB weist allerdings darauf hin, dass diese neue Datenkategorie nicht mit den bestehenden Definitionen der Datenkategorien im Unionsrecht und in den Rechtsvorschriften der Mitgliedstaaten vereinbar ist[43]. Die Schaffung dieser Datenkategorie scheint künstlich zu sein und nur zum Ziel zu haben, geringere Anforderungen mit der Herausgabe solcher Daten zu verbinden, die mit den Anforderungen zur Herausgabe von Teilnehmerdaten (Artikel 4 Absatz 1) vergleichbar sind. Daher **empfiehlt der EDSB, die Notwendigkeit für die Einführung dieser neuen Datenkategorie der Zugangsdaten zu prüfen.**

22. Alternativ vertritt der EDSB, wie bereits vom EDSA vorgebracht[44], die Ansicht, dass es der vorgeschlagenen Definition der Zugangsdaten an Klarheit fehlt, falls die Kategorie der Zugangsdaten im Text verbleiben sollte. Der EDSB hält fest, dass beide Definitionen der Transaktionsdaten und Zugangsdaten „elektronische Kommunikationsmetadaten", wie im Verordnungsvorschlag über Privatsphäre und elektronische Kommunikation definiert, beinhalten. Beide führen eine Anzahl an Daten als Beispiele auf, die in ihre Kategorie fallen. Einige Beispiele fallen ausdrücklich unter beide Definitionen, wie beispielsweise Datum und Zeit. Zusätzlich schließt die Definition der Transaktionsdaten Daten aus, die unter diese

Kategorie fallen, wenn *„diese Daten Zugangsdaten darstellen“*. Diensteanbieter können in der Praxis Schwierigkeiten haben, zwischen Zugangsdaten und Transaktionsdaten zu unterscheiden, wobei der Verordnungsvorschlag vorsieht, dass diese Kategorien unter verschiedenen Bedingungen bereitgestellt werden sollten. Daher **empfiehlt der EDSB, die Definitionen für Zugangsdaten und Transaktionsdaten klarzustellen und eine klare Abgrenzung zwischen diesen Kategorien zu ziehen, um Rechtssicherheit zu gewährleisten. Gleiche Daten sollten nicht unter verschiedenen Bedingungen bereitgestellt werden, die von der Kategorie abhängen, unter der sie angefordert werden. Ansonsten muss eine EPO für Zugangsdaten den gleichen Bedingungen wie Transaktionsdaten und Inhaltsdaten unterliegen (Artikel 4 Absatz 2).**

23. Darüber hinaus teilt der EDSB ähnliche Bedenken hinsichtlich der Kategorie der Teilnehmerdaten. Das Übereinkommen über Computerkriminalität enthält bereits eine Definition von „Bestandsdaten“[45], die von den Vertragsparteien des Übereinkommens nicht immer einheitlich ausgelegt wird[46]. Der Verordnungsvorschlag sieht die erste Definition von Teilnehmerdaten im Unionsrecht vor. Nach Ansicht des EDSB ist die Definition dieser Datenkategorie im Verordnungsvorschlag eine schwierige, aber wichtige Aufgabe. Der EDSB hebt hervor, dass Verwirrung zwischen den Kategorien der Transaktionsdaten und Teilnehmerdaten vermieden werden muss, insbesondere im Hinblick auf Artikel 2 Absatz 7 Buchstabe b, da die Herausgabe dieser beiden Datenkategorien auch unterschiedlichen Bedingungen unterliegen würde. In dieser Hinsicht hebt der EDSB hervor, dass IP-Adressen neben der Kategorie der Zugangsdaten, in der IP-Adressen konkret genannt werden, in beide Kategorien, d. h. Transaktionsdaten und Teilnehmerdaten, fallen könnten. **Der EDSB empfiehlt die Änderung der vorgeschlagenen Definition der Teilnehmerdaten, um diese Kategorie genauer zu bestimmen, insbesondere Artikel 2 Absatz 7 Buchstabe b,und in Verbindung mit IP-Adressen, und um die Überlappung mit anderen Datenkategorien zu vermeiden.**

3.2. Art der betroffenen Straftaten

24. Der EDSB nimmt die Art der Straftaten, für die Behörden eine EPO und eine EPO-PR erlassen werden können, zur Kenntnis. Erstens kann eine EPO nur erlassen werden, wenn in einer vergleichbaren innerstaatlichen Situation im Anordnungsstaat für dieselbe Straftat eine ähnliche Maßnahme zur Verfügung stünde (Artikel 5 Absatz 2 des Verordnungsvorschlags). Eine EPO zur Herausgabe von Teilnehmerdaten und Zugangsdaten kann für alle Straftaten (Artikel 5 Absatz 3 des Verordnungsvorschlags) erlassen werden, wobei eine EPO zur Herausgabe von Transaktionsdaten und Inhaltsdaten für eine Vielzahl von Straftaten, die in Artikel 5 Absatz 4 des Verordnungsvorschlags aufgeführt sind, erlassen werden kann:

    (a) alle „*Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden*“;
    (b) Straftaten in Verbindung mit Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie und Angriffe auf Informationssysteme, „*wenn diese ganz oder teilweise mittels eines Informationssystems begangen werden*“;
    (c) terroristische Straftaten.

25. Zweitens kann eine EPO-PR zur Sicherung jeder Art von elektronischen Beweismitteln für alle Straftaten ohne Unterscheidung erlassen werden (Artikel 6 Absatz 2 des

Verordnungsvorschlags). Das Erfordernis einer ähnlichen Maßnahme, die für innerstaatliche Fälle verfügbar ist, gilt nicht für EPO-PR.

26. Nach Ansicht des EDSB ist die vorgeschlagene Schwelle von mindestens drei Jahren Höchst-Haftstrafe in Artikel 5 Absatz 4 Buchstabe a und die Liste Straftaten, die mit dem Cyberspace zusammenhängen oder durch den Cyberspace möglich gemacht wurden, in Artikel 5 Absatz 4 Buchstabe b angesichts der Sensibilität der Transaktionsdaten und Inhaltsdaten und der Schwere des Eingriffs in das Recht auf Privatsphäre und das Recht Datenschutz, womit ein Zugriff auf diese Daten verbunden wäre, äußerst problematisch. Die Schwelle einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren in Artikel 5 Absatz 4 Buchstabe a des Verordnungsvorschlags wäre in der Praxis auf eine sehr große Anzahl an Straftaten in den nationalen Strafgesetzbüchern der Mitgliedstaaten, einschließlich vieler Straftaten, die nicht als „schwer" betrachtet werden können, anwendbar[47].

27. Der EDSB erinnert daran, dass der EuGH in Bezug auf Metadaten, die von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste gespeichert werden, feststellte, dass *„aus der Gesamtheit dieser Daten … sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden [können], etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren",*[48] und dass *„diese Daten … insbesondere … die Erstellung des Profils der betroffenen Personen [ermöglichen], das im Hinblick auf das Recht auf Achtung der Privatsphäre eine genauso sensible Information darstellt wie der Inhalt der Kommunikationen selbst"*[49]. In Bezug auf Inhaltsdaten stellte der EuGH fest, dass der Zugang zu diesen Daten sogar das Wesen des Rechts auf Schutz der Privatsphäre und des Rechts auf Datenschutz antasten kann[50].

28. Darüber hinaus wirft der EDSB auf, dass der EuGH in seinem kürzlich ergangenen Urteil in der Rechtssache C-207/16 entschied, dass *„[n]ach dem Grundsatz der Verhältnismäßigkeit [...] ein schwerer Eingriff im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nämlich nur durch einen Zweck der Bekämpfung einer ebenfalls als „schwer" einzustufenden Kriminalität gerechtfertigt sein [kann]"* und *"in [diesen Bereichen], nur die Bekämpfung der schweren Kriminalität einen Zugang öffentlicher Stellen zu von den Betreibern von Kommunikationsdiensten gespeicherten personenbezogenen Daten rechtfertigen kann, aus deren Gesamtheit genaue Schlüsse auf das Privatleben der von diesen Daten betroffenen Personen gezogen werden können"*[51]. Nach Ansicht des EDSB würde der Zugang zu den Kategorien der Transaktionsdaten und Inhaltsdaten durch die zuständigen nationalen Behörden das Ziehen solcher genauen Schlussfolgerungen bezüglich des Privatlebens der Personen, deren Daten mit einer EPO eingeholt werden, ermöglichen. Der Zugang zu diesen Datenkategorien muss daher auf Fälle schwerer Kriminalität beschränkt werden.

29. In Bezug auf die in Artikel 5 Absatz 4 Buchstabe b enthaltene Liste der Straftaten, die mit dem Cyberspace zusammenhängen oder durch den Cyberspace möglich gemacht wurden, ist der EDSB nicht von der Begründung in Erwägungsgrund 32 überzeugt, dass diese Straftaten „*bestimmte Straftatbestände [sind], bei denen die Beweismittel in der Regel ausschließlich in elektronischer [...] Form zur Verfügung stehen*" und dass „*die Anwendung desselben Mindeststrafmaßes wie bei anderen Arten von Straftaten*

hauptsächlich dazu führen [würde], dass Straftaten ungeahndet bleiben". Der EDSB ist der Ansicht, dass nicht alle Straftaten, die mit dem Cyberspace zusammenhängen oder durch den Cyberspace möglich gemacht wurden und in Artikel 5 Absatz 4 Buchstabe b aufgeführt sind, „schwere Straftaten" darstellen können. In der Erkenntnis, dass es notwendig und verhältnismäßig sein könnte, Transaktions- und Inhaltsdaten in bestimmten Fällen einzuholen, könnte dies dennoch durch die Sicherung jeglicher Art von Daten über eine EPO-PR mit einem Ersuchen für die Herausgabe der gesicherten Daten über die herkömmlichen Kooperationskanäle (beispielsweise EEA) erreicht werden. Somit könnten die hohen Garantien gewahrt werden.

30. **Aus diesen Gründen empfiehlt der EDSB, das Gleichgewicht zwischen den Arten von Straftaten, für die EPOs erlassen werden könnten, und den betroffenen Datenkategorien erneut zu bewerten. Insbesondere die Möglichkeit, eine EPO zur Herausgabe von Transaktionsdaten und Inhaltsdaten zu erlassen, sollte nur auf schwere Straftaten beschränkt werden[52].**

31. **Der EDSB ist darüber hinaus der Auffassung, dass angesichts der möglicherweise offenlegenden Art der Transaktionsdaten und Inhaltsdaten nur im Zusammenhang mit bestimmten schweren Straftaten Zugang zu diesen Daten gewährt werden sollte.** Die Vorlage einer geschlossenen Liste dieser schweren Straftaten würde auch die Rechtssicherheit für alle beteiligten Akteure erhöhen. Die Option, den Anwendungsbereich der EPO auf bestimmte Straftaten zu beschränken, wurde zwar im Frühstadium der Vorbereitung der Vorschläge verworfen[53], **doch der EDSB empfiehlt, diese Möglichkeit unter Berücksichtigung der einschlägigen Rechtsprechung des EuGH erneut in Erwägung zu ziehen[54].**

32. Abschließend hebt der EDSB hervor, dass **ähnliche Erwägungen auch für eine EPO zur Herausgabe von Teilnehmerdaten und Zugangsdaten, wie derzeit im Verordnungsvorschlag definiert, relevant sein könnten, und zwar dem Umfang, in dem diese Kategorien nicht näher bestimmt und festgelegt werden und möglicherweise elektronische „Kommunikationsmetadaten" umfassen könnten**[55].

3.3. Datensicherheit

33. Die Gewährleistung der Sicherheit personenbezogener Daten ist eine klare Anforderung gemäß dem EU-Datenschutzrecht[56]. Auch bei der Gewährleistung der Vertraulichkeit von Ermittlungen und Strafverfahren ist Datensicherheit wesentlich. Der EDSB begrüßt zwar Artikel 11 über die Vertraulichkeit von Informationen und Erwägungsgrund 57 des Verordnungsvorschlags[57], hält aber fest, dass er nicht angemessen auf die Fragen der Echtheit der von den Diensteanbietern erhaltenen Zertifikate[58], der Sicherheit der Übermittlung personenbezogener Daten an die betreffenden Behörden als Reaktion[59] und der Sicherheit von Anordnungen, die von Vollstreckungsbehörden eingegangen sind, eingeht[60].

34. Die **Überprüfung der Echtheit der Zertifikate und Anordnungen ist entscheidend,** um zu gewährleisten, dass sämtliche übermittelten personenbezogenen Daten vertraulich bleiben, und um potenzielle Datenschutzverletzungen zu vermeiden, die nachteilig für die betroffenen Personen sein und die Haftung der Vollstreckungsbehörden, Diensteanbieter oder deren Vertreter gemäß dem anwendbaren Datenschutzrecht auslösen könnten. Daher **empfiehlt der EDSB die Aufnahme von Bestimmungen in den Verordnungsvorschlag, mit denen definiert wird, wie die Echtheit der Zertifikate und Anordnungen**

gewährleistet und überprüft werden kann. Der EDSB schlägt insbesondere vor, die Nutzung von digitalen Signaturen in Fällen zu untersuchen, in denen Anordnungen und Zertifikate elektronisch übermittelt werden. Er unterstreicht, dass die Gewährleistung, dass die notwendigen Mittel geschaffen werden, damit die personenbezogenen Daten, die gemäß den Vorschlägen in einer sicheren Umgebung mit den Mitteln offengelegt und mitgeteilt werden, um die Echtheit der Dokumente zu gewährleisten, grundlegend ist, um das Ziel einer schnellen Erhebung elektronischer Beweismittel im Einklang mit den Grundrechten zu erreichen.

35. Der EDPS begrüßt, dass die allgemeine Ausrichtung des Rates im Hinblick auf die **Sicherheit der Übermittlung von Zertifikaten und angeforderten Daten** festlegt, dass die EPOC und EPOC-PR „*auf sichere und zuverlässige Weise [übermittelt werden], die dem Adressaten ermöglicht, einen schriftlichen Nachweis zu erbringen, und die Feststellung der Echtheit des Zertifikats gestattet*,“[61] und dass die angeforderten Daten „*in einer sicheren und zuverlässigen Weise [übermittelt werden], die die Feststellung der Echtheit und der Unversehrtheit gestattet*“[62]. **Er ist allerdings der Auffassung sein, dass weitere besondere und wirksame Garantien erforderlich sind, auch im Hinblick auf die bei den Vollstreckungsbehörden eingegangenen Anordnungen**.

36. Insbesondere in Bezug auf die **Übermittlung von Zertifikaten** würde Artikel 8 Absatz 2 des Verordnungsvorschlags und der allgemeinen Ausrichtung des Rates die Nutzung von bereits eingerichteten speziellen Plattformen oder anderer sicherer Kanäle für die Bearbeitung von Datenersuchen von Strafverfolgungs- und Justizbehörden gestatten. Dies bleibt allerdings fakultativ und würde nicht ausdrücklich für andere Kommunikationen der Anordnungsbehörde in Bezug auf personenbezogene Daten erlaubt, die nach dieser Übermittlung stattfinden.

37. Der ESDB stellt zudem fest, dass *„die Kommission daran [arbeitet] die bestehenden Verfahren zur justiziellen Zusammenarbeit durch bestimmte Maßnahmen zu stärken, etwa die Schaffung einer sicheren Plattform für den schnellen Austausch von Ersuchen zwischen Justizbehörden in der EU“*[63] und dass die Kommission anregt, in Betracht zu ziehen, „*die e-Codex-*[64] *und SIRIUS-Plattformen*[65] *mit dem Ziel einer sicheren Verbindung zu Diensteanbietern für die Übermittlung des EPOC und des EPOC-PR sowie gegebenenfalls für die Antworten der Diensteanbieter zu erweitern.“*[66] Im Hinblick darauf hält der EDSB fest, dass ein Mitgliedstaat während der Verhandlungen im Rat vorschlug, „*einen neuen Erwägungsgrund hinzuzufügen, der die Kommission und die Mitgliedstaaten auffordert, so schnell wie möglich an sicheren elektronischen Kommunikationskanälen, die die Feststellung der Echtheit und der Unversehrtheit gestatten, zu arbeiten und einzurichten*“[67]. Der EDSB erinnert im Hinblick darauf daran, dass jede Einrichtung eines neuen IT-Systems zur Verarbeitung personenbezogener Daten eine Rechtsgrundlage erfordert und dass zumindest dort, wo ein solches IT-System die Einbeziehung eines Organs, einer Einrichtung, einer Agentur oder eines Amts der Union mit sich bringt, diese Rechtsgrundlage in einem Rechtsakt der Union liegen muss. **Daher empfiehlt der EDSB, in der Verordnung klar eine Rechtsgrundlage für ein IT-System zur Nutzung für die Verarbeitung personenbezogener Daten im Sinne der Verordnung vorzusehen**.

38. Der EDSB begrüßt zudem, dass in den Vorschlägen und der allgemeinen Ausrichtung des Rates die Öffentlichkeit der Information in Bezug auf sowohl die **Identifikation der Behörden als auch der Vertreter** der Diensteanbieter vorgesehen ist[68]. Allerdings **empfiehlt er die Änderung der Textvorschläge, sodass diese Pflichten vor dem Beginn**

der Anwendung anderer Bestimmungen eingeführt werden und somit sichergestellt wird, dass alle erforderlichen Informationen zu Beginn der Anwendung der Hauptbestimmungen verfügbar sind und jegliches Risiko einer Verletzung des Schutzes personenbezogener Daten vermieden wird[69].

3.4. Größere Beteiligung von Justizbehörden im Vollstreckungsmitgliedstaat

39. Gemäß dem Verordnungsvorschlag würde die Kontrolle über die Einhaltung der Grundrechte der von einer EPO/EPO-PR betroffenen Personen, einschließlich über die Notwendigkeit und Verhältnismäßigkeit der Anordnungen und die mögliche Anwendbarkeit von Immunitäten und Vorrechten, hauptsächlich von der Anordnungsbehörde gewährleistet. Zuständige Behörden im vollstreckenden Mitgliedstaat würden nur in Fällen, in denen Diensteanbieter eine Anordnung nicht erfüllen, als Vollstreckungsbehörden einschreiten. Daher wären, sobald die Anordnungen erteilt sind, angesichts der Tatsache, dass in den meisten Fällen die betroffenen Personen nicht unmittelbar über die Anordnungen informiert würden[70], die Diensteanbieter die einzigen Akteure mit der Möglichkeit, die Privatsphäre und die Datenschutzrechte von betroffenen Personen zu schützen.

40. In dem traditionellen Ansatz des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln liegt es hauptsächlich in der Verantwortung des Vollstreckungsstaats, die Überprüfung der beschränkten Anzahl an Gründen für die Verweigerung sicherzustellen. Der EDSB erkennt zwar die Notwendigkeit an, dass alternative Ansätze für das Erheben von Beweismaterial in einem grenzüberschreitenden Kontext identifiziert werden müssen, aber es ist und bleibt von ausschlaggebender Bedeutung, dass wirksame Garantien für die Grundrechte der betroffenen Person vorliegen. Es ist zu berücksichtigen, dass sich die einschlägigen Rechtsvorschriften in den Mitgliedstaaten unter anderem über die Zulässigkeit von in einem anderen Mitgliedstaat erhobenen Beweismitteln und die Definition einer Straftat unterscheiden können[71]. Selbst im Rahmen dieser Vorschläge – falls sie angenommen werden – sind die Bedingungen für das Erlassen einer Anordnung nicht vollständig in der EU harmonisiert und gegen die Vollstreckung einer solchen Anordnung können wichtige Einwände bestehen, die aus der Achtung der Grundrechte herrühren[72]. Im Rahmen der Verhandlungen über die EAA-Richtlinie betonte die Agentur für Grundrechte, dass *„die Wahrung der Grundrechte eine Schlüsselkomponente des Raums der Freiheit, der Sicherheit und des Rechts gemäß Artikel 67 Absatz 1 AEUV darstellt: Die Union bildet einen Raum der Freiheit, der Sicherheit und des Rechts, in dem die Grundrechte und die verschiedenen Rechtsordnungen und -traditionen der Mitgliedstaaten geachtet werden[73]. Selbst wenn die gegenseitige Anerkennung als ein „Grundsatz" dargestellt wird,[74] der von den Mitgliedstaaten zur Erleichterung der Zusammenarbeit im Raum der Freiheit, der Sicherheit und des Rechts verwendet wird, müssen die Mitgliedstaaten ihre rechtlichen Verpflichtungen zur Wahrung der Grundrechte erfüllen[75]".*

41. Der EDSA fand *„keine Rechtfertigung für das im Entwurf der Verordnung über elektronische Beweismittel vorgesehene Verfahren, das die Herausgabe von Inhaltsdaten ohne Beteiligung zumindest der zuständigen Behörden des Mitgliedstaats, in dem sich die betroffene Person befindet, ermöglicht"*[76]. Ferner äußerte der EDSA *„seine Bedenken hinsichtlich der Aufhebung jeglicher (doppelten) Überprüfung der übermittelten Anordnung durch die empfangende zuständige Behörde im Vergleich zu den anderen Instrumenten"*[77]. Der Rat hat in seiner allgemeine Ausrichtung zum Verordnungsvorschlag eine Notifizierung an die zuständigen Behörden der Vollstreckungsstaaten eingeführt. Diese Notifizierung würde zur gleichen Zeit wie der Versand der EPOC an die Diensteanbieter erfolgen. Sie

hätte allerdings keine aufschiebende Wirkung; sie hätte einen begrenzten Anwendungsbereich (sie wäre nur für eine EPOC bezüglich Inhaltsdaten[78] – die die am wenigsten häufig angeforderten Daten darstellen[79] – erforderlich, wenn die betroffene Person nicht im anordnenden Mitgliedstaat ansässig ist); schließlich könnten sich die notifizierten Behörden ohne Befugnis, direkt die Vollstreckung der Anordnung zu verhindern, nur auf eine begrenzte Anzahl an Umständen berufen (es gibt keinen allgemeinen, auf die Grundrechte gestützten Ablehnungsgrund an sich)[80]. Daher ersuchten mehrere Mitgliedstaaten darum, dass der notifizierten Behörde umfangreichere Befugnisse gewährt werden und dass diese auch Anordnungen in Bezug auf Nichtinhaltsdaten umfassen[81].

42. **Nach Ansicht des EDSB erfordert der wirksame Schutz der Grundrechte in diesem Zusammenhang ein bestimmtes Maß an Beteiligung der Justizbehörden des vollstreckenden Mitgliedstaats. Er empfiehlt daher, die vom vollstreckenden Mitgliedstaat benannten Justizbehörden so früh wie möglich in den Prozess der Erhebung elektronischer Beweismittel systematisch einzubeziehen, um diesen Behörden die Möglichkeit zu geben, die Übereinstimmung der Anordnungen mit der Charta wirksam und effizient zu prüfen und die Pflicht dieser Behörden zu gewährleisten, auf dieser Grundlage Ablehnungsgründe geltend zu machen[82].**

43. Zudem könnte die systematische Einbeziehung der Justizbehörden im vollstreckenden Mitgliedstaat die Einhaltung des Grundsatzes der beiderseitigen Strafbarkeit gewährleisten. In Erwägung, dass es innerhalb der EU keine Harmonisierung von Straftaten gibt, bedeutet der Verzicht auf den Grundsatz der beiderseitigen Strafbarkeit im Verordnungsvorschlag, dass personenbezogene Daten von einem Diensteanbieter für die Zwecke der Strafverfolgung einer Handlung offengelegt werden können, die gemäß den Rechtsvorschriften des Mitgliedstaats, in dem der Diensteanbieter niedergelassen ist, keine Straftat darstellt[83]. **Nach Ansicht des EDSB ist der Grundsatz der beiderseitigen Strafbarkeit eine zusätzliche Schutzmaßnahme für die Grundrechte, die Bestandteil des Verordnungsvorschlags sein sollte**. Wie bereits vom EDSA vorgebracht[84], würde diese Schutzmaßnahme *„gewährleisten, dass sich ein Mitgliedstaat nicht auf die Unterstützung eines anderen Mitgliedstaates für die Anwendung einer strafrechtlichen Sanktion berufen kann, die nicht im Recht des anderen Mitgliedstaates vorhanden ist“*[85]. **Der EDSB empfiehlt daher, das Erfordernis des Grundsatzes der beiderseitige Strafbarkeit in den Verordnungsvorschlag für alle Fälle aufzunehmen, in denen um Daten auf Grundlage einer Straftat ersucht wird, die weder auf Unionsebene definiert noch auf Unionsebene in einer in die Verordnung aufzunehmenden starren Liste vereinbart wurde**[86].

44. **Die Einbeziehung der Justizbehörden des Vollstreckungsstaates würde schließlich der Wahl von Artikel 82 Absatz 1 AEUV als Rechtsgrundlage für den Verordnungsvorschlag stärker entsprechen.** Der EDSB stellt in der Tat fest, dass dieser Artikel bisher verwendet wurde, um Mechanismen zur Zusammenarbeit nur zwischen den Justizbehörden einzurichten. In Übereinstimmung mit seinen Stellungnahmen 2/2019 und 3/2019[87] hat der EDSB starke Zweifel, dass diese Bestimmung als Rechtsgrundlage für die Annahme einer EU-Verordnung zur Einrichtung direkter grenzüberschreitender Zusammenarbeit zwischen Justizbehörden und Diensteanbietern in Strafsachen – grundsätzlich – ohne Einbeziehung einer Behörde im vollstreckenden Mitgliedstaat dienen könnte[88].

3.5. Beschränkte Sicherung unter Europäischen Sicherungsanordnungen

45. Durch den Verordnungsvorschlag würde die Europäische Sicherungsanordnung Diensteanbieter zur Sicherung von Daten im Hinblick auf ein späteres Ersuchen um Herausgabe dieser Daten i, Rahmen eines Rechtshilfeersuchen, einer EEA oder einer EPO zwingen. Das Ziel dieser Anordnungen besteht darin, *„die Entfernung, Löschung oder Änderung relevanter Daten in Situationen zu verhindern, in denen mehr Zeit für die Erwirkung der Herausgabe dieser Daten benötigt wird"*[89]. Der EDSB geht davon aus, dass die EPO-PR bestimmte Daten betrifft, die bei den Diensteanbietern zum Zeitpunkt des Erhalts der EPOC-PR gespeichert sind, und sich nicht auf zukünftige Daten bezieht, die nach diesem Zeitpunkt gespeichert werden. Zudem ist hervorzuheben, dass eine EPO-PR keine allgemeine Verpflichtung zur Datenspeicherung einrichtet[90].

46. Der EDSB erinnert an den Grundsatz der Speicherbegrenzung,[91] demgemäß personenbezogene Daten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Der Verordnungsvorschlag sieht vor, dass die Sicherung auf höchstens 60 Tage begrenzt werden muss, *„es sei denn, die Anordnungsbehörde bestätigt, dass das entsprechende Ersuchen um Herausgabe in die Wege geleitet wurde"* (Artikel 10 Absatz 1). Wenn die Anordnungsbehörde diese Bestätigung während der 60-Tage-Frist ausstellt, sichert der Adressat die Daten so lange, wie dies notwendig ist, um ihre Herausgabe zu ermöglichen (Artikel 10 Absatz 2). Erwägungsgrund 42 führt weiter aus, dass die 60-Tage-Frist berechnet wurde, um die Stellung eines offiziellen Ersuchens zu ermöglichen, und dass für diese „Stellung" zumindest einige formelle Schritte unternommen wurden, beispielsweise indem die Übersetzung eines Rechtshilfeersuchens in Auftrag gegeben wurde. Wenn die Sicherung nicht mehr erforderlich ist, setzt die Anordnungsbehörde den Adressaten unverzüglich hiervon in Kenntnis (Artikel 10 Absatz 3). **Der EDSB geht davon aus, dass jede Sicherungsanordnung grundsätzlich mit einem nachfolgenden Ersuchen um Herausgabe verbunden sein sollte. Der angestrebte Zeitraum für die Sicherung der Daten ist somit mit der Zukunft dieses nachfolgenden Ersuchens verbunden. Der EDSB schlägt vor, klarzustellen, dass die Sicherung nicht länger erforderlich sein würde und enden sollte, wenn das nachfolgende Ersuchen abgelehnt oder zurückgezogen wird.** Diese Spezifikation gilt auch für Artikel 9 Absatz 6 letzter Satz[92].

47. Darüber hinaus sollte, wie bereits vom EDSA vorgebracht[93], die Europäische Sicherungsanordnung *„niemals als Grundlage für den Dienstleister dienen […], die Daten nach dem ursprünglichen Löschungsdatum zu verarbeiten"*. Der EDSB geht auch davon aus, dass **die gesicherten Daten ab den Zeitpunkt des Erhalts des Zertifikats über eine Europäische Sicherungsanordnung und bis zu ihrer Herausgabe infolge eines nachfolgenden Ersuchens um Herausgabe nicht geändert werden sollten.** Daher **empfiehlt der EDSB, im Verordnungsvorschlag genauer festzulegen, dass die Daten, die mit einer EPO-PR ersucht werden, separat gespeichert werden sollten und ihre Verarbeitung auf ihre Speicherung bis zu ihrer Herausgabe begrenzt werden sollte.**

4. WEITERE EMPFEHLUNGEN

4.1. Vollständiger Verweis auf den geltenden Rechtsrahmen für den Datenschutz

48. Der EDSB begrüßt, dass der Verordnungsvorschlag den EU-Rechtsrahmen für den Datenschutz berücksichtigt, und hält fest, dass personenbezogene Daten nur in Übereinstimmung mit der DSGVO und der Richtlinie zum Datenschutz bei der

Strafverfolgung für Polizei und Justiz in Erwägungsgrund 56 des Verordnungsvorschlags verarbeitet werden dürfen. **Der EDSB empfiehlt, eine Bezugnahme auf die Verordnung über Privatsphäre und elektronische Kommunikation 2002/58/EG hinzuzufügen (wird vom Verordnungsvorschlag über Privatsphäre und elektronische Kommunikation ersetzt, sobald er angenommen wird[94]).**

49. Der EDSB hält fest, dass der Rat in seine allgemeine Ausrichtung eine Bestimmung über die weitere Übermittlung der von den Behörden der Mitgliedstaaten erhaltenen Daten an Behörden von Drittstaaten aufgenommen hat und auf die im Verordnungsvorschlag niedergelegten Bedingungen und Kapitel V der Richtlinie (EU) 2016/680[95] verweist. Der EDSB erinnert daran, dass gemäß Artikel 35 der Richtlinie (EU) 2016/680 eine Übermittlung personenbezogener Daten an ein Drittland nicht nur den Bedingungen gemäß Kapitel V unterliegt, sondern auch der Einhaltung der Vorschriften des nationalen Rechts, die gemäß den anderen Bestimmungen dieser Richtlinie angenommen wurden. **Der EDSB rät daher von der Aufnahme einer solchen Bestimmung in den endgültigen Wortlaut ab.**

4.2. Rechte der betroffenen Personen

4.2.1. Höhere Transparenz

50. Nach Ansicht des EDSB würde ein allgemeines Bewusstsein über die Häufigkeit und das Volumen der Sicherungs- und Herausgabeanordnungen, die an Diensteanbieter gerichtet werden, den Bürgern im Allgemeinen und auch den öffentlichen Einrichtungen die Möglichkeit geben, die Allgemeinpraxis bei der Anwendung dieser Instrumente zu bewerten und zu beurteilen. Transparenz kann also eine wichtige Rolle bei der Gewährleistung der Wahrung der Grundrechte spielen. Der EDSB hält fest, dass einige Diensteanbieter[96] bereits regelmäßig Transparenzberichte veröffentlichen, in denen sie die Gesamtzahl der von Behörden eingegangenen Ersuchen um Auskunft und der Antworten auf diese Ersuchen angeben.

51. **Der EDSB schlägt also vor, eine Verpflichtung einzuführen, in regelmäßigen Abständen und zusammengefasster Form die Anzahl der bei den Diensteanbietern unter dem Verordnungsvorschlag eingegangenen EPOC und EPOC-PR offenzulegen und dabei anzugeben, ob diesen Ersuchen nachgekommen wurde[97].**

4.2.2. Recht auf einen Rechtsbehelf

52. Der EDSB begrüßt Artikel 17 des Verordnungsvorschlags, der klarstellt, dass Rechtsbehelfe gemäß der DSGVO und der Richtlinie zum Datenschutz bei der Strafverfolgung für Polizei und Justiz für die betroffene Person, deren Daten eingeholt wurden, bestehen bleiben. **Er empfiehlt, den Fall hinzuzufügen, in dem die Daten gesichert wurden** (da nicht ausgeschlossen werden kann, dass ein Verstoß gegen die Datenschutzpflichten in Bezug auf diese Daten entsteht).

53. Die Bedingungen für Rechtsbehelfe gegen Diensteanbieter aufgrund von Verletzungen der Datenschutzbestimmungen nach dem Unionsrecht als für die Verarbeitung Verantwortliche oder Auftragsverarbeiter sind bereits in der DSGVO niedergelegt. Gemäß Artikel 82 Absatz 3 DSGVO wird beispielsweise *„[ein] Verantwortliche oder [ein] Auftragsverarbeiter […] von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass*

er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.".

54. Erwägungsgrund 46 des Verordnungsvorschlags sieht vor, dass *„[u]ngeachtet ihrer Datenschutzpflichten [...] die Diensteanbieter in den Mitgliedstaaten nicht für Schäden haftbar gemacht werden [sollten], die ihren Nutzern oder Dritten ausschließlich aufgrund der Befolgung eines EPOC oder eines EPOC-PR in guter Absicht entstehen".* **Nach Ansicht des EDSB sollte ein Instrument in Bezug auf die Zusammenarbeit in Strafsachen nicht die Haftungsbedingungen der für die Verarbeitung Verantwortlichen oder der Auftragsverarbeiter (d. h. der Diensteanbieter oder zuständigen Behörden) nach dem Datenschutzrecht ändern. Erwägungsgrund 46 sollte daher gelöscht werden**.

4.3. Betroffene Personen, die Immunitäten und Vorrechte genießen

55. Der EDSB begrüßt Artikel 5 Absatz 7 des Verordnungsvorschlags, durch den keine EPO in Bezug auf Zugangs-, Transaktions- oder Inhaltsdaten erteilt werden sollten, wenn die Anordnungsbehörde feststellt, dass die Daten von Immunitäten und Vorrechten nach den Rechtsvorschriften des Mitgliedstaates, in dem die Anordnung an den Diensteanbieter gerichtet würde, geschützt sind[98]. Er bedauert, dass die Verpflichtung der Anordnungsbehörde, Immunitäten und Vorrechte zu berücksichtigen und gegebenenfalls keine EPO zu erlassen oder anzupassen, gemäß der allgemeinen Ausrichtung des Rates nur auf Situationen begrenzt wurde, in denen Immunitäten und Vorrechte gemäß den Rechtsvorschriften des Vollstreckungsstaates Transaktionsdaten betreffen und die „Person, deren Daten angefordert werden", ihren Wohnsitz nicht im anordnenden Mitgliedsstaat hat[99].

56. Zudem könnte die Anordnungsbehörde sich vernünftigerweise keiner Immunitäten oder Vorrechte nach dem Recht des Vollstreckungsstaates bewusst sein. Daher begrüßt der EDSB die Tatsache, dass, wenn eine EPO trotz dieser Immunitäten und Vorrechte nach dem Recht des Vollstreckungsstaates erlassen wurde, Artikel 14 Absatz 2 des Verordnungsvorschlags der Vollstreckungsbehörde die Ablehnung der Vollstreckung einer Anordnung ohne Einschränkungen im Hinblick auf die betroffenen Daten ermöglicht[100]. Der EDSB hält allerdings fest, dass die Vollstreckungsbehörde nur in Fällen, in denen der Diensteanbieter aus einem anderen Grund dem Zertifikat nicht entsprochen hätte, einen solchen Einwand erheben könnte[101]. Nach der allgemeinen Ausrichtung des Rates wurde ein solcher Einwand auf Fälle, in denen die „Person, deren Daten angefordert werden", ihren Wohnsitz nicht im Anordnungsstaat hat, und auf Inhaltsdaten begrenzt[102].

57. Er nimmt auch Artikel 18 des Verordnungsvorschlags zur Kenntnis,[103] der vorsieht, dass, wenn Daten trotz dieser Immunitäten und Vorrechte eingeholt würden, „*diese Gründe genauso berücksichtigt werden als wären sie im nationalem Recht vorgesehen*"[104].

58. Der EDSB **empfiehlt die Änderung des Verordnungsvorschlags, um mindestens zu gewährleisten, dass:**
    - **eine EPO nicht erteilt werden kann, wenn die Transaktionsdaten und Inhaltsdaten von Immunitäten und Vorrechten nach dem Recht des vollstreckenden Mitgliedstaats geschützt sind und keine Aufhebung dieser Immunitäten und Vorrechte erreicht werden konnte[105];**

- **für den Vollstreckungsstaat eine Verpflichtung besteht, diesen Grund für alle diese Daten zu prüfen[106].**

4.4. Gesetzlicher Vertreter

59. Wie der EDSA bereits hervorgehoben hat[107], sollte jede Verwirrung in Bezug auf Vertreter, die von den Diensteanbietern, die in der EU Dienstleistungen anbieten, für die Zwecke der Erhebung von Beweismitteln in Strafverfahren benannt wurden, und in Bezug auf Vertreter, die zur Einhaltung von Artikel 27 DSGVO benannt wurden, vermieden werden. In ähnlicher Weise sollte Verwirrung in Bezug auf Vertreter vermieden werden, die zur Einhaltung der vorgeschlagenen Verordnung über Privatsphäre und elektronische Kommunikation benannt werden müssten[108].

60. Vertreter, die zur Einhaltung des Richtlinienvorschlags und der DSGVO benannt wurden, können einige Ähnlichkeiten aufweisen, da sie als Kontaktstelle der Diensteanbieter, die sie vertreten, dienen. Sie würden allerdings Aufgaben und Verantwortungen sehr unterschiedlicher Art haben und verschiedenen Arten von Akteuren Rede und Antwort stehen.[109] Diese beiden Funktionen erfordern unterschiedliche Kenntnisse und Kompetenzen. Außerdem können diese Pflichten zur Bestellung von Vertretern für verschiedene Diensteanbieter gelten, je nachdem, ob sie dem Richtlinienvorschlag oder der DSGVO unterliegen[110]. Daher **empfiehlt der EDSB, klarzustellen, dass diese verschiedenen Arten von Vertretern unterschiedliche Ziele verfolgen und verschiedene Aufgaben und Verantwortungen haben würden**.

4.5. Fristen zur Herausgabe von Daten

61. Eines der Hauptziele des Verordnungsvorschlags ist die Beschleunigung des grenzüberschreitenden Verfahrens zum Erhalt von Beweismitteln in einem anderen Mitgliedstaat im Vergleich zum bestehenden Mechanismus der Zusammenarbeit. Der EDSB hält fest, dass die Fristen gemäß dem Verordnungsvorschlag nicht nur eine Frist zur Gewährleistung einer schnellen Sicherung und Herausgabe von Daten sondern auch den Zeitraum betreffen, in der die Prüfung auf Übereinstimmung der Zertifikate mit den Grundrechten, neben anderen Gründen, stattzufinden hat.

62. Auch wenn der EDSB die Ziele des Verordnungsvorschlags (wie beispielsweise die Verhinderung der Volatilität von Daten oder die Gewährleistung der Wirksamkeit der Strafverfahren) versteht, vertritt er die Ansicht, dass die Fristen in allen Fällen[111] zu kurz sind, um die erhaltenen Zertifikate angemessen zu bewerten und zu ermitteln, ob es Gründe gibt, sie nicht einzuhalten (z. B. Verstoß gegen die Charta oder Rechtskollision) und um eine angemessene Entscheidung zu treffen. Er hält vergleichsweise fest, dass die EEA-Richtlinie für die Justizbehörden im Vollstreckungsstaat eine Frist von 30 Tagen für ihre Beurteilung und Entscheidung über die „*Anerkennung oder Vollstreckung*“ einer Anordnung[112] und 90 Tage nach Treffen dieser Entscheidung für die Durchführung der Ermittlungsmaßnahme[113] vorsieht. Er unterstreicht ebenfalls, dass Artikel 9 Absatz 6 zur Vermeidung der Löschung von angeforderten Daten während der Bewertung des Zertifikats über eine Europäische Herausgabeanordnung den Diensteanbieter in jedem Fall verpflichtet, „*[…] die angeforderten Daten [zu sichern], wenn er sie nicht unverzüglich herausgibt,*“ und “*[d]ie Daten werden so lange gesichert, bis sie herausgegeben werden*“.

63. Daher **empfiehlt der EDSB, längere Fristen als 10 Tage zu setzen, wodurch eine angemessene Beurteilung des Zertifikats sowie der Übermittlung der angeforderten Daten fristgerecht ermöglicht würde.**

64. Der EDSB stellt außerdem fest, dass es der Verordnungsvorschlag – außer in Notfällen – in allen Fällen den Anordnungsbehörden ermöglicht, kürzere Fristen als 10 Tage festzulegen, wenn sie „*Gründe für eine frühere Offenlegung*" angeben. Soweit keine eingehendere Begründung dafür vorgelegt wird, dass den Anordnungsbehörden die Möglichkeit gegeben wird, in allen Fällen selbst kürzere Fristen festzulegen und von den gemäß der EEA-Richtlinie erlaubten Fristen abzuweichen, **empfiehlt der EDSB, diese Möglichkeit für die Anordnungsbehörden, den Diensteanbietern verbindliche Fristen aufzuerlegen, die kürzer als die Frist sind, die im Verordnungsvorschlag vorgesehen ist, zu entfernen.**

65. Nach Ansicht des EDSB könnte die Frist von 6 Stunden zur Herausgabe von Daten in Notfällen schließlich nicht immer realistisch sein und **er empfiehlt, daraus eine bevorzugte Frist anstelle einer verbindlichen Frist zu machen**.

4.6. Einspruchsmöglichkeit für Diensteanbieter

66. Der EDSB befürwortet, dass es der Verordnungsvorschlag den Diensteanbietern ermöglicht, gegen die Vollstreckung einer Anordnung Einspruch einzulegen. Diese Einsprüche sollten allerdings auf einer begrenzte Anzahl von Gründen beruhen. Diese Gründe sollten klar definiert sein, damit Anbieter nicht die Möglichkeit haben, von Fall zu Fall zu entscheiden, ob und wie sie kooperieren. In dieser Hinsicht empfiehlt der EDSB insbesondere die Einführung eines Grundes für den Einspruch gegen die Vollstreckung eines EPOC (Artikel 9) und die Vollstreckung einer EPO (Artikel 14), wenn die Daten nach dem Recht des vollstreckenden Mitgliedstaats durch Immunitäten und Vorrechte geschützt sind (siehe Abschnitt 4.3). Der EDSB hält fest, dass Diensteanbieter nicht verpflichtet sind, diese Gründe vor Vollstreckung der Anordnung zu beurteilen, sondern dass sie nur die Vollstreckung einer Anordnung auf dieser Grundlage „ablehnen können" (Artikel 14 Absatz 4 und 5). Der EDSB könnte einen solchen Ansatz befürworten, wenn andererseits ein echter Überprüfungsmechanismus durch die Behörden eines anderen Mitgliedstaates als des Anordnungsstaates eingeführt würde, wie vorstehend erläutert (siehe Abschnitt 3.4). Der EDSB ist insbesondere besorgt, dass die Tatsache, dass die Diensteanbieter möglichen finanziellen Sanktionen im Falle eines Verstoßes gegen ihre Pflichten unterliegen – unter anderem, die Daten bei Eingang der Zertifikate zu sichern oder zu übermitteln[114] – sie in der Praxis davon abhalten könnte, im Einzelfall Einsprüche zu erheben[115].

4.7. Wechselbeziehungen zu anderen Instrumenten

67. Der EDSB hält fest, dass der Anwendungsbereich des Verordnungsvorschlags so definiert ist, dass er es den zuständigen Behörden in der EU grundsätzlich ermöglichen würde, Daten ungeachtet des Standorts der angeforderten Daten von einem in einem Drittland niedergelassenen Diensteanbieter zu erheben, solange dieser Dienste in der Union anbietet. Der Diensteanbieter oder die Verarbeitung dieser Daten kann somit der Gerichtsbarkeit eines Drittlandes unterliegen, was für Diensteanbieter zu kollidierenden Pflichten nach dem EU-Rahmen einerseits und nach dem Recht eines Drittlandes andererseits führen kann. Der „Stored Communications Act" der Vereinigten Staaten beispielsweise untersagt nach US-Recht grundsätzlich die Offenlegung von Inhaltsdaten durch einen Anbieter elektronischer Kommunikationsdienste[116] auf Ersuchen ausländischer Behörden, soweit solche Ersuchen nicht von Behörden qualifizierter ausländischer Regierungen stammen, die eine

Durchführungsvereinbarung mit den USA[117] abgeschlossen haben und die Daten Nicht-US-Personen betreffen.

68. Die Kommission strebte eine Lösung dieses Problems an, indem sie im Verordnungsvorschlag ein Überprüfungsverfahren vorsieht, das einen Dialog mit den Behörden des betroffenen Drittlandes im Falle von auf Grundrechten basierenden kollidierenden Pflichten (Artikel 15) einrichtet, in dem Bestreben, ausländischen Gesetzgebern bei der Ausgestaltung ihrer eigenen Rechtsvorschriften ein Beispiel zu geben[118]. Gleichzeitig gab die Kommission Empfehlungen für Beschlüsse des Rates zur Aufnahme von Verhandlungen mit den USA über ein internationales Übereinkommen und die Ermächtigung zur Aushandlung des zweiten Zusatzprotokolls zum Übereinkommen über Computerkriminalität im Auftrag der EU (siehe Abschnitt 1). Im Mai 2019 nahm der Rat die Beschlüsse an[119]. Die Verhandlungsrichtlinien für ein Abkommen zwischen der EU und den USA sehen konkrete Ziele vor, darunter „*Rechtskollisionen zu regeln*“ und „*gemeinsame Regeln für Anordnungen zum Erhalt von elektronischen Beweismitteln in Form von Inhalts- und Nichtinhaltsdaten von einer Justizbehörde in einem Vertragsstaat, die an einen Diensteanbieter gerichtet sind, der dem Recht des anderen Vertragsstaats unterliegt, festzulegen*“[120]. Die Verhandlungsrichtlinien zum zweiten Zusatzprotokoll zum Übereinkommen über Computerkriminalität sehen vor, dass das Protokoll *„eine Bestimmung [enthalten sollte], die vorsieht, dass Mitgliedstaaten in ihren Beziehungen zueinander weiterhin die Vorschriften der Europäische Union anstatt der des zweiten Zusatzprotokolls anwenden“*[121]. Zum gegenwärtigen Zeitpunkt ist jedoch nicht klar, auf Grundlage welcher Kriterien die Abgrenzung zwischen grenzüberschreitenden Fällen innerhalb der EU (d. h. Fälle, die in den Anwendungsbereich der Vorschläge fallen) und internationalen Fällen (d. h. Fälle, die unter ein internationales Übereinkommen fallen) vorgenommen werden wird. Diesbezüglich nahm der EDSB die Bestimmung zur Kenntnis, die der Rat in seine allgemeine Ausrichtung aufnahm (Artikel 23)[122]. **Der EDSB empfiehlt allerdings, mehr Klarheit zu diesem Problem zu schaffen, um Rechtssicherheit zu gewährleisten.** Das ist für die Rechtmäßigkeit jeglicher Verarbeitung personenbezogener Daten in diesem Zusammenhang wichtig.

69. Der EDSB erinnert daran, dass, soweit der Datenschutz betroffen ist, die Kommunikation personenbezogener Daten an Behörden von Drittländern zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Strafverfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen in Ermangelung von internationalen Übereinkommen, die auf die Beweisaufnahme in Strafsachen zwischen dem betreffenden Mitgliedstaat und dem betreffenden Drittstaat anwendbar sind, nur in Übereinstimmung mit den Übermittlungsregeln gemäß Kapitel V der Richtlinie zum Datenschutz bei der Strafverfolgung für Polizei und Justiz stattfinden darf. Im Allgemeinen **betont der EDSB, dass es wichtig ist, zu gewährleisten, dass der endgültige Wortlaut des Verordnungsvorschlags das hohe Datenschutzniveau in der EU beibehält,** sodass er bei der Aushandlung eines internationalen Übereinkommens über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln **eine Referenz darstellt, die die Wahrung der Grundrechte, einschließlich des Rechts auf Privatsphäre und des Rechts auf Datenschutz, gewährleistet und solide Garantien vorsieht.**

5. SCHLUSSFOLGERUNGEN

70. Der EDSB **befürwortet die Zielsetzung**, zu gewährleisten, dass den Strafverfolgungs- und Justizbehörden wirksame Instrumente zur Verfügung stehen, um Straftaten in einer von

neuen Technologien veränderten Welt zu ermitteln und zu verfolgen. Gleichzeitig möchte der EDSB sicherstellen, dass diese Maßnahme in vollem Umfang der Charta und dem EU-Besitzstand in Sachen Datenschutz Rechnung tragen. Der Verordnungsvorschlag würde die Speicherung und Kommunikation personenbezogener Daten innerhalb und außerhalb der EU zwischen den zuständigen Behörden der Mitgliedstaaten, privatrechtlichen juristischen Personen und in einigen Fällen den Behörden von Drittländern erforderlich machen. Er würde mit Einschränkungen in Bezug auf die beiden Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten, die durch Artikel 7 und 8 der Charta garantiert werden, einhergehen. Diese Einschränkungen müssen den in Artikel 52 Absatz 1 der Charta niedergelegten Bedingungen entsprechen und insbesondere der Bedingung der Notwendigkeit einhalten, damit sie rechtmäßig sind.

71. Erstens ist der EDSB der Auffassung, dass andere **Alternativen,** die umfassendere Garantien biete und dabei die gleichen Ziele erreichen, eingehender geprüft werden sollten.

72. Zweitens nimmt der EDSB zur Kenntnis, dass der Verordnungsvorschlag bereits eine Reihe von Verfahrensgarantien enthält. Allerdings ist der EDSB besorgt, dass die wichtige Verantwortung der Überprüfung der Vereinbarkeit von EPOC und EPOC-PR mit der Charta den Diensteanbietern übertragen wird, und empfiehlt, die **die vom Vollstreckungsstaat benannten Justizbehörden** so früh wie möglich in den Prozess der Erhebung von elektronischen Beweismitteln **einzubeziehen**.

73. Der EDSB empfiehlt, die Kohärenz zwischen den Definitionen der Kategorien der elektronischen Beweismitteldaten und der im EU-Recht bestehenden **Definitionen spezifischer Datenkategorien** zu verbessern und **die Kategorie der Zugangsdaten zu überprüfen** oder den Zugang zu diesen Daten ähnlichen Bedingungen wie denen für den Zugang zu den Kategorien der Transaktionsdaten und Inhaltsdaten zu unterwerfen. Der Verordnungsvorschlag sollte klare und einfache Definitionen jeder Datenkategorie enthalten, um Rechtssicherheit für alle betroffenen Akteure zu gewährleisten. Er empfiehlt ebenso, **die vorgeschlagene Definition der Kategorie der Teilnehmerdaten zu ändern,** um sie zu konkretisieren.

74. Er empfiehlt außerdem **die Neubewertung des ausgewogenen Verhältnisses zwischen der Arten von Straftaten, für die EPOs erlassen werden könnten, und den betreffenden Datenkategorien** unter Berücksichtigung der jüngsten einschlägigen Rechtsprechung des EuGH. Insbesondere die Möglichkeit, eine EPO zur Herausgabe von Transaktionsdaten und Inhaltsdaten zu erlassen, sollte auf schwere Straftaten beschränkt werden. Der EDSB würde im Idealfall die Definition einer starren Liste schwerer Straftaten für EPOs zur Herausgabe von Transaktionsdaten und Inhaltsdaten, die auch die Rechtssicherheit für alle betroffenen Akteure erhöhen wird, vorziehen.

75. Der EDSB gibt auch Empfehlungen, die darauf abzielen, die Achtung der Rechte auf Datenschutz und Privatsphäre zu gewährleisten und zugleich eine rasche Erhebung von Beweismitteln für spezifische Strafverfahren zu erreichen. Sie konzentrieren sich auf die **Sicherheit der Übermittlung** von Daten zwischen allen betroffenen Akteuren, die **Echtheit** von Anordnungen und Zertifikaten und die **begrenzte Sicherung** von Daten im Rahmen einer EPO-PR.

76. Über die vorstehenden allgemeinen Anmerkungen und Hauptempfehlungen hinaus hat der EDSB in dieser Stellungnahme bezüglich folgender Aspekte der Vorschläge weitere Empfehlungen formuliert:
    - **Verweis auf den geltenden Rechtsrahmen für den Datenschutz**;
    - **Rechte betroffener Personen** (höhere Transparenz und das Recht auf Rechtsmittel);
    - betroffene Personen, die **Immunitäten und Vorrechte** genießen;
    - **Bestellung von Vertretern** für das Erheben von Beweismitteln in Strafsachen;
    - **Fristen zur Einhaltung** eines EPOC und zur Herausgabe der Daten;
    - Möglichkeit für **Diensteanbieter, auf Grundlage einer begrenzten Anzahl von Gründen Einspruch gegen Anordnungen zu erheben**.

77. Schließlich ist dem EDSB der **weitere Kontext** bekannt, in dem die Initiative vorgestellt und die beiden Beschlüsse des Rates angenommen wurden, einer in Bezug auf das zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität beim Europarat und einer in Bezug auf die Aufnahme von Verhandlungen mit den Vereinigten Staaten. Er bittet um mehr Klarheit in Bezug auf die Wechselwirkungen des Verordnungsvorschlags zu internationalen Übereinkommen. Dem EDSB liegt daran, konstruktive Beiträge zu leisten, um Kohärenz und Vereinbarkeit zwischen den endgültigen Textfassungen und dem EU-Datenschutzrahmen zu gewährleisten.

Brüssel, 6. November 2019

Wojciech Rafał WIEWIÓROWSKI
Stellvertretender Datenschutzbeauftragter

ANMERKUNGEN

[1] ABl. L 295 vom 21.11.2018, S. 39.
[2] ABl. L 119 vom 4.5.2016, S. 1 (nachstehend „DSGVO“).
[3] ABl. L 119 vom 4.5.2016, S. 89 (nachstehend „Richtlinie zum Datenschutz bei der Strafverfolgung“).
[4] Arbeitsdokument der Kommissionsdienststellen: Folgenabschätzung, SWD(2018) 118 final (im Folgenden „Folgenabschätzung“), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=SWD%3A2018%3A118%3AFIN.
[5] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, COM(2018) 225 final.
[6] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren, COM(2018) 226 final.
[7] Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen, ABl. L 130 vom 1.5.2014, S. 1, siehe Artikel 23 des Verordnungsvorschlags.
[8] In der EEA-Richtlinie ist eine direkte Zusammenarbeit zwischen der Anordnungsbehörde in einem Mitgliedstaat und der Vollstreckungsbehörde eines anderen Mitgliedstaates vorgesehen oder, je nach Lage des Falles, über die vom betreffenden Mitgliedstaat/von den betreffenden Mitgliedstaaten benannte(n) zentrale(n) Behörde(n). Sie bezweckt die Erleichterung und Beschleunigung dieser Zusammenarbeit, indem standardisierte Formulare und strenge Fristen vorgesehen und mehrere Hindernisse für die grenzüberschreitende Zusammenarbeit entfernt werden; zum Beispiel: *„[d]ie Anordnungsbehörde kann eine EEA erlassen, damit Maßnahmen ergriffen werden, mit denen die Vernichtung, Veränderung, Entfernung, Übertragung oder Veräußerung von Gegenständen, die als Beweismittel dienen können, vorläufig verhindert wird“* und *„[d]ie Vollstreckungsbehörde entscheidet so schnell wie möglich und sofern praktikabel innerhalb von 24 Stunden nach Erhalt der EEA über die vorläufige Maßnahme und teilt diese Entscheidung innerhalb der genannten Frist mit“* (Artikel 32); auch die Vollstreckung einer EEA zur Identifizierung von Inhabern eines bestimmten Telefonanschlusses oder einer bestimmten IP-Adresse unterliegt nicht dem Erfordernis der beiderseitigen Strafbarkeit (Artikel 10 Absatz 2 Buchstabe e in Verbindung mit Artikel 11 Absatz 2).
[9] Alle EU-Mitgliedstaaten mit Ausnahme Dänemarks und Irlands.
[10] Alle teilnehmenden Mitgliedstaaten haben die EEA-Richtlinie 2017 oder 2018 in einzelstaatliches Recht umgesetzt. Siehe den Stand der Umsetzung im Europäischen Justiziellen Netz für Strafsachen: https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?l=DE&CategoryId=120.
[11] Der durch Artikel 68 DSGVO eingerichtete EDSA löste auf die Datenschutzgruppe ab, die durch Artikel 29 der aufgehobenen Richtlinie 95/46/EC eingerichtet wurde. Der EDSA besteht, ähnlich wie die Artikel-29-Datenschutzgruppe, aus Vertretern der nationalen Datenschutzbehörden und dem EDSB.
[12] Stellungnahme 23/2018 vom 26. September 2018 zu den Vorschlägen der Kommission über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (Artikel 70 Absatz 1 Buchstabe b) (im Folgenden „EDSA-Stellungnahme 23/2018“), abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf.
[13] https://www.consilium.europa.eu/de/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/.
[14] https://www.consilium.europa.eu/de/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/.
[15] Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen, COM(2019) 70 final.
[16] 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. Alle Mitgliedstaaten haben das Übereinkommen des Europarats über eine verstärkte internationale Zusammenarbeit bezüglich Computerkriminalität und elektronische Beweismittel unterzeichnet und fast alle haben es ratifiziert. Irland und Schweden befinden sich noch im Ratifizierungsverfahren des Übereinkommens über Computerkriminalität. Das Übereinkommen über Computerkriminalität ist eine verbindliche internationale Übereinkunft, mit der sich die Vertragsstaaten verpflichten, spezifische, gegen elektronische Netzwerke gerichtete oder durch elektronische Netzwerke begangene Straftaten in ihr nationales Recht aufzunehmen und spezifische Vollmachten und Verfahren festzulegen, mit Hilfe derer ihre nationalen Behörden ihre Ermittlungsverfahren, einschließlich des Sammelns von Beweisen einer Straftat in elektronischer Form, durchführen können. Das Übereinkommen fördert zudem die internationale Zusammenarbeit zwischen den Vertragsstaaten. Es gibt spezifische Maßnahmen, um den mit der Volatilität der Daten verbundenen Herausforderungen zu begegnen. Hierzu sieht das Übereinkommen die beschleunigte Sicherung der gespeicherten Computerdaten vor. Da die

Übermittlung der gesicherten Beweismittel an den ersuchenden Mitgliedstaat einer endgültigen Entscheidung über das formelle Rechtshilfeersuchen unterliegt, sind nicht alle Ablehnungsgründe auf die Sicherung anwendbar; insbesondere die beiderseitige Strafbarkeit ist nur in Ausnahmefällen erforderlich (Artikel 29).

[17] Stellungnahme 2/2019 des EDSB zu dem Mandat für die Verhandlung eines Abkommens zwischen der EU und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln und die Stellungnahme 3/2019 des EDSB zu der Teilnahme an den Verhandlungen mit Blick auf ein Zweites Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität.

[18] Abrufbar unter: https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

[19] https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_de.

[20] https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

[21] Begründung des Verordnungsvorschlags, S. 2.

[22] Gerichtshof der Europäischen Union (im Folgenden „EuGH"), verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger, ECLI:EU:C:2014:238, Rn. 33, in der das Gericht in Verbindung mit der Feststellung einer Einschränkung des Rechts auf Achtung der Privatsphäre feststellte, dass „*es nicht darauf an[kommt], ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben könnten*". Siehe auch EuGH, Rechtssache C-207/16, Ministerio Fiscal, ECLI:EU:C:2018:788, Rn. 51.

[23] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger, ECLI:EU:C:2014:238, Rn. 36, in der das Gericht feststellte, dass eine Maßnahme „*in das durch Art. 8 der Charta garantierte Grundrecht auf den Schutz personenbezogener Daten ein[greift], da sie eine Verarbeitung personenbezogener Daten vorsieht*".

[24] Abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_de.pdf. Siehe Abschnitt II 4) des Instrumentariums zur Beurteilung der Notwendigkeit („Necessity Toolkit") des EDSB, S. 7, und EuGH, Gutachten 1/15, ECLI:EU:C:2017:592, Rn. 140: „*Zum Grundsatz der Verhältnismäßigkeit ist festzustellen, dass der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das absolut Notwendige beschränken (...)* ".

[25] Grenzüberschreitende Situationen beziehen sich auf Situationen, in denen der adressierte Diensteanbieter in einem anderen Mitgliedstaat als dem der Anordnungsbehörde niedergelassen oder vertreten ist.

[26] Innerstaatliche Situationen beziehen sich auf Situationen, in denen der adressierte Diensteanbieter in demselben Mitgliedstaat wie die Anordnungsbehörde niedergelassen oder vertreten ist. In solchen Fällen müssen Behörden dieses Mitgliedstaats nationale Maßnahmen ergreifen, um den Dienstleister zu zwingen. Siehe Erwägungsgrund 15 des Verordnungsvorschlags.

[27] Siehe Artikel 2 Absatz 4 des Verordnungsvorschlags bezüglich der Definition von „*der/die in der Union Dienstleistungen anbietet/anbieten*". Das bedeutet, dass Personen in einem oder in mehreren Mitgliedstaaten nicht nur die Nutzung der aufgeführten Dienstleistungen, sondern auch eine wesentliche Verbindung zu einem solchen Mitgliedstaat/zu solchen Mitgliedstaaten ermöglicht wird.

[28] Begründung des Richtlinienvorschlags, S. 3; siehe auch Artikel 7 des Verordnungsvorschlags. Artikel 7 Absatz 1 sieht vor, dass eine EPO und eine EPO-PR direkt an den vom betreffenden Diensteanbieter benannten Vertreter gerichtet wird. Artikel 7 Absatz 2 sieht als Alternative Folgendes: „*Wenn kein Vertreter zu diesem Zweck benannt wurde, können die Europäische Herausgabeanordnung und die Europäische Sicherungsanordnung an eine beliebige Niederlassung des Diensteanbieters in der Union gerichtet werden*".

[29] Artikel 3 des Richtlinienvorschlags sieht vor, dass die Mitgliedstaaten sicherstellen, dass Diensteanbieter, die in der EU Dienstleistungen anbieten, mindestens einen Vertreter in der Union benennen, und das ungeachtet dessen, ob sie eine Niederlassung in der EU haben oder nicht.

[30] Gemäß Artikel 7 des Verordnungsvorschlags ist der Adressat der Anordnungen grundsätzlich der vom Diensteanbieter benannte Vertreter; in einigen Fällen kann er die Niederlassung des Diensteanbieters in der EU sein. Die Begriffe „Diensteanbieter" und „Adressat" werden in dieser Stellungnahme zur Benennung des Vertreters oder der Niederlassung verwendet, an den oder an die eine Anordnung durch ein Zertifikat übermittelt wird.

[31] Folgenabschätzung, S. 94, 156 und 179.

[32] Die Rechte aus Artikel 6 sind die durch Artikel 5 der Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten gewährten Rechte und in Übereinstimmung mit Artikel 52 Absatz 3 der Charta haben sie die gleiche Bedeutung und den gleichen Anwendungsbereich. Siehe Erläuterungen zur Charta der Grundrechte (2007/C 303/02).

[33] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger, ECLI:EU:C:2014:238, Rn. 54-55.

[34] Siehe Rede von Prof. Koen Lenaerts, Präsident des EuGH, auf einer Nebenveranstaltung der 40. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre („The General Data Protection Regulation five months on"), abrufbar unter: https://webcast.ec.europa.eu/the-general-data-protection-regulation-five-months-on-25-10-2018#.

[35] Begründung des Verordnungsvorschlags, S. 18: *„Transaktions- und Inhaltsdaten sollten strengeren Anforderungen unterliegen, um dem sensibleren Charakter solcher Daten und der im Vergleich zu Teilnehmer- und Zugangsdaten entsprechend höheren Invasivität von Anordnungen bezüglich derartiger Daten Rechnung zu tragen".*

[36] Diese Anforderungen sind in den Artikeln 4, 5 und 6 des Verordnungsvorschlags niedergelegt und betreffen die Straftaten, für die Anordnungen zur Herausgabe oder Sicherung dieser Datenkategorien erlassen werden können, und die Justizbehörde, die die Anordnung erteilt oder bestätigt.

[37] Artikel 4 Absatz 3 Buchstabe a des Verordnungsvorschlags über Privatsphäre und elektronische Kommunikation definiert „elektronische Kommunikationsdaten" als „*elektronische Kommunikationsinhalte und elektronische Kommunikationsmetadaten*".

[38] Artikel 4 Absatz 3 Buchstabe b des Verordnungsvorschlags über Privatsphäre und elektronische Kommunikation definiert „elektronische Kommunikationsinhalte" als „*Inhalte, die mittels elektronischer Kommunikationsdienste übermittelt werden, z.B. Textnachrichten, Sprache, Videos, Bilder und Ton*".

[39] Artikel 4 Absatz 3 Buchstabe c des Verordnungsvorschlags über Privatsphäre und elektronische Kommunikation definiert „elektronische Kommunikationsmetadaten" als „*Daten, die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden; dazu zählen die zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts einer Kommunikation verwendeten Daten, die im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdienste erzeugten Daten über den Standort des Geräts sowie Datum, Uhrzeit, Dauer und Art der Kommunikation*".

[40] https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_de.

[41] Begründung des Verordnungsvorschlags, S. 2: *„Mit diesem Vorschlag soll die Rechtssicherheit für Behörden, Diensteanbieter und betroffene Menschen verbessert und zugleich dafür gesorgt werden, dass Ersuchen von Strafverfolgungsbehörden weiterhin hohen Standards genügen und somit der Schutz der Grundrechte, Transparenz und Rechenschaftspflicht gewährleistet werden"*

[42] Begründung des Verordnungsvorschlags, S. 17.

[43] Folgenabschätzung, S. 129: *„Die Definition der Datentypen (Teilnehmer-, Verkehrs- und Inhaltsdaten) weicht innerhalb der Mitgliedstaaten deutlich voneinander ab, wobei spezifische Datenkategorien in mehreren Ländern bestehen. Vom Diensteanbieter angeforderte Daten sind im Allgemeinen Teilnehmerdaten (21 Mitgliedstaaten) und Verkehrsdaten (18 Mitgliedstaaten), wobei es in einigen Mitgliedstaaten (9) auch möglich ist, Inhaltsdaten und „sonstige Daten" (4 Mitgliedstaaten) anzufordern."*

[44] Siehe Stellungnahme 23/2018 des EDSA, S. 14: *„[D]ie vier vorgeschlagenen Kategorien [erscheinen] nicht klar abgegrenzt, und die Definition von „Zugangsdaten" bleibt [...] weiterhin unklar."*

[45] Artikel 18 Absatz 3 des Übereinkommen über Computerkriminalität definiert „Bestandsdaten" als „*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.*"

[46] Siehe Ausschuss zum Übereinkommen über Computerkriminalität des Europarats, „Bedingungen für das Einholen von Bestandsdaten in Verbindung mit dynamischen gegenüber statischen IP-Adressen: Überblick über die maßgeblichen Gerichtsentscheidungen und Entwicklungen", T-CY (2018)26, 25. Oktober 2018, zu der Frage, ob dynamische IP-Adressen Vorschriften zur Einholung von Bestandsdaten oder Vorschriften zur Einholung von Verkehrsdaten unterworfen werden sollten (entsprechend der Definition nach Artikel 1 Buchstabe d des Übereinkommens). Der Ausschuss gelangt dabei zu der Schlussfolgerung, dass *„die Einführung neuer Datenkategorien, wie beispielsweise „Zugangsdaten", zu weiteren Missverständnissen im Hinblick auf die anwendbaren Vorschriften zur Vorratsspeicherung von oder Zugang zu diesen Daten führt und von den betreffenden Personen nur schwer anzuwenden sind".*

[47] Siehe Schlussanträge des Generalanwalts, Rechtssache C-207/16, Ministerio Fiscal, ECLI:EU:C:2018:300, Rn. 117 und Rn. 118:
„(...) der Gerichtshof (...) verzichtet (darauf), sich für ein bestimmtes Strafmaß auszusprechen, weil das, was für manche Mitgliedstaaten angemessen ist, für andere nicht notwendig angemessen sein wird und das, was heute für eine bestimmte Art von Straftat gilt, nicht notwendig unwiderruflich für die Zukunft gilt (...)

(...) (...) (Ich) stelle (...) fest, dass vorliegend das vorlegende Gericht auf die, oben bereits erwähnte (132), Gefahr einer Umkehrung des Grundsatzes und der in der Richtlinie 2002/58 vorgesehenen Ausnahmen hinweist, indem es erklärt, dass „[d]ie Bezugnahme auf die Strafe – wobei der [vom spanischen Gesetzgeber 2015 eingeführte (133)] Strafrahmen mindestens drei Jahre Freiheitsentzug erreichen muss – ... eine deutliche Mehrheit der Straftypen [umfasst]". Die aktuelle, durch die Reform der Strafprozessordnung eingeführte Liste der Straftaten, die in Spanien Beschränkungen der gemäß den Art. 7 und 8 der Charta geschützten Rechte rechtfertigen können, würde mit anderen Worten nach diesem Gericht dazu führen, dass die Mehrheit der im Strafgesetzbuch geregelten Straftaten Bestandteil dieser Liste wäre.".

[48] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger, ECLI:EU:C:2014:238, Rn. 27.

[49] EuGH, verbundene Rechtssachen C-203/15 und C-698/15, Tele2 Sverige und Watson, ECLI:EU:C:2016:970, Rn. 99.

[50] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger, ECLI:EU:C:2014:238, Rn. 39 und EuGH, verbundene Rechtssachen C-203/15 und C-698/15, Tele2 Sverige und Watson, ECLI:EU:C:2016:970, Rn. 101.

[51] EuGH, Rechtssache C-207/16, Ministerio Fiscal, ECLI:EU:C:2018:788, Rn. 54 und 56.

[52] Siehe Schlussanträge des Generalanwalts, Rechtssache C-207/16, Ministerio Fiscal, ECLI:EU:C:2018:300, die Hinweise zu den Kriterien gaben, die zur Definition von „schweren Straftaten" im Sinne der Rechtsprechung des EuGH verwendet werden könnten, einschließlich im Hinblick auf das Kriterium des eingetretenen Urteils.

[53] Folgenabschätzung, S. 240.

[54] EuGH, Rechtssache C-207/16, Ministerio Fiscal, ECLI:EU:C:2018:788.

[55] Siehe Abschnitt 3.1 dieser Stellungnahme über die Notwendigkeit, diese Datenkategorien im Verordnungsvorschlag klarzustellen.

[56] Personenbezogene Daten müssen in einer Weise verarbeitet werden, die ihre angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (Grundsatz der „Integrität und Vertraulichkeit" nach Artikel 5 Absatz 1 Buchstabe f DSGVO und Artikel 4 Absatz 1 Buchstabe f der Richtlinie zum Datenschutz bei der Strafverfolgung). Die Verarbeitungssicherheit deckt insbesondere die Fähigkeit ab, die fortlaufende Vertraulichkeit und Integrität von Verarbeitungssystemen sicherzustellen.

[57] Erwägungsgrund 57 gibt an, dass *„die Mitgliedstaaten sicherstellen [sollten], dass für die Übermittlung personenbezogener Daten von den zuständigen Behörden an die Diensteanbieter [...] geeignete Datenschutzvorkehrungen und -maßnahmen gelten, [...] zur Gewährleistung der Datensicherheit. Die Diensteanbieter sollten für die Übermittlung personenbezogener Daten an die zuständigen Behörden dasselbe sicherstellen. Der Zugang zu Informationen mit personenbezogenen Daten sollte befugten Personen vorbehalten sein, wofür durch Authentifizierungsverfahren gesorgt werden kann. Zur Gewährleistung der Authentifizierung sollte die Verwendung von Mechanismen erwogen werden, beispielsweise der notifizierten nationalen elektronischen Identifizierungssysteme oder Vertrauensdienste gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG".*

[58] Artikel 8 Absatz 2 sieht nur vor, dass *„[d]ie Übermittlung des EPOC oder des EPOC-PR direkt und in einer Form [erfolgt], die einen schriftlichen Nachweis unter Bedingungen ermöglicht, die dem Adressaten die Feststellung der Echtheit gestatten"* [Unterstreichung hinzugefügt].

[59] Artikel 9 sieht vor, dass *„der Adressat dafür [sorgt], dass die angeforderten Daten [...] direkt an die Anordnungsbehörde [...] gemäß den Angaben im EPOC übermittelt werden"*. Er bezieht sich nicht auf angemessene Sicherheitsmaßnahmen für die Übermittlung der durch die Adressaten der EPOC herausgegebenen Daten. Der Verordnungsvorschlag regelt nicht die Sicherheit der Kommunikation nach Übermittlung einer EPOC-PR.

[60] Artikel 14 Absatz 1 sieht nur vor, dass die Anordnungsbehörde die Anordnung mit anderen Dokumenten *„in einer Form, die einen schriftlichen Nachweis unter Bedingungen ermöglicht, die dem Adressaten die Feststellung der Echtheit gestatten"*, übermitteln kann [Unterstreichung hinzugefügt].

[61] Artikel 8 der allgemeine Ausrichtung zum Verordnungsvorschlag.

[62] Artikel 9 der allgemeine Ausrichtung zum Verordnungsvorschlag.

[63] Begründung des Verordnungsvorschlags, S. 2.

[64] Siehe Folgenabschätzung in der Anfangsphase über grenzüberschreitenden elektronischen Rechtsverkehr in Europa (e-CODEX), abrufbar unter: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3600084_de, S. 1: *„„e-CODEX" ist ein IT-System für grenzüberschreitende justizielle Zusammenarbeit, dass den Nutzern, seien es Justizbehörden, Rechtspraktiker oder Bürger, das Senden und Empfangen von Unterlagen, Rechtsformularen, Beweismitteln oder anderen Informationen auf sichere Weise ermöglicht. Es wird als ein*

dezentralisiertes Netzwerk mit Zugangspunkten betrieben, die einzelstaatliche und europäische IT-Systeme miteinander verknüpfen. Eine spezielle Software ist zur Einrichtung eines e-CODEX-Zugangspunkts erforderlich. Das e-CODEX-System wurde im Zusammenhang mit dem digitalen Binnenmarkt von einer Gruppe aus Mitgliedstaaten mit Hilfe von EU-Subventionen entwickelt. Verschiedene Mitgliedstaaten verwenden bereits e-CODEX zur Unterstützung grenzüberschreitender Rechtsverfahren sowohl in zivilrechtlichen als auch strafrechtlichen Angelegenheiten, beispielsweise für den Austausch von Ersuchen zur gegenseitigen Rechtshilfe zwischen Staatsanwaltschaften".

Siehe auch die e-Codex-Website, die angibt, dass das Projekt zu Ende gegangen ist, aber dass *„das Ziel von Me-CODEX (Maintenance of e-CODEX (Wartung von e-CODEX)) darin besteht, die Zeit zwischen dem Ende von e-CODEX als Projekt und der Aufnahme der Wartung von e-CODEX durch eine EU-Agentur zu überbrücken. Es wird 2-4 Jahre dauern, um die notwendige Erweiterung des Mandats der EU-Agentur umzusetzen. Da die Mitgliedstaaten, die Informationen über e-CODEX austauschen, ihre Lösungen nicht nach dem Ende von e-CODEX als Projekt abschalten werden, muss eine vorübergehende Wartungslösung gefunden werden. Die Europäische Kommission hat die ständige Sachverständigengruppe zu e-CODEX gedrängt, eine Lösung vorzulegen, um den Betrieb sicherzustellen und die Nutzergemeinschaft zu erweitern. Die Lösung, „Me-CODEX", wird auf eine reibungslose Übergabe an eine EU-Agentur, auf die Wartung der e-CODEX-Bausteine, auf der Ausweitung auf andere Länder, Akteure/Management der Gemeinschaft und F&E hinwirken. Die Unterstützung für andere grenzüberschreitende Rechtsverfahren als die bereits von e-CODEX unterstützten Rechtsverfahren erfordert unterschiedliche Projekte. Die Projekte können natürlich auf das Betriebsmanagement von Me-CODEX bauen"*, abrufbar unter: https://www.e-codex.eu/sites/default/files/newsletter/newsletter_2016-6.html.

[65] Für weitere Informationen über SIRIUS siehe Antwort der Kommission auf die schriftliche Frage E-007204/2017: *„Da aus den Mitgliedstaaten immer mehr Ersuchen um operative Unterstützung eingehen, hat die EU-Meldestelle für Internetinhalte (EU IRU) bei Europol vor kurzem SIRIUS gestartet, um strafrechtliche Ermittlungen im Internet zu unterstützen. SIRIUS schafft sichere Rahmenbedingungen für Informationen im Zusammenhang mit Online-Diensteanbietern und enthält Leitfäden, Tipps, Foren, Fragen & Antworten sowie Tools der Strafverfolgungsbehörden zur Unterstützung von Ermittlungen im Internet. Es umfasst auch Anleitungen für Ermittler über die Arten von Daten, die direkt von den Diensteanbietern abgerufen werden können.*

SIRIUS enthält keine personenbezogenen Daten oder Anträge auf Löschung von Nutzerkonten. Es ist ein Instrument, das den Aufbau von Kapazitäten und den Austausch von Wissen fördert. Derzeit sind 372 Vertreter von Strafverfolgungsbehörden aus den EU-Mitgliedstaaten als SIRIUS-Nutzer registriert. Zur Unterstützung ihrer Ermittlungen im Internet nutzen sie die Leitlinien zu 19 Online-Diensteanbietern sowie 13 Instrumente, die von der EU IRU und den Mitgliedstaaten bereitgestellt wurden.

Die EU IRU arbeitet nach wie vor daran, terroristische Inhalte an die betroffenen Internetplattformen zu melden. Bislang hat die EU IRU 42 066 Einzelinhalte geprüft und in 40 714 Fällen beschlossen, die Inhalte zu melden; dies betraf 80 Plattformen in über 10 Sprachen."

[66] Begründung des Verordnungsvorschlags, S. 21.

[67] Siehe allgemeine Ausrichtung des Rates 15292/18, Fußnote 33, S. 35.

[68] Artikel 22 des Verordnungsvorschlags und Artikel 6 des Richtlinienvorschlags.

[69] Siehe beispielsweise Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates vom 12. Dezember 2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen, ABl. L 351, 20.12.2012, S. 1, insbesondere Artikel 75 und 81, deren Informationsmitteilungspflichten ein Jahr vor Beginn der Anwendung der anderen Bestimmungen der Verordnung erfüllt werden mussten.

Gemäß Artikel 4 Absatz 12 DSGVO und Artikel 3 Absatz 11 der Richtlinie zum Datenschutz bei der Strafverfolgung ist eine Verletzung des Schutzes personenbezogener Daten als „*eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden*" definiert.

[70] Siehe Artikel 11 des Verordnungsvorschlags.

[71] Siehe http://www.ejtn.eu/Documents/About%20EJTN/Criminal%20Justice%202017/CJSWG%20meeting%20Brussels%2013-14%20March%202017/COMMON%20CONCLUSIONS%20EJTN%20Barcelona%20seminar.pdf

[72] Siehe Liste der Gründe für eine Ablehnung in Artikel 14 und die Rechtsprechung des EuGH im Rahmen des Europäischen Haftbefehls (EuGH, Rechtssache C-404/15, Pál Aranyosi und Robert Căldăraru gegen Generalstaatsanwaltschaft Bremen, ECLI:EU:C:2016:198, Rn. 82ff).

[73] Siehe Agentur der Europäischen Union für Grundrechte, Gutachten zu dem Richtlinienentwurf über die Europäische Ermittlungsanordnung, 14. Februar 2011, S. 10: *„Im Allgemeinen muss das Sekundärrecht der EU die Grundrechtestandards einhalten. Siehe EuGH, verbundene Rechtssachen C-92 und 93/09, Volker und Markus*

Schecke GbR und Hartmut Eifert v. Land Hessen, in denen der EuGH eine Rechtsvorschrift des Sekundärrechts der EU wegen Nichtübereinstimmung mit den Grundrechten niederschlug".

[74] „*Siehe Artikel 70 AEUV*".

[75] „*Das Asylsystem der EU, in dem das Primärrecht die Grundsätze festlegt, dass die Mitgliedstaaten füreinander als „sichere Herkunftsländer gelten", erlaubt weiterhin die Abweichung von dieser Vermutung, um zu gewährleisten, dass die Grundrechte einer Person in Ausnahmefällen berücksichtigt werden können. Siehe einziger Artikel Buchstabe d des Protokolls 24 zu den Verträgen*".

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

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

[78] Erwägungsgrund 35c der allgemeinen Ausrichtung des Rates scheint diese Begrenzung der folgenden Begründung zu rechtfertigen: „*Bei Inhaltsdaten handelt es sich im Gegensatz zu Nichtinhaltsdaten um besonders sensible Daten, da damit unter Umständen persönliche Gedanken sowie sensible Einzelheiten aus dem Privatleben preisgegeben werden. Dadurch ist es gerechtfertigt, diese Daten anders zu behandeln und die Behörden des Vollstreckungsstaats frühzeitig in das Verfahren einzubeziehen."*. Der EDSB erinnert diesbezüglich daran, dass gemäß seinem Plädoyer bei der gemeinsamen Anhörung von Rechtsache C-623/17 (Privacy International) mit den verbundenen Rechtssachen C-511/18 und C-512/18 (La Quadrature du Net u. a.) und der Rechtssache C-520/18 (Ordre des barreaux francophones et germanophone u. a.), „*sonstige Daten in Bezug auf elektronische Kommunikation – sogenannte Metadaten (...) genauso offenlegend wie die tatsächlichen Inhalte der Kommunikation sein können. Wir sollten ebenfalls beachten, dass die Unterscheidung von „Inhalts-" und „Metadaten" in einer multiplen Dienstumgebung wie dem Internet nicht eindeutig ist. Daher rät der EDSB im Rahmen des Vorschlags für die Verordnung über Privatsphäre und elektronische Kommunikation, Metadaten sowie Inhaltsdaten ein hohes Schutzniveau zuzuweisen*", siehe Plädoyer des EDSB (S. 4-5), abrufbar auf der Website des EDSB: https://edps.europa.eu/data-protection/our-work/publications/court-cases/edps-pleading-hearing-court-justice-cases-c-62317_de

[79] Folgenabschätzung, S. 14. *„Ersuchen um Nicht-Inhaltsdaten übersteigen diejenigen um Inhalt innerhalb der EU und darüber hinaus. Um Nicht-Inhaltsdaten von elektronischen Kommunikationen wird am häufigsten ersucht"*.

[80] Siehe Artikel 7a.

[81] Siehe Fußnote 32, S. 34, der allgemeine Ausrichtung zum Verordnungsvorschlag: „*Die Tschechische Republik, Finnland, Deutschland, Griechenland, Ungarn und Lettland haben Vorbehalte zum Notifizierungsverfahren und plädieren für ein Verfahren von größerer Tragweite, das auch Transaktionsdaten einschließt, sowie für eine Grundrechteklausel, d. h. für die Nennung von Gründen, wenn eine notifizierte Behörde abgewiesen wird; außerdem sollte die Bestimmung, in der dargelegt wird, was als „nationaler Fall" gilt, rückgängig gemacht werden; und schließlich sollte aus Sicht Deutschlands nicht das Zertifikat, sondern die Anordnung selbst übermittelt werden, während die Tschechische Republik die Ansicht vertritt, dass beide – Anordnung und Zertifikat – übermittelt werden sollten"*.

[82] Das Thema wurde auch von EGMR-Richter Prof. Dr. Bošnjak in persönlicher Funktion bei der Anhörung über elektronische Beweismittel in Strafsachen des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments am 27. November 2018 aufgeworfen (insbesondere 16.55-16.58 ausdrücklich zum Thema – „*Soweit das Recht des vollstreckenden Mitgliedstaats betroffen ist, scheint es gemäß dem bestehenden Vorschlag nicht von Relevanz zu sein. Vom Standpunkt des Übereinkommens kann dies ein Problem erzeugen, weil die Hohen Vertragsparteien des EGMR, darunter alle 28 EU-Mitgliedstaaten, für den Schutz der Menschenrechte in dem seiner Hoheitsgewalt unterstehenden Gebiet verantwortlich sind. Sie müssen einen regulatorischen Rahmen und auch rechtlichen, wenn nicht gerichtlichen, Schutz in Sonderfällen garantieren. […] Wenn die Behörden des Vollstreckungsstaats einer Beschwerde gegenüberstehen, dass der Schutz des Rechts des Übereinkommens offenkundig unzureichend ist und diesem nicht durch Unionsrecht abgeholfen werden kann, können sie nicht auf die Prüfung der Beschwerde aus dem Grund, dass sie nur Unionsrecht anwenden, verzichten. Dies wurde klar im Urteil Avotinš gg. Lettland ausgeführt und später in mehreren Instanzen bestätigt. Der Vorschlag, so wie er Ihnen vorliegt, schafft eine eher einzigartige Situation aus Sicht der EGMR-Rechtsprechung. Die Eingriffe in Bezug auf Artikel 8 sind nämlich ohne Einbeziehung der Behörden des Vollstreckungsstaats. Ich frage mich, ob dies auf den EGMR ausgerichtet ist, weil es ein berechtigtes Vertrauen darauf geben könnte, dass das Recht des Vollstreckungsstaats in jeder einzelnen besonderen Situation gelten würde. Dies würde sich natürlich die Beurteilung der Rechtmäßigkeit auswirken…"*, abrufbar unter http://www.europarl.europa.eu/ep-live/en/committees/video?event=20181127-1430-COMMITTEELIBE.

[83] Mit Ausnahme der Straftaten, die auf Unionsebene definiert und in Artikel 5 Absatz 4 Buchstabe b des Verordnungsvorschlags aufgeführt sind.

[84] Stellungnahme 23/2018 des EDSA, Abschnitt 2, Buchstabe b.

[85] Siehe auch die Präsentation des EGMR-Richters Prof. Dr. Bošnjak in persönlicher Funktion bei der Anhörung über elektronische Beweismittel in Strafsachen des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments am 27. November 2018 (Fußnote 82 *supra*).

[86] Siehe Abschnitt 3.2 dieser Stellungnahme.
[87] Siehe Stellungnahme 2/2019 des EDSB, Rn. 28, und Stellungnahme 3/2019 des EDSB, Rn. 53.
[88] Folgenabschätzung, S. 37.
[89] Erwägungsgrund 36.
[90] Erwägungsgrund 19 des Verordnungsvorschlags: *„Diese Verordnung regelt nur das Erheben gespeicherter Daten, das heißt derjenigen Daten, die ein Diensteanbieter zum Zeitpunkt des Erhalts des Zertifikats über die Europäische Herausgabe- oder Sicherungsanordnung besitzt. Sie enthält weder eine allgemeine Verpflichtung zur Datenspeicherung noch wird mit ihr das Abfangen von Daten oder das Einholen von Daten, die zu einem späteren Zeitpunkt nach Erhalt eines Zertifikats über eine Herausgabe- oder Sicherungsanordnung gespeichert werden, genehmigt.“*
[91] Artikel 5 Absatz 1 Buchstabe e DSGVO und Artikel 4 Absatz 1 Buchstabe e der Richtlinie zum Datenschutz bei der Strafverfolgung.
[92] Dies ist der Fall, wenn Daten gesichert werden, wenn der Diensteanbieter, der ein Zertifikat über eine Europäische Herausgabeanordnung erhalten hat, die Daten nicht sofort herausgibt.
[93] Stellungnahme 23/2018 des EDSA, Abschnitt 7 Buchstabe d, Europäische Sicherungsanordnungen sollten nicht dazu verwendet werden dürfen, die Vorhaltepflichten der Dienstleister zu umgehen.
[94] Siehe Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 10 final, (im Folgenden „vorgeschlagene Verordnung über Privatsphäre und elektronische Kommunikation“).
[95] Artikel 12b Absatz 3.
[96] Beispielsweise Facebook, Google, Microsoft, Twitter und Apple; siehe Folgenabschätzung, S. 14.
[97] Eine ähnliche Bestimmung ist beispielsweise in Artikel 8 des Verordnungsvorschlags des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte (COM/2018/640 final) enthalten.
[98] Artikel 5 legt die Bedingungen für den Erlass einer EPO fest. Dem Wortlaut der Bestimmung mangelt es allerdings an Klarheit: Artikel 5 Absatz 7 sieht vor, dass *„[w]enn die Anordnungsbehörde Grund zu der Annahme hat, dass angeforderte Transaktions- oder Inhaltsdaten durch Immunitäten und Vorrechte geschützt sind, die nach dem Recht des Mitgliedstaats, in dem die Anordnung an den Diensteanbieter gerichtet wird, gewährt werden, muss [sie] vor Erlass der Europäischen Herausgabeanordnung den Sachverhalt klären, unter anderem indem sie die zuständigen Behörden des betreffenden Mitgliedstaats entweder direkt oder über Eurojust oder das Europäische Justizielle Netz konsultiert“*. Darüber hinaus, *„[s]tellt die Anordnungsbehörde fest, dass die angeforderten Zugangs-, Transaktions- oder Inhaltsdaten durch solche Immunitäten und Vorrechte geschützt sind, (...) so erlässt sie die Europäische Herausgabeanordnung nicht“* [Unterstreichung hinzugefügt].
[99] Siehe Artikel 5 Absatz 7 der allgemeinen Ausrichtung des Rates.
[100] Es scheint, dass dieser Grund für einen Einwand auch für die Europäische Sicherungsanordnung zur Verfügung steht.
[101] Siehe Begründung des Verordnungsvorschlags, S. 24: *„Sollte das Vollstreckungsverfahren eingeleitet werden, kann zudem der Adressat selbst die Anordnung vor der Vollstreckungsbehörde ablehnen. Der Adressat kann dies auf Basis derartiger Gründe unter Ausschluss von Immunitäten und Vorrechten (...) tun“*.
[102] Siehe Artikel 7a der allgemeinen Ausrichtung des Rates. Die Bestimmung legt nur eine Möglichkeit (und keine Verpflichtung) für die zuständige Behörde im Vollstreckungsstaat fest, die Anordnungsbehörde zu informieren.
[103] Artikel 18 sieht vor, dass *„das Gericht des Anordnungsstaats bei der Prüfung der Relevanz und der Zulässigkeit der betreffenden Beweismittel während des Strafverfahrens, für das die Anordnung erlassen wurde, sicher(stellt), dass diese Gründe genauso berücksichtigt werden als wären sie im nationalem Recht vorgesehen. Das Gericht kann die Behörden des betreffenden Mitgliedstaats, das Europäische Justizielle Netz für Strafsachen oder Eurojust konsultieren“*.
[104] In der allgemeinen Ausrichtung des Rates wurde dies auf Situationen begrenzt, in denen die betroffene Person ihren Wohnsitz nicht im Anordnungsstaat hat (Artikel 12a).
[105] Die allgemeine Ausrichtung des Rates sieht nur die Zuständigkeit, jedoch nicht die Verpflichtung der Anordnungsbehörde vor, bei den Behörden des Vollstreckungsstaats um die Ausübung ihrer Zuständigkeit, das Vorrecht oder die Immunität aufzuheben, zu ersuchen (Artikel 5 Absatz 8).
[106] Dieser Grund besteht nach Artikel 11 der Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen.
[107] Stellungnahme 23/2018 des EDSA, Abschnitt 5 Buchstabe b, Gesetzlicher Vertreter, S. 12.
[108] Die Begründung des Richtlinienvorschlags hält auf S. 3 fest, dass *„[i]n einigen für bestimmte Bereiche geltenden EU-Rechtsakten [...] bereits vorgeschrieben [ist], dass Diensteanbieter, die in der EU nicht niedergelassen sind, dort aber Dienste anbieten, einen Vertreter benennen müssen. Dies gilt beispielsweise für die Datenschutz-Grundverordnung (EU) 2016/679 (Artikel 27) und für die Richtlinie (EU) 2016/1148 über*

Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (Artikel 18). Der Vorschlag der Kommission für eine Verordnung über Privatsphäre und elektronische Kommunikation enthält ebenfalls eine solche Verpflichtung (Artikel 3)". Die Begründung (S. 5) legt auch nahe, dass die gemäß dem Richtlinienvorschlag benannten Vertreter zusätzlich andere Funktionen ausüben können, darunter auch die von Vertretern gemäß DSGVO und der Verordnung über Privatsphäre und elektronische Kommunikation. Zusätzlich verweist Erwägungsgrund 6 des Richtlinienvorschlags auf die DSGVO und die darin enthaltene Pflicht, unter bestimmten Bedingungen einen Vertreter in der Union zu benennen. Zudem hält die Folgenabschätzung (S. 91) fest, dass der gemäß dem Richtlinienvorschlag benannte Vertreter *„mehrere Funktionen ausüben könnte (z. B. DSGVO, Verordnung über Privatsphäre und elektronische Kommunikation und EPO), wodurch die Kosten [für die Diensteanbieter] gesenkt würden"*.

[109] In diesem Zusammenhang hob die Artikel-29-Datenschutzgruppe in ihrer Erklärung zum Datenschutz und Aspekte der Privatsphäre bei grenzüberschreitendem Zugang zu elektronischen Beweismitteln hervor, dass „*während der Vertreter gemäß der DSGVO die Kontaktstelle der Überwachungsbehörden der für die Verarbeitung Verantwortlichen oder der Auftragsverarbeiter für die Erfüllung ihrer Pflichten werden soll, ist das Ziel des Vertreters gemäß der beabsichtigten Maßnahme die Durchsetzung der von der zuständigen Behörde erteilten Herausgabeanordnung"*.

[110] Gemäß dem Richtlinienvorschlag wird die Pflicht zur Bestellung eines Vertreters allen Diensteanbietern auferlegt, die ihre Dienste in der Union im Sinne des Vorschlags (Artikel 2 Absatz 3 in Verbindung mit Erwägungsgrund 13) anbieten, und das unabhängig davon, ob sie in der Union niedergelassen sind.
Gemäß der DSGVO (Artikel 3 Absatz 2 in Verbindung mit Artikel 27) wird die Pflicht zur Bestellung eines Vertreters den für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern auferlegt, die keine Niederlassung in der Union haben, aber „*personenbezogene Daten von betroffenen Personen, die sich in der Union befinden*" verarbeiten, und die Datenverarbeitung im Zusammenhang damit steht, Waren oder Dienstleistungen anzubieten oder „*das Verhalten betroffener Personen [der vorgenannten betroffenen Personen] zu beobachten, soweit ihr Verhalten in der Union erfolgt*" [Unterstreichung hinzugefügt]. Zudem sieht Artikel 27 Absatz 2 DSGVO eine Ausnahme von dieser Pflicht vor für „*eine Verarbeitung, die gelegentlich erfolgt, nicht die umfangreiche Verarbeitung besonderer Datenkategorien im Sinne des Artikels 9 Absatz 1 oder die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt"* oder für *„Behörden oder öffentliche Stellen*".

[111] Artikel 9 legt Fristen zur Einhaltung eines EPOC fest. Die angeforderten Daten müssen „*spätestens innerhalb von zehn Tagen nach Erhalt des EPOC [...] übermittelt werden, er sei denn, die Anordnungsbehörde gibt Gründe für eine frühere Offenlegung an*". Der Verordnungsvorschlag sieht zudem vor, dass *"[i]n Notfällen [...] der Adressat die angeforderten Daten unverzüglich [übermittelt], spätestens jedoch innerhalb von sechs Stunden nach Erhalt des EPOC"*. Bei EPOC-PR speichert der Adressat die Daten oder wendet sich an die Anordnungsbehörde, wenn das Zertifikat bei Eingang des Zertifikats nicht ohne ungebührliche Verzögerung eingehalten werden kann (Artikel 9 Absatz 2). Notfälle werden in Artikel 2 Absatz 15 als *„Situationen, in denen eine unmittelbare Gefahr für das Leben oder die körperliche Unversehrtheit einer Person oder für eine kritische Infrastruktur im Sinne des Artikels 2 Buchstabe a der Richtlinie 2008/114/EG des Rates besteht"* definiert.

[112] Artikel 12 Absatz 3 EEA-Richtlinie.

[113] Artikel 12 Absatz 4 der EEA-Richtlinie.

[114] Artikel 13 des Verordnungsvorschlags legt den Mitgliedstaaten auf, für Fälle von Nichtbefolgung einer Anordnung finanzielle Sanktionen in ihrer nationalen Gesetzgebung vorzusehen, die *„wirksam, verhältnismäßig und abschreckend"* sind. Bei einem Verstoß gegen eine Anordnung sieht Artikel 14 Absatz 3 vor, dass die Vollstreckungsbehörde den Adressaten von der Möglichkeit, die in Artikel 14 Absätze 4 und 5 aufgeführten Einsprüche zu erheben, in Kenntnis setzt und auch an die bei Nichtbefolgung anwendbaren Sanktionen erinnert.

[115] Diese Sanktionen sollten in jedem Fall nicht Adressaten auferlegt werden, die gegen eine Anordnung Einspruch einlegen, weil sie in gutem Glauben davon überzeugt sind, dass sie gegen die EU-Charta verstößt.

[116] Er umfasst „jede Dienstleistung, die deren Nutzern die Fähigkeit gibt, drahtgebundene oder elektronische Kommunikationen zu senden oder zu erhalten" (18 U.S.Code § 2510(15)).

[117] Siehe neuer Unterabsatz (i), der durch den US CLOUD Act in Kapitel 119 „Wire and electronic communications interception and interception of oral communications" in Titel 18 des USC eingefügt wurde.

[118] Artikel 15 und 16 des Verordnungsvorschlags. Begründung des Verordnungsvorschlags, S. 24*: „Die Festlegung eines hohen Niveaus hat den Zweck, Drittstaaten zu motivieren, für einen ähnlich hohen Schutz zu sorgen. Im umgekehrten Fall, in dem Behörden aus Drittstaaten bei einem EU-Diensteanbieter Daten eines EU-Bürgers anfordern, können die Rechtsvorschriften der Union oder der Mitgliedstaaten zum Schutz der Grundrechte wie etwa der Besitzstand im Bereich des Datenschutzes gleichfalls die Offenlegung verhindern. Die*

Europäische Union erwartet von Drittländern, ihrerseits derartige Verbote zu respektieren, wie in diesem Vorschlag geschehen".

[119] Dokumente 9114/19 und 9116/19 des Rates, abrufbar unter https://www.consilium.europa.eu/de/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

[120] Ergänzung zur Entscheidung, Absatz I. 1, Ratsdokument 9666/19.

[121] Ergänzung zur Entscheidung, Absatz II.1. Buchstabe a, Ratsdokument 9664/19.

[122] Diese Bestimmung hält fest, dass „diese Verordnung die EU und andere internationale Übereinkünfte, Abkommen und Vereinbarungen über das Erheben von Beweismitteln, die auch in den Anwendungsbereich der Verordnung fallen würden, nicht berührt".