Stellungnahme 23/2018 zu den Vorschlägen der Kommission über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (Artikel 70 Absatz 1 Buchstabe b)

angenommen am 26. September 2018

Inhalt

Der Europäische Datenschutzausschuss

gestützt auf Artikel 70 Absatz 1 Buchstaben b der Verordnung 2016/679/EU 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,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

Einführung

Im April 2018 legte die Kommission einen Vorschlag für eine Verordnung über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und einen Vorschlag für eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren vor. Die beiden Vorschläge (COM(2018) 225 final und COM(2018) 226 final) ergänzen sich. Das von der Kommission verfolgte übergeordnete Ziel besteht darin, die Zusammenarbeit zwischen den Behörden der Mitgliedstaaten und den Dienstleistern, auch aus Drittländern, zu verbessern und Lösungen für das Problem der Ermittlung und Vollstreckung der Zuständigkeiten im Cyberspace vorzuschlagen.

Während der Verordnungsentwurf die Regeln und Verfahren für die Erlass, Zustellung und Vollstreckung von Herausgabe- und Sicherungsanordnungen an Anbieter von elektronischen Kommunikationsdiensten vorsieht, sieht der Richtlinienentwurf Mindestvorschriften für die Ernennung eines gesetzlichen Vertreters für Dienstleister vor, die nicht in der EU niedergelassen sind.

Im November 2017[1], bevor die Kommission den Entwurf eines Vorschlags vorlegte, erinnerte die Artikel-29-Datenschutzgruppe (Article 29 Working Party, im Folgenden „WP29“) daran, dass gewährleistet sein müsse, dass jeder Legislativvorschlag vollständig mit dem bestehenden Besitzstand der Union im Bereich des Datenschutzes im Besonderen sowie mit EU-Recht und Rechtsprechung im Allgemeinen übereinstimmt.

Insbesondere warnte die WP29 vor Beschränkungen des Rechts auf Datenschutz und Privatsphäre in Bezug auf Daten, die von Telekommunikations- und Informationsdienstleistern verarbeitet werden, insbesondere wenn sie von Strafverfolgungsbehörden weiterverarbeitet werden. Die WP29 erinnerte daran, dass die Kohärenz jedes EU-Instruments mit dem bestehenden Budapester Übereinkommen des Europarats über Computerkriminalität und mit der EU-Richtlinie über die Europäische Ermittlungsanordnung (EEA) gewährleistet sein müsse und empfahl, die jeweiligen Verfahrensvorschriften für den Zugang zu elektronischen Beweismitteln auf nationaler und auf europäischer Ebene zu präzisieren, um sicherzustellen, dass das neue Instrument den Behörden keine neuen Befugnisse gewährt, über die sie intern nicht verfügen würden. Zusätzlich zu diesen allgemeinen Bemerkungen bezog die WP29 Stellung zu den von der Kommission damals in Betracht gezogenen legislativen Optionen in Bezug auf die betreffenden Datenkategorien und die entsprechenden Schutzmechanismen für den Zugang zu ihnen, zu der Möglichkeit, Herausgabeanordnungen zu erteilen bzw. Dienstleistern Pflichten zur Datenübermittlung von außerhalb der EU belegenen Daten

[1] Siehe WP29-Stellungnahme (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801).

aufzuerlegen, sowie zu den materiellen und den verfahrensrechtlichen Bedingungen, die für den direkten Zugang zu Daten erforderlich sind.

Anhand der nun vorliegenden konkreten Vorschläge zum Thema elektronische Beweismittel möchte der Europäische Datenschutzausschuss (EDSA) eine detailliertere Analyse der vorgeschlagenen Rechtsakte aus datenschutzrechtlicher Sicht vornehmen.

1. Rechtsgrundlage des Verordnungsvorschlags (Artikel 82 AEUV)

Die für den Entwurf einer Verordnung über elektronische Beweismittel vorgeschlagene Rechtsgrundlage ist Artikel 82 Absatz 1 AEUV über die justizielle Zusammenarbeit in Strafsachen, der Folgendes vorsieht:

> „*(1) Die justizielle Zusammenarbeit in Strafsachen in der Union beruht auf dem Grundsatz der gegenseitigen Anerkennung gerichtlicher Urteile und Entscheidungen und umfasst die Angleichung der Rechtsvorschriften der Mitgliedstaaten in den in Absatz 2 und in Artikel 83 genannten Bereichen.*
>
> *Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Maßnahmen, um*
>
> *a) Regeln und Verfahren festzulegen, mit denen die Anerkennung aller Arten von Urteilen und gerichtlichen Entscheidungen in der gesamten Union sichergestellt wird;*
>
> *b) Kompetenzkonflikte zwischen den Mitgliedstaaten zu verhindern und beizulegen;*
>
> *c) die Weiterbildung von Richtern und Staatsanwälten sowie Justizbediensteten zu fördern;*
>
> *d) die Zusammenarbeit zwischen den Justizbehörden oder entsprechenden Behörden der Mitgliedstaaten im Rahmen der Strafverfolgung sowie des Vollzugs und der Vollstreckung von Entscheidungen zu erleichtern.*"

Wie die Kommission in der den Vorschlägen beigefügten Folgenabschätzung betonte, „legt Artikel 82 Absatz 1 fest, dass die justizielle Zusammenarbeit in Strafsachen auf dem Grundsatz der gegenseitigen Anerkennung beruht. Diese Rechtsgrundlage würde mögliche Rechtsvorschriften über die direkte Zusammenarbeit mit Dienstleistern umfassen, nach denen die Behörde des anordnenden Mitgliedstaats ein Unternehmen (den Dienstleister) im Vollstreckungsstaat direkt ansprechen und ihm sogar Verpflichtungen auferlegen könnte. Damit würde eine neue Dimension der gegenseitigen Anerkennung über die traditionelle justizielle Zusammenarbeit in der Union hinaus eingeführt, die bisher auf Verfahren beruht, an denen zwei Justizbehörden beteiligt sind, eine im Anordnungsstaat und eine weitere im Vollstreckungsstaat." (hervorgehoben)

Angesichts der Neuartigkeit der Anwendung dieser Rechtsgrundlage im Zusammenhang mit direkten Ersuchen zwischen Behörden und privaten Parteien bedauert der EDSA, dass die Kommission keine weitere Analyse oder Bewertung durchgeführt hat.

Wie die Arbeitsgruppe bereits in ihrer früheren Stellungnahme betont hat, hegt der EDSA weiterhin Zweifel an der Angemessenheit dieser Rechtsgrundlage, welche durch die in der Stellungnahme 1/15 der WP29 aufgegriffene Analyse des EuGH und des Schlussantrags seines Generalanwalts gestützt werden. Im Rahmen der Entwicklungen im Zusammenhang mit der Gültigkeit von Artikel 82 als Rechtsgrundlage für den Entwurf eines PNR-Abkommens zwischen der EU und Kanada betonte der Gerichtshof, dass die zuständige kanadische Behörde „*weder eine Justizbehörde, noch eine gleichwertige Behörde darstellt*"[2]. Im Zusammenhang mit den Vorschlägen zu elektronischen

[2] Siehe Ziffer 103 der Stellungnahme 1/15 der WP29 sowie Rn. 108 des Schlussantrags des Generalanwalts.

Beweismitteln besteht eines der von der Kommission genannten Hauptziele offensichtlich darin, die „zu schwerfällige“ justizielle Zusammenarbeit zu umgehen. Folglich basiert der Vorschlag auf dem Grundsatz, dass die Zusammenarbeit eher zwischen einer Behörde und einem Dienstleister als zwischen zwei Behörden stattfinden sollte. Das vorgesehene Verfahren verleiht in erster Linie privaten Unternehmen die Möglichkeit, die empfangende Partei zu sein und die von den Justizbehörden gestellten Ersuchen zu beantworten.

Der EDSA nimmt zur Kenntnis, dass der Prozess der Vollstreckung von Herausgabe- oder Sicherungsanordnungen die Beteiligung einer empfangenden Behörde bedeuten könnte, wenn der empfangende Dienstleister seinen Verpflichtungen nicht nachkommt, und somit die nachträgliche Vollstreckung der Anordnung erforderlich würde. Da das Hauptziel des eingeleiteten Verfahrens jedoch gerade darin besteht, keine empfangende Behörde einzubeziehen, bezweifelt der EDSA, dass dieses ergänzende Verfahren die Anwendung von Artikel 82 als einzige Rechtsgrundlage für das Instrument rechtfertigen könnte.

Daher ist der EDSA der Ansicht, dass für die Anwendung von Artikel 82 als Rechtsgrundlage die wichtigsten Verfahrensschritte der Zusammenarbeit zwischen zwei Justizbehörden stattfinden müssen und dass für diese Art der Zusammenarbeit eine andere Rechtsgrundlage herangezogen werden sollte.

2. Die Notwendigkeit elektronischer Beweismittel im Vergleich zum MLAT und zur EEA

Der EDSA merkt an, dass die Kommission sich verpflichtet hat, die Hindernisse für strafrechtliche Ermittlungen zu überprüfen, insbesondere in Bezug auf die Frage des Zugangs zu elektronischen Beweismitteln. In ihrer Begründung erläutert die Kommission den Hintergrund des Vorschlags und betont die Volatilität elektronischer Beweismittel, ihre internationale Dimension sowie die Notwendigkeit, die Kooperationsverfahren an das digitale Zeitalter anzupassen. Die Vorschläge für eine Verordnung und eine Richtlinie für die Übermittlung und den Zugang zu elektronischen Beweismitteln zielen nicht darauf ab, frühere Kooperationsinstrumente in Strafsachen wie das Budapester Übereinkommen, das Rechtshilfeabkommen (MLAT) und die Europäische Ermittlungsanordnung (EEA-Richtlinie) zu ersetzen. Der Kommission zufolge zielen die Vorschläge für elektronische Beweismittel auf eine Verbesserung der justiziellen Zusammenarbeit in Strafsachen zwischen Behörden und Dienstleistern innerhalb der Europäischen Union sowie mit Drittländern, insbesondere den Vereinigten Staaten von Amerika, ab.

Da diese neuen zusätzlichen Instrumente speziell für den Zugang zu und die Übermittlung von elektronischen Beweismitteln bestimmt sind, wird der EDSA den Mehrwert der Instrumente im Zusammenhang mit der EEA-Richtlinie und dem MLAT bewerten.

a) Die Notwendigkeit von elektronischen Beweismitteln im Vergleich zu den Garantien im Rahmen der EEA und des MLAT

Das Hauptargument der Kommission für die Vorschläge im Bereich der elektronischen Beweismittel besteht darin, das Verfahren zur Sicherung und Beschaffung elektronischer Beweismittel zu beschleunigen, die bei Dienstleistern mit Sitz in einem anderen Land gespeichert werden oder sich in ihrem Besitz befinden.

Der EDSA bedauert jedoch, dass die Notwendigkeit eines neuen Instruments zur Organisation des Zugangs zu elektronischen Beweismitteln in der Folgenabschätzung nicht nachgewiesen wurde. Den Vorschlägen fehlt in der Tat der Nachweis, dass keine anderen weniger eingreifenden Mittel hätten eingesetzt werden können, um das Ziel des Vorschlags für elektronische Beweismittel zu erreichen, obgleich alternative Lösungen hätten erwogen werden können. So hätte beispielsweise die Möglichkeit einer Änderung und Verbesserung der EEA-Richtlinie geprüft werden können, womit auch der spezifischen Anforderung der EEA-Richtlinie entsprochen worden wäre, die Notwendigkeit einer Änderung des Textes bis zum 21. Mai 2019[3] zu bewerten. Eine weitere Möglichkeit hätte darin bestehen können, die Verwendung von Sicherungsanordnungen zum Sperren der Daten vorzusehen, solange eine formelle Anfrage auf der Grundlage eines MLAT gestellt wurde. Diese Maßnahmen hätten es ermöglicht, die in diesen Instrumenten vorgesehenen Garantien beizubehalten und gleichzeitig sicherzustellen, dass die angeforderten personenbezogenen Daten nicht gelöscht werden.

Der EDSA weist darauf hin, dass die in der EEA-Richtlinie festgelegten Fristen länger sind als die im Vorschlag für elektronische Beweismittel. Tatsächlich hat die Vollstreckungsbehörde 30 Tage Zeit, um ihre Entscheidung über die Anerkennung des Antrags zu treffen[4] und sollte den Beschluss dann innerhalb von 90 Tagen vollstrecken[5]. Der EDSA ist der Ansicht, dass die Gewährung einer 30-tägigen Reflexion für die Vollstreckungsbehörden in der EEA ein entscheidender Schutz ist, der es ihnen ermöglicht zu beurteilen, ob der Vollstreckungsantrag begründet ist und alle Bedingungen für die Erteilung und Übermittlung einer EEA erfüllt[6].

Der EDSA ist besorgt darüber, dass die in den Vorschlägen für elektronische Beweismittel vorgesehene 10-tägige Frist für die Ausführung des Zertifikats über eine Europäische Herausgabeanordnung (European Produktion Order Certificate; im Folgenden „EPOC“) ohne Zeit zur Reflexion die ordnungsgemäße Beurteilung der Frage erschwert, ob das EPOC alle Kriterien erfüllt und korrekt vervollständigt wurde.

Daher empfiehlt der EDSA, dem EPOC-Empfänger mehr Zeit einzuräumen, um festzustellen, ob die Anordnung ausgeführt werden soll oder nicht.

Der EDSA stellt fest, dass im Falle einer Europäischen Sicherungsanordnung (EPOC-PR) nicht garantiert ist, dass die Speicherung der Daten auf das für die Datenverarbeitung erforderliche Maß beschränkt ist. Die Speicherdauer der Daten kann in der Tat 60 Tage überschreiten, da es für die Anordnungsbehörde keine Frist gibt, um den Adressaten zu informieren, von der Erteilung abzusehen oder eine Herausgabeanordnung zu widerrufen. Daher empfiehlt der EDSA der Anordnungsbehörde zumindest eine Frist zu setzen, um die Herausgabeanordnung zurückzuhalten oder zu widerrufen, um dem in der DSGVO festgelegten Grundsatz der Datenminimierung zu entsprechen[7].

Schließlich weist der EDSA darauf hin, dass die EEA-Richtlinie die Rückgabe von Beweismitteln vom Anordnungsstaat an die Vollstreckungsbehörde vorsieht[8]. Der Vorschlag zu elektronischen Beweismitteln schweigt jedoch über eine solche Möglichkeit. Was mit den elektronischen Beweismitteln nach ihrer Übermittlung an die Anordnungsbehörde geschieht, ist unklar.

Daher empfiehlt der EDSA, dass der Verordnungsvorschlag mehr Informationen über die Verwendung elektronischer Beweismittel nach ihrer Übermittlung an die Anordnungsbehörde enthalten sollte, um

[3] Siehe Artikel 37 der EEA-Richtlinie.
[4] Artikel 12 Absatz 3 der EEA-Richtlinie.
[5] Artikel 12 Absatz 4 der EEA-Richtlinie.
[6] Artikel 6 der EEA-Richtlinie.
[7] Artikel 5 Absatz 1 Buchstabe c der DSGVO.
[8] Artikel 13 Absätze 3 und 4 der EEA-Richtlinie.

der DSGVO und dem Grundsatz der Transparenz[9] sowie dem von den MLAT festgelegten Grundsatz der Spezifität zu entsprechen.

b) Die Aufgabe des Grundsatzes der doppelten Strafbarkeit

Der EDSA erkennt an, dass die gegenseitige Anerkennung von der Anwendung der beidseitigen Strafbarkeit abhängt, die für die Mitgliedstaaten ein Weg ist, ihre Souveränität zu wahren. Die beidseitige Strafbarkeit wird jedoch zunehmend als Hindernis für eine reibungslose justizielle Zusammenarbeit angesehen. Die EU-Mitgliedstaaten zeigen sich immer kooperationsbereiter, selbst wenn sich die Ermittlungsmaßnahmen auf Handlungen beziehen, die in ihrem nationalen Recht nicht als Straftat gelten. Der EDSA erinnert jedoch daran, dass das Prinzip der beidseitigen Strafbarkeit darauf abzielt, einen zusätzlichen Schutz zu bieten, um zu gewährleisten, dass sich ein Staat bei der Anwendung einer strafrechtlichen Sanktion, die im Recht eines anderen Staates nicht existiert, nicht auf die Hilfe eines anderen verlassen kann. Dies würde beispielsweise einen Staat daran hindern, die Hilfe eines anderen Staates zu ersuchen, um jemanden für seine politischen Meinungen zu inhaftieren, wenn diese Meinungen im ersuchten Staat nicht kriminalisiert werden, oder jemanden wegen Schwangerschaftsabbruch zu verfolgen, wenn diese Person in einem anderen Staat wohnt, in dem dies nicht illegal ist. Der Grundsatz der beidseitigen Strafbarkeit geht oft auch mit zusätzlichen Einschränkungen oder Garantien in Bezug auf die Sanktionen einher, wenn diese sich zwischen dem ersuchenden und dem vollstreckenden Staat zu stark unterscheiden. Das bedeutendste Beispiel ist die Verpflichtung, die Todesstrafe in bestimmten MLAT nicht anzuwenden, wenn sie nach dem Recht einer der beiden Parteien nicht existiert.

Der EDSA merkt an, dass das Prinzip der beidseitigen Strafbarkeit im Vorschlag für die Verordnung über elektronische Beweismittel ausgeschlossen ist. Dies führt jedoch nicht nur zur Aufhebung der üblichen Formalitäten der gegenseitigen Anerkennung, sondern auch zur Aufhebung der Garantien im Zusammenhang mit dem Grundsatz der beidseitigen Strafbarkeit selbst.

Der EDSA weist ferner darauf hin, dass kein Verweis auf die Rechtsordnung des Landes erfolgt, in dem der ersuchte Dienstleister niedergelassen ist, und dass die Speicherung von Daten sowie die Erhebung von Nutzer- oder Zugangsdaten für alle Straftaten ausgestellt werden können[10], unabhängig davon, ob es ähnliche Straftaten in anderen Mitgliedstaaten gibt oder nicht.

Derweil dürfen Herausgabeanordnungen nur erteilt und ausgeführt werden, wenn eine ähnliche Maßnahme für die gleiche Straftat in einer vergleichbaren innerstaatlichen Situation im Anordnungsstaat vorliegt[11]. Darüber hinaus wird, wie von der Kommission in der Begründung des Verordnungsvorschlags erläutert, die Besonderheit von Transaktionsdaten und Inhaltsdaten festgestellt, da sie als sensibler angesehen werden. Tatsächlich können Anordnungen über Transaktions- oder Inhaltsdaten nur für Straftaten mit einer Androhung von einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren ersucht werden, um die Einhaltung der Verhältnismäßigkeit und der Rechte der betroffenen Personen zu gewährleisten[12]. Der EDSA betont jedoch, dass es noch keine Harmonisierung innerhalb der EU in Bezug auf Straftaten gegeben habe, die mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden.

Der EDSA lehnt die Aufhebung des Grundsatzes der doppelten Strafbarkeit ab, der darauf abzielt, sicherzustellen, dass ein Staat sich nicht auf die Hilfe anderer verlassen kann, damit sein nationales

[9] Artikel 5 Absatz 1 Buchstabe a der DSGVO.
[10] Artikel 5 Absatz 3 und Artikel 6 Absatz 2 der vorgeschlagenen Verordnung über elektronische Beweismittel.
[11] Artikel 5 Absatz 2 der vorgeschlagenen Verordnung über elektronische Beweismittel.
[12] Artikel 5 Absatz 4 Buchstabe a der vorgeschlagenen Verordnung über elektronische Beweismittel.

Strafrecht außerhalb des Staatsgebiets eines Staates angewendet wird, der nicht den gleichen Ansatz verfolgt, insbesondere angesichts des Wegfalls anderer traditioneller wichtiger Garantien im Bereich des Strafrechts (siehe unten Nummer 3 in Bezug auf die Standortkriterien und Nummer 7 Buchstabe g bezüglich möglicher Konflikte mit den Gesetzen von Drittländern).

c) Die Folgen der direkten Ansprache von Unternehmen

Der EDSA ist sich darüber im Klaren, dass elektronische Beweismittel zunehmend in der privaten Infrastruktur verfügbar sind und sich außerhalb des Ermittlungslandes im Besitz von Dienstleistern befinden können.

Der EDSA weist darauf hin, dass gemäß den Entscheidungen bezüglich *Yahoo*[13]! und *Skype*[14] in Belgien und im Rahmen von Terroranschlägen eine reibungslosere und schnellere Zusammenarbeit zwischen öffentlichen und privaten Stellen erforderlich ist. In der Folgenabschätzung verweist die Kommission auf drei Arten von Verfahrensinstrumenten, die sowohl Behörden als auch Dienstleister betreffen. Dies sind die justizielle Zusammenarbeit, die direkte Zusammenarbeit und der direkte Zugriff. Wenn das erste Instrument nicht dem Dienstleister die Verantwortung für die Vollstreckung der EEA überträgt, sondern der ausführenden Behörde[15], dann basiert das zweite Instrument, die direkte Zusammenarbeit, auf der Kooperation des Dienstleisters. Aus Sicht des Dienstleisters ist der direkte Zugriff am gravierendsten, da die Behörden ohne Hilfe eines Zwischenstelle auf Daten zugreifen können.

Daher befürchtet der EDSA, dass die Dienstleister bei direkter Ansprache den Schutz personenbezogener Daten nicht so wirksam gewährleisten werden, wie es die Behörden können und müssen, und betont, dass dies auch dazu führt, dass bestimmte Verfahrensgarantien, die im Rahmen der justiziellen Zusammenarbeit für Einzelpersonen und auch für Unternehmen selbst vorgesehen sind, nicht anwendbar sind[16]. So müsste beispielsweise ein ersuchter Dienstleister vor das Gericht eines anderen (Mitglieds-)Staates ziehen, um die Anordnung anzufechten, während er im Rahmen der justiziellen Zusammenarbeit vor seinen eigenen Behörden auftreten würde. Der EDSA empfiehlt die Aufnahme zusätzlicher Voraussetzungen in den Verordnungsvorschlag, die gewährleisten, dass Dienstleister die individuellen Grundrechte wie den Schutz personenbezogener Daten und die Achtung des Privat- und Familienlebens schützen werden und dass die zuständigen Datenschutzbehörden benachrichtigt werden, um eine Kontrolle zu ermöglichen.

[13] Belgischer Kassationshof, YAHOO! Inc., Nr. P.13.2082.N vom 1. Dezember 2015.
[14] Strafvollzugsgericht Antwerpen, Abteilung Mechelen, Belgien, Nr. ME20.F1.105151-12 vom 27. Oktober 2016 (Skype hat gegen die Entscheidung Berufung eingelegt).
[15] Artikel 10 bis 16.
[16] Aus internationaler Datenschutzsicht siehe in diesem Zusammenhang auch das „Working Paper on Standards for Data Protection and Personal Privacy in cross-border data requests for criminal law enforcement purposes“, Internationale Arbeitsgruppe „Datenschutz in der Telekommunikation“, 63. Treffen, 9. und 10. April 2018, Budapest (Ungarn).

3. Der neue Zuständigkeitsgrund und der so genannte Wegfall der Standortes der Daten als Kriterium

Der EDSA stellt fest, dass die Kommission hervorhebt, dass eine der wichtigsten Änderungen, die durch diese Vorschläge bewirkt werden, darin besteht, dass der Standort der Daten als Kriterium wegfällt und die zuständigen Behörden die Möglichkeit haben, die Speicherung und Erhebung von Daten zu verlangen, unabhängig davon, wo diese Daten tatsächlich gespeichert sind.

Aus datenschutzrechtlicher Sicht ist es nicht neu, dass das EU-Datenschutzrecht unabhängig davon gilt, wo die Daten der betroffenen Personen gespeichert sind. Die Anwendbarkeit der DSGVO hängt nämlich entweder davon ab, dass der Verantwortliche oder Auftragsverarbeiter innerhalb der EU niedergelassen ist, oder davon, ob die Daten von betroffenen Personen aus der EU verarbeitet werden, auch wenn der Verantwortliche oder Auftragsverarbeiter nicht auf dem Gebiet der EU niedergelassen ist[17]; in diesem Fall müssen sie auch einen gesetzlichen Vertreter in der EU benennen[18]. Aus datenschutzrechtlicher Sicht ist es wichtig, darauf hinzuweisen, dass der erweiterte territoriale Geltungsbereich darauf abzielt, den betroffenen Personen in der EU einen umfassenderen Schutz zu bieten, unabhängig davon, wo das Unternehmen, das ihre Daten verarbeitet, seinen Sitz hat.

Obwohl es im Bereich des Strafrechts neu ist, wenn der Standort der Daten als Kriterium wegfällt, scheint dies aus datenschutzrechtlicher Sicht keine wesentliche Veränderung. Darüber hinaus stellt der EDSA fest, dass nach wie vor eine Verbindung zum Hoheitsgebiet der EU besteht, da nur Dienstleister, die Dienstleistungen in der Union anbieten, in den Anwendungsbereich der Vorschläge fallen, und auch die Tatsache, dass Anträge nur im Rahmen von strafrechtlichen Ermittlungen bearbeitet werden können, bedeutet eine Verbindung zur EU (entweder weil die Straftat auf dem Hoheitsgebiet eines Mitgliedstaats begangen wurde oder weil das Opfer oder der Straftäter Bürger eines Mitgliedstaats war).

Wenn das Wegfallen des Standorts als Kriterium nunmehr im Strafrecht Anwendung finden soll, stellt sich für den EDSA vor allem die Frage, wie sichergestellt werden kann, dass eine solche Entwicklung dem Datenschutz und den Strafprozessrechten der betroffenen Personen und der ersuchten Dienstleister nicht abträglich ist. In diesem Zusammenhang erkennt der EDSA an, dass die Verfahrensgarantien innerhalb der EU zumindest teilweise harmonisiert wurden und in Übereinstimmung mit der Europäischen Menschenrechtskonvention gewährt werden müssen. Es kann daher davon ausgegangen werden, dass das Wegfallen des Standorts als Kriterium wahrscheinlich geringere Folgen nach sich zieht, wenn die Beweise innerhalb der EU angefordert werden, als in der umgekehrten Situation, in der Behörden aus Drittländern Daten von Unternehmen mit Sitz in der EU unter den Bedingungen anfordern, die im Entwurf der Verordnung über elektronische Beweismittel festgelegt sind. Der EDSA ist in der Tat besonders besorgt, dass dies zu problematischen Situationen führen könnte. So könnten Behörden aus einem Drittland, in dem im Bereich des Strafrechts andere und möglicherweise geringere Verfahrensgarantien gelten, Zugang zu Daten haben, die in der EU durch zusätzliche Garantien geschützt wären. Unter diesem Gesichtspunkt erinnert der EDSA an seine Bedenken hinsichtlich ungleicher Standards und einer Schwächung der Grundrechte, wenn Dienstleister und Betroffene nicht von den Verfahrensgarantien des EU-Rechts profitieren, wenn der Antrag von einer Drittlandsbehörde gestellt wird.

[17] Siehe Artikel 3, insbesondere Absatz 2.
[18] Siehe Artikel 27.

Da dieser neue Zuständigkeitsgrund „unabhängig vom Standort der Daten“ mit einem Verfahren verbunden ist, das sich hauptsächlich auf direkte Anfragen der zuständigen Behörden an Dienstleister stützt, ist der EDSA besorgt, dass Privatunternehmen im Falle von Anfragen auf Datenschutzgarantien verzichten könnten, da sie nicht an ein Rechtsinstrument wie ein MLAT gebunden sind, das traditionell den Datenaustausch zwischen Justizbehörden regelt und Schutzmaßnahmen vorsieht. Insbesondere im Zusammenhang mit MLAT beinhalten Mindestdatenschutzgarantien beispielsweise eine Geheimhaltungspflicht und den Grundsatz der Spezifizität, der besagt, dass Daten nicht für einen anderen Zweck verarbeitet werden dürfen.

Der EDSA erinnert daher daran, dass zumindest die in der Richtlinie 2016/680 vorgesehenen Garantien anwendbar gemacht werden sollten, auch in Bezug auf die Datenübermittlung, und insbesondere Artikel 39, falls der Dienstleister ohne eine Angemessenheitsentscheidung in diesem Bereich in einem Drittland niedergelassen sein sollte. Der EDSA hebt insbesondere hervor, dass diese Bestimmung besonders die Information der zuständigen Datenschutzbehörde des Mitgliedstaats der anordnenden Behörde(n) über die Anordnung(en) und die Dokumentation der Übermittlung vorsieht, auch im Hinblick auf die Begründung der Unzweckmäßigkeit oder Unangemessenheit einer Übermittlung an die zuständige Behörde des Drittlandes.

4. Der Begriff „Dienstleister“ sollte durch zusätzliche Garantien für die Rechte der betroffenen Personen eingegrenzt oder ergänzt werden.

Was die Dienstleister anbelangt, so begrüßt der EDSA die weit gefasste Definition, die es ermöglicht, sowohl Kommunikationsdienste als auch Over-the-top-Dienste (OTT) einzubeziehen, da alle diese Dienste funktional gleichwertig sind und daher die vorgesehenen Maßnahmen ähnliche Auswirkungen auf das Recht auf Privatsphäre und das Recht auf Geheimhaltung der Kommunikation haben könnten, wie in der Erklärung der WP29 und zuvor in deren Stellungnahme 01/2017 zur vorgeschlagenen Datenschutzrichtlinie für elektronische Kommunikation (e-Privacy) hervorgehoben. Der Vorschlag für eine Verordnung über elektronische Beweismittel umfasst Dienstleister, die entweder elektronische Kommunikationsdienste im Sinne von Artikel 2 Absatz 4 der Richtlinie über den europäischen Kodex für die elektronische Kommunikation, Dienste der Informationsgesellschaft im Sinne von Artikel 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535, „für die die Speicherung von Daten ein wesentlicher Bestandteil des dem Nutzer angebotenen Dienstes ist, einschließlich sozialer Netzwerke und Online-Märkte, die Transaktionen zwischen ihren Nutzern und anderen Anbietern von Hostdiensten erleichtern“, oder Internet-Domain-Namen und IP-Adressendienste „wie IP-Anbieter von Domain-Namen-Registern, Domain-Namen-Registrierungsstellen und zugehörige Datenschutz- und Proxy-Dienste“ anbieten[19].

Da als Dienstleister im Sinne des Verordnungsentwurfs jedoch „jede natürliche oder juristische Person, die eine oder mehrere der folgenden Kategorien von Dienstleistungen erbringt“ gilt, ist der EDSA besorgt, dass dieses Instrument sowohl für Verantwortliche als auch für Auftragsverarbeiter im Sinne der DSGVO gelten könnte. Da das „Anbieten von Dienstleistungen“ im Sinne von Artikel 2 Absatz 4 des Verordnungsentwurfs sowohl das Angebot der aufgeführten Dienstleistungen für juristische oder natürliche Personen in einem oder mehreren Mitgliedstaaten als auch eine wesentliche Verbindung

[19] Artikel 2 Absatz 3 Buchstabe c der vorgeschlagenen Verordnung über elektronische Beweismittel.

zu dem/den betreffenden Mitgliedstaat(en) beinhaltet, umfassen diese Tätigkeiten Aktivitäten, die von einem Auftragsverarbeiter für einen Verantwortlichen ausgeübt werden, wie z. B. die Speicherung von Daten.

Der EDSA befürchtet daher, dass die Rechte der betroffenen Personen ohne Einschränkungen für Dienstleister, die als Verantwortliche im Sinne der DSGVO tätig sind, und ohne besondere Verpflichtung für den Auftragsverarbeiter, den Verantwortlichen zu benachrichtigen, wenn eine Herausgabe- oder Sicherungsanordnung an ihn gerichtet wird, umgangen werden könnten. Dies gilt umso mehr, als die Justizbehörden im Falle möglicher widerstreitender Verpflichtungen, die den Adressaten daran hindern, den erhaltenen Anordnungen nachzukommen, im Verordnungsentwurf selbst aufgefordert werden, sich unabhängig von den geltenden Datenschutzbestimmungen an den jeweils geeignetsten Akteur zu wenden, insbesondere da jegliche Daten angefordert werden könnten und nicht nur personenbezogene Daten, die unter die DSGVO fallen[20].

Gemäß DSGVO handelt ein Auftragsverarbeiter nur nach den Anweisungen des Verantwortlichen. Daher liegt es in der Zuständigkeit des Verantwortlichen, für die Wahrung der Rechte der betroffenen Personen zu sorgen und ihnen die relevanten Informationen zur Verfügung zu stellen, auch in Bezug auf die Empfänger ihrer Daten, beispielsweise im Rahmen ihres Anspruchs auf Auskunft. Die Auftragsverarbeiter erhalten diese Anfragen nicht direkt von den betroffenen Personen und können diese nur dann beantworten, wenn der Verantwortliche dies ausdrücklich verlangt.

Sofern ihre Rechte in Anwendung der DSGVO nicht eingeschränkt wurden, betont der EDSA daher, dass betroffene Personen, die unter die Anwendung der DSGVO fallen, ihre Rechte möglicherweise nicht effizient ausüben können, wenn der Verantwortliche nicht in der Lage ist, vollständige Informationen zur Verfügung zu stellen. Der EDSA weist ferner darauf hin, dass die Wahrscheinlichkeit, dass keine Informationen vorliegen, noch höher ist, wenn der Auftragsverarbeiter nicht ausdrücklich verpflichtet ist, den Verantwortlichen zu informieren, wenn die angeforderten Daten sich auf Betroffene beziehen, die nicht unter den durch die DSGVO gewährten Schutz fallen. Die anfordernden Justizbehörden sind nämlich nicht unbedingt verpflichtet, die betroffenen Personen in diesem Fall über ihre eigene Weiterverarbeitung zu informieren. Der EDSA fordert daher die Beschränkung des Anwendungsbereichs auf die Verantwortlichen im Sinne der DSGVO oder die Einführung einer Bestimmung, die präzisiert, dass der Dienstleister, wenn er nicht der Datenverantwortliche ist, den Verantwortlichen informiert.

5. Die Begriffe „Niederlassung“ und „gesetzlicher Vertreter“ in diesen Vorschlägen sollten eindeutig von den Begriffen in der DSGVO abgegrenzt werden.

Da dem Standort der Daten keine Bedeutung zukommt, beschränken sich die Adressaten von Herausgabe- und Sicherungsanordnungen im Rahmen des Verordnungsvorschlags auf Dienstleister, die Dienstleistungen in der Union anbieten, unabhängig davon, ob sie in der EU niedergelassen sind oder nicht, mit der Verpflichtung, einen gesetzlichen Vertreter gemäß den im Richtlinienentwurf vorgeschlagenen Regeln zu benennen. Diese Begriffe „Niederlassung“ und „gesetzlicher Vertreter“ sind daher in den Entwurfs-Instrumenten definiert.

[20] Siehe Artikel 7 Absätze 3 und 4.

Der EDSA stellt fest, dass diese Begriffe auch im Zusammenhang mit anderen EU-Instrumenten und insbesondere im Zusammenhang mit der DSGVO zu finden sind. Daher sollten Erläuterungen zur Definition und Abgrenzung dieser Begriffe im Rahmen der Vorschlagsentwürfe und im Rahmen der DSGVO erfolgen.

a) Niederlassung

Der EDSA erinnert außerdem daran, dass der Begriff „Niederlassung“ im Zusammenhang mit dem Verordnungsentwurf nicht mit der Begrifflichkeit im Kontext der DSGVO verwechselt werden darf. Für die Zwecke des Verordnungsentwurfs ist der Begriff der Niederlassung im Sinne von Artikel 2 Absatz 5 weiter gefasst als in der DSGVO, da er „entweder die tatsächliche Ausübung einer wirtschaftlichen Tätigkeit auf unbestimmte Zeit durch eine feste Einrichtung, von der aus die Erbringung von Dienstleistungen erfolgt, oder eine feste Einrichtung, von der aus das Unternehmen geführt wird“, umfasst, unabhängig davon, ob die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten dieser Einrichtung erfolgt oder nicht. Wenn also der Begriff „Niederlassung“ im Sinne der DSGVO zweifellos in die im Verordnungsentwurf definierte Niederlassung einbezogen werden soll, dann wäre das umgekehrt möglicherweise nicht zutreffend.

Der EDSA warnt daher davor, dass Niederlassungen von Dienstleistern im Sinne des Verordnungsentwurfs unter Umständen nicht bedeuten, dass die Bedingungen für die Anwendung der DSGVO gemäß Artikel 3 Absatz 1 erfüllt sind. In diesem Zusammenhang werden Verantwortliche und Auftragsverarbeiter aufgefordert zu prüfen, ob sich die Anwendbarkeit der DSGVO nicht aus Artikel 3 Absatz 2 ergibt, was die Benennung eines gesetzlichen Vertreters innerhalb der EU und das Fehlen eines Verfahrens der Zusammenarbeit und Kohärenz bedeuten würde.

b) Gesetzlicher Vertreter

In ihrer Stellungnahme betonte die WP29, dass jede Verwechslung zwischen der Verpflichtung, einen gesetzlichen Vertreter gemäß Artikel 27 der DSGVO zu benennen, und dem nach dem Entwurf der Verordnung über elektronische Beweismittel vorgesehenen gesetzlichen Vertreter vermieden werden sollte.

Im Zusammenhang mit dem vorliegenden Vorschlagsentwurf möchte der EDSA an diese Empfehlungen anknüpfen und insbesondere betonen, dass nach seinem Verständnis der gesetzliche Vertreter im Sinne des Richtlinienentwurfs über die Bestellung eines gesetzlichen Vertreters im Rahmen der Vorschläge für elektronische Beweismittel in jedem Fall benannt werden muss, mit spezifischen Funktionen ausgestattet ist, unabhängig von einem vom Dienstleister erteilten Mandat die Befugnis hat, Anfragen zu beantworten und im Namen des Dienstleisters zu handeln sowie einer strengeren Haftung als der gesetzliche Vertreter im Rahmen der DSGVO unterliegt.

Darüber hinaus betont der EDSA, dass sich die Verpflichtung, einen gesetzlichen Vertreter im Rahmen der Vorschlagsentwürfe für elektronische Beweismittel zu benennen, unabhängig davon, ob der Dienstleister in der EU niedergelassen ist oder nicht, die Möglichkeit, sogar mehrere gesetzliche Vertreter für denselben Dienstleister im Rahmen des Richtlinienentwurfs für elektronische Beweismittel zu benennen, und die Verpflichtung, die Benennung des gesetzlichen Vertreters den Behörden der Mitgliedstaaten mitzuteilen, von der DSGVO unterscheiden, die keine solchen Verpflichtungen zur Meldung des benannten gesetzlichen Vertreters, Ausnahmen von der Benennung und begrenzte Verantwortlichkeiten des gesetzlichen Vertreters vorsieht.

Angesichts der erheblichen Unterschiede in Bezug auf die Rolle, die Haftung und die Beziehung zu den anderen Niederlassungen des Dienstleisters einerseits und auf den Verantwortlichen oder

Auftragsverarbeiter andererseits empfiehlt der EDSA daher, dass, wenn ein Dienstleister nicht in der EU niedergelassen ist, sondern sowohl der DSGVO gemäß Artikel 3 Absatz 2 als auch der Verordnung über elektronische Beweismittel unterliegt, zwei verschiedene gesetzliche Vertreter benannt werden sollten, jeweils mit klaren, unterschiedlichen Funktionen gemäß dem Instrument, auf dessen Grundlage sie benannt werden.

6. Neue Datenkategorien

Die vorgeschlagene Verordnung definiert in Artikel 2 verschiedene Datenkategorien: Teilnehmerdaten, Zugangsdaten, Transaktionsdaten und Inhaltsdaten. In Erwägungsgrund 20 des Vorschlags der Kommission heißt es ferner: *„Zu den Datenkategorien, die unter diese Verordnung fallen, gehören Teilnehmerdaten, Zugangsdaten, Transaktionsdaten (diese drei Kategorien werden als „Nichtinhaltsdaten" bezeichnet) und Inhaltsdaten. Diese Unterscheidung ist – abgesehen von den Zugangsdaten – in den Rechtsvorschriften vieler Mitgliedstaaten und auch im derzeitigen Rechtsrahmen der USA vorgesehen, der es den Dienstleistern ermöglicht, Nichtinhaltsdaten freiwillig an ausländische Strafverfolgungsbehörden weiterzugeben."*

In diesem Zusammenhang betont der EDSA zunächst, dass alle vier oben genannten Datenkategorien als personenbezogene Daten im Sinne des EU-Datenschutzrechts anzusehen sind, da sie Informationen über eine identifizierte oder identifizierbare natürliche Person enthalten, unabhängig davon, ob die betroffene Person im Verordnungsvorschlag als „Teilnehmer" oder „Nutzer" bezeichnet wird. Ebenso ist anzumerken, dass „elektronische Beweismittel" im Sinne von Artikel 2 Absatz 6 des Vorschlags der Kommission alle vier Kategorien von Daten umfassen und sich daher auf personenbezogene Daten beziehen. Daher sieht der Verordnungsvorschlag keine Vorschriften für den Zugang zu Beweismitteln vor, die gemäß den nationalen Rechts- und Gerichtsverfahren definiert und qualifiziert sind, sondern neue materielle und verfahrensrechtliche Bedingungen für den Zugang zu personenbezogenen Daten.

Während der Verordnungsvorschlag neue Unterkategorien von personenbezogenen Daten einführt, für die unterschiedliche verfahrensrechtliche Zugangsbedingungen gelten, erinnert der EDSA daran, dass es gemäß der einschlägigen Rechtsprechung des EuGH, um das Bestehen eines Eingriffs in das Grundrecht auf Privatsphäre festzustellen, keine Rolle spielt, ob die Informationen über das betreffende Privatleben sensibel sind oder ob den betroffenen Personen in irgendeiner Weise Unannehmlichkeiten entstanden sind.

Darüber hinaus erinnert der EDSA daran, dass der Gerichtshof der Europäischen Union in seinem Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 Tele*2 Sverige AB* in Bezug auf „Nichtinhaltsdaten", die Teilnehmerdaten, Zugangsdaten und Transaktionsdaten umfassen, entschieden hat, dass Metadaten wie Verkehrsdaten und Standortdaten die Möglichkeit bieten, ein Profil der betroffenen Personen zu erstellen, d. h. Informationen, die in Bezug auf das Recht auf Privatsphäre nicht weniger sensibel sind als der eigentliche Inhalt der Kommunikation[21].

Wie bereits in der Stellungnahme der WP29 vom 29. November 2017 zu den Aspekten des Datenschutzes und der Privatsphäre beim grenzüberschreitenden Zugang zu elektronischen Beweismitteln dargelegt, bekräftigt der EDSA daher seine Zweifel und Bedenken in Bezug auf die derzeitige Abgrenzung zwischen „Nichtinhaltsdaten" und Inhaltsdaten sowie auf die vier Kategorien von personenbezogenen Daten, die im Verordnungsvorschlag festgelegt sind. Tatsächlich erscheinen

[21] EuGH-Urteil vom 21. Dezember 2016, Rn. 99.

die vier vorgeschlagenen Kategorien nicht klar abgegrenzt, und die Definition von „Zugangsdaten“ bleibt im Vergleich zu den anderen Kategorien weiterhin unklar. Der EDSA beklagt daher, dass in der Folgenabschätzung und dem Vorschlag der Kommission die Begründung für die Schaffung dieser neuen Unterkategorien personenbezogener Daten nicht weiter substantiiert wurde, und äußert seine Besorgnis über das unterschiedliche Maß an Garantien im Zusammenhang mit den materiellen und verfahrensrechtlichen Bedingungen für den Zugang zu den Kategorien personenbezogener Daten, insbesondere angesichts der praktischen Schwierigkeiten bei der Bewertung, zu welcher Kategorie von Daten die angeforderten Daten in einigen Fällen gehören werden. Beispielsweise könnten IP-Adressen sowohl als Transaktionsdaten als auch als Teilnehmerdaten klassifiziert werden.

In diesem Zusammenhang erinnert der EDSA auch daran, dass die Kommission in Erwägungsgrund 14 ihres Verordnungsvorschlags über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (e-Datenschutz-Richtlinie) die Auffassung vertritt, dass „der Ausdruck „elektronische Kommunikationsdaten“ [...] hinreichend breit und technologieneutral definiert werden [sollte], damit er alle Informationen bezüglich der übermittelten oder ausgetauschten Inhalte (elektronische Kommunikationsinhalte) und die Informationen bezüglich der Endnutzer von elektronischen Kommunikationsdiensten erfasst, die zum Zwecke der Übermittlung, Verbreitung oder Ermöglichung des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden; dazu zählen die zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts eines Kommunikationsvorgangs verwendeten Daten, des geografischen Standorts sowie von Datum, Uhrzeit, Dauer und Art der Kommunikation“. Da der derzeitige und künftige Rechtsrahmen zum Schutz der Privatsphäre in der elektronischen Kommunikation sowie die damit verbundenen Einschränkungen des Rechts auf Privatsphäre auf die Vorschriften über den Zugang der Strafverfolgungsbehörden zu elektronischen Beweismitteln Anwendung finden werden, empfiehlt der EDSA, dass in den Verordnungsvorschlag eine umfassendere Definition der Daten zur elektronischen Kommunikation aufgenommen wird, um sicherzustellen, dass die festzulegenden angemessenen Garantien und Bedingungen für den Zugang sowohl „Nichtinhaltsdaten“ als auch „Inhaltsdaten“ konsequent umfassen.

7. Analyse der Verfahren für Europäische Herausgabe- und Sicherungsanordnungen

Im Großen und Ganzen stellt sich das Verfahren zum Erlass einer Herausgabe- oder Sicherungsanordnung wie folgt dar:

- Die zuständige Justizbehörde – die Anordnungsbehörde – erlässt die Anordnung je nach Art der angeforderten Daten und der Art der Anordnung nach den in den Artikeln 5 und 6 genannten (knappen) Bedingungen, sendet sie unter Verwendung eines harmonisierten Zertifikats an den gesetzlichen Vertreter des Dienstleisters oder an eine seiner Niederlassungen in der EU – den Adressaten.
- Nach Erhalt des Zertifikats führt der Empfänger die Anordnung aus – d. h. übermittelt die Daten innerhalb von 10 Tagen oder 6 Stunden im Dringlichkeitsfall oder speichert sie bis zu 60 Tage – es sei denn, dies ist unmöglich, weil das Zertifikat unvollständig ist oder weil *höhere Gewalt* oder faktische Unmöglichkeit auf Seiten des Empfängers vorliegen, oder weil der Empfänger sich aus Gründen widerstreitender Verpflichtungen, sei es in Bezug auf Grundrechte oder Grundinteressen eines Drittlandes oder aus anderen Gründen, weigert.

- Hat der Empfänger die erhaltene Anordnung ohne Angabe von Gründen, die von der Anordnungsbehörde akzeptiert werden, nicht befolgt, sind Verfahren zur Vollstreckung der Anordnungen durch eine zuständige Vollstreckungsbehörde des Mitgliedstaats, in dem der Dienstleister vertreten oder niedergelassen ist, vorgesehen, es sei denn, es gelten begrenzte Ablehnungsgründe und die Vollstreckungsbehörde erhebt Einwände gegen die Anerkennung oder Vollstreckung der Anordnung.
- Hat der Adressat aufgrund widerstreitender Verpflichtungen einen begründeten Einwand gegen die Anordnung erhoben, so verweist die Anordnungsbehörde die Angelegenheit an das zuständige Gericht in ihrem Mitgliedstaat, das dann für die Beurteilung des möglichen Konflikts und die Aufrechterhaltung der Anordnung in Ermangelung eines Konflikts zuständig ist. Im Falle eines Konflikts muss sich das zuständige Gericht entweder über seine nationalen zentralen Behörden an die zentralen Behörden des Drittlandes mit einer Frist von 15 Tagen zur Beantwortung wenden, die auf begründeten Antrag um 30 Tage verlängert werden kann, wenn es sich um widerstreitende Verpflichtungen in Bezug auf die Grundrechte oder Grundinteressen eines Drittlandes handelt, oder selbst entscheiden, ob es die vom Empfänger geltend gemachte Ablehnung des Beschlusses aus anderen Gründen aufrechterhalten oder zurücknehmen soll.
- Unbeschadet der im Rahmen der DSGVO und der Richtlinie zum Datenschutz bei der Strafverfolgung verfügbaren Rechtsbehelfe müssen Personen, deren Daten über eine Herausgabeanordnung bezogen wurden, auch das Recht auf wirksame Rechtsbehelfe gegen diesen Anordnung haben.

Der EDSA hat die geplanten Verfahren und die im Verordnungsentwurf vorgesehenen Garantien für die verschiedenen Schritte bewertet und empfiehlt zu jedem der nachfolgend vorgestellten Aspekte die folgenden Garantien und Änderungen.

a) Die Schwelle für die Erteilung von Anordnungen sollte angehoben werden, und die Anordnungen sollten von Gerichten erlassen oder genehmigt werden.

Was die Bedingungen für den Erlass von Anordnungen betrifft, so begrüßt der EDSA den Grundsatz höherer Garantien für den Zugang zu Transaktions- oder Inhaltsdaten. Er stellt jedoch fest, dass in Anbetracht der fehlenden vollständigen Harmonisierung der strafrechtlichen Sanktionen zwischen den Mitgliedstaaten die Bezugnahme auf „Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden“[22], nach wie vor unterschiedliche Schwellenwerte und Diskrepanzen beim Schutz der Daten von Betroffenen innerhalb der EU impliziert.

Darüber hinaus betont der EDSA, dass insbesondere angesichts der weiten Definition der Teilnehmerdaten der vorgesehene Schwellenwert für Sicherungsanordnungen und Herausgabeanordnungen bezüglich Teilnehmer- oder Zugangsdaten eher niedrig erscheint, da alle Straftaten grundsätzlich die Erteilung solcher Anordnungen rechtfertigen können. Ebenso sind die Behörden, die zur Erteilung solcher Anordnungen ermächtigt sind, im Rahmen von Herausgabeanordnungen für Transaktions- oder Inhaltsdaten eingeschränkter als bei der Erteilung von Sicherungs- oder Herausgabeanordnungen zur Erhebung von Teilnehmer- oder Zugangsdaten, da

[22] Siehe Artikel 5 Absatz 3 Buchstabe a.

Staatsanwälte nur die letztgenannten Anordnungen erlassen oder genehmigen können, während alle Richter, Gerichte oder Untersuchungsrichter jegliche Anordnung erlassen oder genehmigen können.

Insbesondere bedauert der EDSA, dass die niedrigste Schwelle, die den Strafverfolgungsbehörden die Möglichkeit einräumt, den Zugang zu Teilnehmer- und Zugangsdaten für jede Straftat zu beantragen, auf einem *Umkehrschluss* der Rechtsprechung des EuGH (die sich auf die anderen Daten konzentriert) beruht, um eine Unterscheidung für die zu gewährenden Garantien zu treffen. Tatsächlich betonte der EuGH ausdrücklich, dass der Zugang der zuständigen Behörden für Verkehrs- und Standortdaten ausschließlich auf die Verfolgung schwerer Straftaten beschränkt ist[23]. Der EDSA könnte nachvollziehen, dass der Vorschlag die Möglichkeit vorsah, Zugang zu grundlegenden Informationen zu beantragen, um lediglich eine Identifikation der Person zu ermöglichen, ohne jedoch Kommunikationsdaten ohne vorherige Genehmigung durch ein Gericht offenzulegen. Er beklagt jedoch die weite Auslegung des „*Umkehrschlusses*" dieses Urteils durch die Kommission und fordert die Einführung höherer Garantien, um die Zugangsmöglichkeiten zu anderen Teilnehmerdaten und Zugangsdaten zu begrenzen. Der EDSA schlägt vor, den Zugang zu diesen Daten entweder auf eine im Verordnungsentwurf enthaltene Liste von Straftaten oder zumindest auf „schwere Straftaten" zu beschränken, insbesondere angesichts der niedrigeren für diese Daten vorgesehenen Schwelle für die vorherige Genehmigung.

Darüber hinaus betont der EDSA, dass dieser „*Umkehrschluss*" auch dazu führt, dass der Vorschlag den Staatsanwälten die Möglichkeit eröffnet, Anordnungen zu treffen oder zu genehmigen. Der EDSA ist der Auffassung, dass dies, abgesehen von Anfragen zu grundlegenden Informationen, die nur die Identifizierung einer Person ohne Offenlegung von Kommunikationsdaten ermöglichen würden, einen Rückschritt gegenüber der Rechtsprechung des EuGH über den Zugang zu Kommunikationsdaten darstellt. In der Tat hat der EuGH in seiner Rechtsprechung über den Zugang zu Kommunikationsdaten für Strafverfolgungszwecke die Möglichkeit des Zugangs sowie andere Kriterien „*außer in ordnungsgemäß begründeten Dringlichkeitsfällen*"[24] auf eine „*vorherige Überprüfung durch ein Gericht oder eine unabhängige Verwaltungsbehörde*" und „*auf begründeten Antrag der zuständigen nationalen Behörden im Rahmen von Verfahren der Prävention, Ermittlung oder Strafverfolgung*" begrenzt. [25]

Der EDSA erinnert daran, dass der Begriff „Gericht" ein autonomer Begriff des Unionsrechts ist, und dass der EuGH stets die Kriterien betont und bekräftigt hat, die für die Qualifikation als Gericht zu erfüllen sind, einschließlich des Kriteriums der Unabhängigkeit[26], das bei Staatsanwälten nicht gegeben zu sein scheint, wie auch der EGMR in seiner Rechtsprechung hervorhob[27].

Folglich führen Artikel 4 Absatz 1 Buchstaben a und b und Artikel 3 Buchstaben a und b zu Verfahren, bei denen deutlich weniger Garantien für Teilnehmer- und Zugangsdaten gelten, da ein Staatsanwalt allein Daten anfordern kann, ohne weitere Kontrolle durch die Behörde des Staates, in dem sich die angeforderten Daten befinden, oder durch die Behörde, in der sich der gesetzliche Vertreter des ersuchten Unternehmens befindet, und ohne Kontrolle durch eine unabhängige Verwaltungsbehörde.

Darüber hinaus verweist der EDSA auf die in Artikel 5 Absatz 2 vorgesehene so genannte zusätzliche Garantie, die die Möglichkeit der Erteilung einer Herausgabeanordnung einschränkt, wenn für die gleiche Straftat in einer vergleichbaren nationalen Situation eine ähnliche Maßnahme zur Verfügung

[23] Siehe Rechtssache 203/15, Rn. 125.
[24] Siehe Rechtssache 203/15, Rn. 120.
[25] Siehe die verbundenen Rechtssachen C 293/12 und C 594/12, Rn. 62.
[26] Siehe zum Beispiel die Rechtssache C 203/14.
[27] Siehe zum Beispiel Moulin gegen Frankreich, 23.11.2010,

stand. Er warnt jedoch vor der kontraproduktiven Wirkung einer solchen Bestimmung: statt zusätzliche Garantien zu bieten, erscheint sie als Anreiz für die Mitgliedstaaten, ihre nationalen Möglichkeiten zu erweitern, um die Herausgabe von Teilnehmer- oder Zugangsdaten verlangen zu können und um sicherzustellen, dass Herausgabeanordnungen gemäß dieser Verordnung erteilt werden können.

b) Die Fristen für die Bereitstellung von Daten sollten begründet werden.

Der EDSA weist darauf hin, dass europäische Herausgabeanordnungen spätestens innerhalb von 10 Tagen nach Erhalt des Zertifikats beantwortet werden müssen, es sei denn, die Anordnungsbehörde gibt Gründe für eine frühere Offenlegung an, in Dringlichkeitsfällen spätestens innerhalb von 6 Stunden, wie in Artikel 9 Absätze 1 und 2 vorgesehen.

Der EDSA hat jedoch keine Kriterien für die Verpflichtung der Behörden gesehen, den Dringlichkeitsgrad der Herausgabe von Daten nachzuweisen, auch nicht *ex post*, um eine mögliche Kontrolle der Anwendung dieses sehr schnellen Verfahrens zu ermöglichen, obgleich eine Frist von sechs Stunden wahrscheinlich eine sehr geringe Kontrolle vor der Herausgabe der Daten bedeuten würde, wenn nicht gar das Fehlen einer Kontrolle seitens des Dienstleisters. In der Folgenabschätzung wird jedoch die Notwendigkeit betont, dass die zuständigen Behörden rechtzeitig Zugang zu den Daten haben müssen. Die in der Folgenabschätzung angeführten Beispiele beziehen sich jedoch alle auf Beweismittel, die im Falle schwerer Straftaten benötigt werden (terroristische Handlungen mit Geiseln, anhaltender sexueller Kindesmissbrauch); jedoch scheint die Begründung auf der Grundlage der Volatilität der Beweismittel nicht auszureichen, wenn es keine andere besondere Dringlichkeit als diese mögliche Volatilität der Daten gibt. Darüber hinaus bietet die Volatilität der Daten keine zusätzliche Rechtfertigung für die Verhältnismäßigkeit des Zugangs zu Daten bei geringeren Garantien in diesen Situationen, in denen es keine andere Dringlichkeit als die Volatilität der Daten gibt.

Darüber hinaus bezweifelt der EDSA die Notwendigkeit, eine Frist von sechs Stunden vorzusehen, während eine die Anordnungsbehörde zusätzliche Erläuterungen „innerhalb von fünf Tagen“ liefern kann, falls der Dienstleister seiner Verpflichtung nicht nachkommen kann.

Der EDSA fordert daher zusätzliche Elemente in der Folgenabschätzung, um die Notwendigkeit dieser Fristen in Fällen zu begründen, in denen die begangene oder verfolgte Straftat nicht schwerwiegend ist, und, falls solche detaillierten Elemente nicht zur Verfügung gestellt werden, explizite Kriterien für die Begründung der Dringlichkeit im Falle des Erlasses von EPOC. So könnte beispielsweise das gleiche Modell wie in der EEA-Richtlinie vorgesehen werden. Die EEA-Richtlinie sieht eine kürzere Frist vor, wenn sie durch „Verfahrensfristen, die Schwere der Straftat oder andere besonders dringliche Umstände“ begründet ist (siehe Artikel 12 Absatz 2) oder eine Frist von 24 Stunden, um über vorläufige Maßnahmen zu entscheiden (siehe Artikel 32 Absatz 2). Die Folgenabschätzung des Verordnungsentwurfs sieht in der Tat keine detaillierten Elemente vor, um zu rechtfertigen, warum diese Fristen nicht effizient sind; die einzigen hervorgehobenen Elemente sind, dass die Anzahl der übermittelten Anträge die empfangenden Justizbehörden überlastet, da sie die Fristen nicht einhalten können.

c) Europäische Herausgabe- und Sicherungsanordnungen sollten nicht dazu verwendet werden dürfen, Daten der betroffenen Person eines anderen Mitgliedstaats anzufordern, ohne zumindest die zuständigen Behörden dieses Mitgliedstaats zu informieren, insbesondere nicht im Fall von Inhaltsdaten.

Der EDSA verweist darauf, dass in den bestehenden Instrumenten die justizielle Zusammenarbeit und damit zusätzliche Garantien vorgesehen sind, insbesondere um die Notwendigkeit und Verhältnismäßigkeit von Ersuchen zu gewährleisten, und betont, dass diese Garantien umso gerechtfertigter sind, wenn es sich bei den angeforderten Daten um Inhaltsdaten handelt, die eine stärkere Einschränkung der Rechte der betroffenen Personen auf Schutz ihrer personenbezogenen Daten und ihrer Privatsphäre mit sich bringen. In diesem Zusammenhang erinnert der EDSA daran, dass die EEA-Richtlinie ferner die Möglichkeit vorsieht, die Telekommunikation mit der technischen Unterstützung eines anderen Mitgliedstaats abzufangen (siehe Artikel 30), sowie die Verpflichtung, die zuständige Behörde eines anderen Mitgliedstaats über jede Abfangmaßnahme von Daten zu informieren, wenn keine Unterstützung erforderlich ist und die betroffene Person sich im Gebiet dieses Mitgliedstaats befindet oder befinden wird (siehe Artikel 31).

Der EDSA findet 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.

d) Europäische Sicherungsanordnungen sollten nicht dazu verwendet werden dürfen, die Vorhaltepflichten der Dienstleister zu umgehen.

Der EDSA stellt fest, dass das Hauptziel der Europäischen Sicherungsanordnungen darin besteht, zu verhindern, dass Daten gelöscht werden.

Obwohl der EDSA anerkennt, dass die Verhinderung der Löschung in einigen Fällen notwendig und verhältnismäßig sein kann, bedauert er, dass es keine Schutzmechanismen bei dem Erlass solcher Anordnungen gibt. Insbesondere empfiehlt der EDSA in den Fällen, in denen Sicherungsanordnungen nur für bestimmte Daten erlassen werden (der Entwurf scheint umfassende Anfragen zu ermöglichen) und wenn die ersuchten Dateneigentlich zur Löschung anstehen würden, die Anordnung niemals als Grundlage für den Dienstleister dienen sollte, die Daten nach dem ursprünglichen Löschungsdatum zu verarbeiten. Mit anderen Worten, die Daten sollten „eingefroren“ werden.

Darüber hinaus sollte die Verbindung zwischen der Sicherungsanordnung und der nachfolgenden Anordnung auf Herausgabe der Daten, sei es durch eine Europäische Herausgabeanordnung, einen EEA-Antrag oder ein Rechtshilfeersuchen, verstärkt werden, um sicherzustellen, dass Europäische Sicherungsanordnungen nur dann erteilt werden, wenn der andere Antrag feststeht (und nicht nur als Möglichkeit in Betracht gezogen wird), und dass mit der Ablehnung der Anordnung auf Herausgabe auch die Sicherungsanordnung erlischt, ohne dass 60 Tage[28] gewartet werden muss, wenn der nachfolgende Antrag früher abgelehnt wird.

[28] Siehe Artikel 10 Absatz 1.

e) Geheimhaltung und Benutzerdaten

Der EDSA weist darauf hin, dass ein spezifischer Artikel[29] über die Geheimhaltung der ergangenen Anordnungen in den Verordnungsentwurf aufgenommen wurde. Um Missverständnissen und Verwechslungen mit dem Datenschutzrecht vorzubeugen, erinnert der EDSA daran, dass die DSGVO zwar vorsieht, dass Beschränkungen der Rechte der betroffenen Personen auf die Garantie von Prävention, Ermittlung, Aufdeckung oder Verfolgung strafrechtlicher Sanktionen zwar gesetzlich vorgesehen und daher öffentlich zugänglich sein sollten[30] und dass diese Legislativmaßnahmen besondere Bestimmungen über das Recht der betroffenen Personen auf Information über die Beschränkung enthalten müssen, es sei denn, dies könnte dem Zweck der Beschränkung abträglich sein[31], jedoch nicht die Verpflichtung zur Unterrichtung der einzelnen betroffenen Personen über jeden von den Strafverfolgungsbehörden beantragten Zugang.

Der EDSA weist darauf hin, dass die Datenschutzrichtlinie dieses Auskunftsrecht für die betroffenen Personen gegenüber den zuständigen Behörden selbst vorsieht, wenn dieses Recht nicht beschränkt ist, ohne dass es darauf ankäme, ob die betroffene Person auf dem Gebiet der EU ansässig ist.

f) Verfahren zur Vollstreckung einer Anordnung, wenn der Dienstleister die Ausführung verweigert

Der EDSA weist darauf hin, dass Artikel 14 des Verordnungsentwurfs ein Verfahren vorsieht, um die Vollstreckung einer Anordnung zu gewährleisten, wenn der Adressat ihr nicht nachkommt. In diesem Fallstützen sich die Anordnungsbehörde und die zuständige Behörde im Vollstreckungsstaat auf die justizielle Zusammenarbeit.

Dieses Verfahren erlaubt es der Vollstreckungsbehörde jedoch nicht, die Vollstreckung der übermittelten Anordnung aus anderen als rein verfahrensrechtlichen Gründen (wie beim Adressaten, vor allem wegen des Fehlens von Informationen oder der faktischen Unmöglichkeit der Datenübermittlung) zu verweigern, weil die betreffenden Daten durch eine Immunität oder ein Vorrecht nach innerstaatlichem Recht geschützt sind oder weil ihre Offenlegung ihre grundlegenden Interessen, wie die nationale Sicherheit und Verteidigung, beeinträchtigen kann[32].

Der EDSA äußert daher erneut seine Bedenken hinsichtlich der Aufhebung jeglicher (doppelten)Überprüfung der übermittelten Anordnung durch die empfangende zuständige Behörde im Vergleich zu den anderen Instrumenten. Selbst der Grund, die Vollstreckung einer Anordnung mit der Begründung zu verweigern, dass sie gegen die Charta verstoßen würde, erscheint höher als die klassische Schwelle für eine Verletzung der Grundrechte des Betroffenen. Folglich sollte nach den Beispielen des Europäischen Haftbefehls, der sowohl obligatorische als auch fakultative Ablehnungsgründe vorsieht, oder zumindest der EEA-Richtlinie, die im Allgemeinen vorsieht, dass die Voraussetzung, nach der „die Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts innerhalb der Union auf gegenseitigem Vertrauen und einer Vermutung, dass andere Mitgliedstaaten das Unionsrecht und insbesondere die Grundrechte einhalten, beruht“ widerlegbar ist[33], der Verordnungsentwurf zumindest die klassische Mindestabweichung vorsehen, wonach beim Vorliegen substanzieller Gründe für die Annahme, dass die Vollstreckung einer Verordnung zu einer Verletzung eines Grundrechts der betreffenden Person führen würde und dass der Vollstreckungsstaat seine

[29] Siehe Artikel 11.
[30] Siehe Artikel 23 Absatz 1 Buchstabe d.
[31] Siehe Artikel 23 Absatz 2 Buchstabe h.
[32] Siehe Artikel 14 Absatz 2.
[33] Siehe Erwägungsgrund 19 der EEA-Richtlinie.

Verpflichtungen zum Schutz der in der Charta anerkannten Grundrechte missachten würde, die Vollstreckung der Verordnung verweigert werden sollte.

g) Vollstreckung von Anordnungen und widerstreitenden Verpflichtungen nach dem Recht eines Drittlandes (Artikel 15 und 16)

Der EDSA begrüßt die im Verordnungsentwurf vorgesehene Möglichkeit für die Adressaten, eine Anordnung mit der Begründung abzulehnen, dass sie im Widerspruch zu den Grundrechten stehe, da sie darauf abziele, Garantien bei widerstreitenden rechtlichen Verpflichtungen zu bieten. Er hält es auch für wesentlich, dass der Vorschlag die Konsultation der Behörden von Drittländern vorsieht, zumindest im Falle eines Konflikts, sowie die Verpflichtung zur Aufhebung der Anordnung, wenn die Behörde eines Drittlandes Einspruch erhebt.

Daher sollte das Verfahren, das vorgesehen ist, um die Vollstreckung einer Anordnung aufgrund widerstreitender Verpflichtungen aus dem Drittlandrecht zu verweigern, erheblich verbessert werden.

Erstens stellt der EDSA fest, dass der Verordnungsentwurf ein privates Unternehmen als Empfänger einer Herausgabeanordnung anvertraut, zu prüfen, ob diese Anordnung im Widerspruch zu dem geltenden Recht eines Drittlandes steht, das die Offenlegung der angeforderten Daten verbietet oder nicht. Das Unternehmen muss einen begründeten Einwand erheben, der alle relevanten Einzelheiten des Rechts des Drittlandes, seine Anwendbarkeit auf den vorliegenden Fall und die Art der widerstreitenden Verpflichtungen enthält.

Vor allem ist der EDSA beunruhigt, dass bei einem solchen Einspruch allein das zuständige Gericht des Mitgliedstaats der Anordnungsbehörde beurteilt, ob ein Konflikt vorliegt oder nicht, da das Gericht erst dann mit den Behörden der Drittländer in Kontakt treten kann, wenn es einen Konflikt feststellt. Dem zuständigen EU-Gericht wird somit die Befugnis eingeräumt, das Recht eines Drittlandes in diesem Zusammenhang abschließend auszulegen, ohne in dieser Hinsicht ein echter Spezialist zu sein. Nach Ansicht des EDSA ist die Verpflichtung zur Konsultation der zuständigen Behörden des Drittlandes daher im vorliegenden Vorschlag zu begrenzt. Im Bereich des Datenschutzes weist der EDSA den Gesetzgeber darauf hin, dass, falls ein zuständiges Gericht eines Drittlandes die DSGVO auslegen würde, um zu beurteilen, ob sie im Widerspruch zu seinen eigenen Anforderungen steht, die Datenschutzbehörden der EU und die zuständigen Gerichte weiterhin befugt wären, die Rechtmäßigkeit der Übermittlung auf der Grundlage eines Gerichtsurteils oder einer Entscheidung einer Verwaltungsbehörde eines Drittlandes zu beurteilen, die eine Übermittlung oder Offenlegung personenbezogener Daten im Rahmen der DSGVO verlangt[34].

Darüber hinaus betont der EDSA, dass die Beurteilung des Rechts des Drittlandes durch das zuständige Gericht des ersuchenden Staates der EU auf objektiven Elementen beruhen muss, und ist besorgt über die Kriterien, die das zuständige Gericht bei der Beurteilung des Rechts des Drittlandes gemäß Artikel 15 Absatz 4 und Artikel 16 Absatz 5 Buchstabe a des Verordnungsentwurfs zu berücksichtigen hat. Das Gericht müsste nämlich prüfen, ob das Recht des Drittlandes „nicht dazu bestimmt ist, die Grundrechte oder Grundinteressen des Drittlandes im Zusammenhang mit der nationalen Sicherheit oder Verteidigung zu schützen“, „offensichtlich andere Interessen zu schützen versucht oder darauf abzielt, illegale Aktivitäten vor Strafverfolgungsersuchen im Rahmen von Strafermittlungen zu schützen“ oder „die durch das einschlägige Recht des Drittlandes geschützten Interessen, einschließlich des Interesses des Drittlandes an der Verhinderung der Offenlegung von Daten schützt“. Obwohl diese Bewertung beispielsweise zumindest grundsätzlich eine faktengestützte Bewertung

[34] Siehe Artikel 48 DSGVO.

unter Berücksichtigung aller verfügbaren Informationen im Hinblick auf die potenziellen Auswirkungen einer solchen Entscheidung erfordern sollte, erscheint der Wortlaut („wird angestrebt“) unklar und sollte angepasst werden („hat zum Ziel“).

Der EDSA bedauert, dass der einzige Fall, in dem die Behörden eines Drittlandes konsultiert würden und der Ausführung einer Herausgabeanordnung widersprechen könnten, darin bestünde, dass dieses zuständige EU-Gericht der Ansicht wäre, dass ein relevanter Konflikt vorliegt, alle Elemente an die Zentralbehörden des betreffenden Drittlandes weiterleitet und die Zentralbehörde dieses Drittlandes innerhalb der knappen Fristen von höchstens 50 Tagen (15 Tage, gegebenenfalls um 30 Tage verlängert, und nach einer letzten möglichen Mahnung mit fünf zusätzlichen Tagen) Widerspruch einlegt. In allen anderen Fällen könnte das zuständige Gericht die Herausgabeanordnung aufrechterhalten und eine Geldstrafe gegen den Dienstleister verhängen, der die Ausführung der Anordnung verweigert. Daher ist der EDSA besorgt, dass die zuständigen EU-Gerichte keine umfassendere Verpflichtung haben werden, die zuständigen Behörden der betroffenen Drittländer zu konsultieren, um sicherzustellen, dass das Verfahren in einer systematischeren Weise gewährleistet, dass die Argumente beider Seiten berücksichtigt werden, und um noch mehr Respekt vor den Gesetzen von Drittländern zu zeigen.

Wie bereits in der Stellungnahme der WP29 und vorstehend hervorgehoben, erinnert der EDSA daran, dass Drittländern besondere Aufmerksamkeit geschenkt werden sollte, wenn sie ähnliche Gesetze annehmen, die die Rechte der betroffenen Personen und ihr Recht auf Privatsphäre innerhalb der EU beeinträchtigen könnten, und insbesondere an das Risiko, dass diese in direktem Konflikt mit dem EU-Datenschutzrecht stehen würden.

Darüber hinaus betont der EDSA, dass das zuständige Gericht des Mitgliedstaats der Anordnungsbehörde möglicherweise nicht einmal das zuständige Gericht ist, um die in Artikel 14 des Verordnungsentwurfs vorgesehene Anordnung durchzusetzen, was das Risiko widerstreitender Verfahren und das Fehlen von Gegenkontrollen in einer Situation widerstreitender Gesetze sogar erhöhen würde. Dies ergibt sich daraus, dass in einigen Fällen drei Staaten beteiligt sein könnten: derjenige der Anordnungsbehörde, das Drittland des Dienstleisters und der Mitgliedstaat, in dem sich der gesetzliche Vertreter des Dienstleisters in der EU befindet und in dem die Anordnung vollstreckt werden müsste. Folglich könnte das Gericht der ersuchenden Behörde des Mitgliedstaats A nach dem derzeit geplanten Verfahren das Recht des Drittlandes B des Dienstleisters selbst auslegen, ohne die Meinung der Behörden dieses Drittlandes einzuholen (auch wenn sie gegen die Anordnung Einspruch eingelegt hätten), und ein Gericht eines anderen EU-Mitgliedstaats C ersuchen, seine Entscheidung ohne Widerspruchsmöglichkeit zu vollstrecken.

Darüber hinaus begrüßt der EDSA die Einführung spezifischer Rechtsbehelfe gegen Herausgabeanordnungen, zusätzlich zu den in der DSGVO und in der Richtlinie zum Datenschutz bei der Strafverfolgung vorgesehenen Rechtsbehelfen. Die WP29 hatte bereits in ihrer früheren Stellungnahme solche Schutzmaßnahmen gefordert. Der EDSA beklagt jedoch, dass solche Rechtsbehelfe nicht auch gegen Sicherungsanordnungen vorgesehen sind, da diese auch zu Einschränkungen der Grundrechte der Personen führen können, deren Daten gespeichert werden. Tatsächlich können Sicherungsanordnungen dazu führen, dass Daten länger gespeichert werden, als in den Datenschutzrichtlinien vorgesehen. Daher führt die Sicherungsanordnung an sich zu einer Einschränkung der Grundrechte der betroffenen Person, deren Rechtfertigung einer Überprüfung und spezifischen Rechtsbehelfen unterworfen werden muss, insbesondere in Fällen, in denen die Sicherungsanordnung zusammen mit einer Herausgabeanordnung zur Beschaffung der Daten erlassen wurde. Wie von der WP29 in ihrer Stellungnahme empfohlen, sollten Rechtsbehelfe vorgesehen werden, die mindestens den in einem inländischen Fall verfügbaren Rechtsbehelfen gleichwertig sind.

h) Sicherheit der Datenübermittlung bei der Beantwortung einer Anordnung

Der EDSA stellt fest, dass der Verordnungsentwurf nur Anordnungen für Empfänger innerhalb der Europäischen Union vorsieht und daher keinen spezifischen Kanal für die Übermittlung von Daten zwischen den Empfängern und Dienstleistern mit Sitz außerhalb der Europäischen Union vorsieht.

Der EDSA begrüßt zwar, dass es keine weiteren Ausnahmen vom allgemeinen Datenschutzrechtsrahmen der EU gibt, erinnert aber daran, dass jede an einen Adressaten gesendete Anordnung, die in der Folge eine Übermittlung außerhalb der EU bedeuten würde, den durch die DSGVO vorgegebenen Rechtsrahmen einhalten müsste. Die Umgehung des Rechtsrahmens der justiziellen Zusammenarbeit, der die Einhaltung der Datenschutzgarantien vorsieht, sollte nämlich nicht gleichermaßen zur Umgehung der Anforderungen an die Datenübermittlung durch die Adressaten von Herausgabe- oder Sicherungsanordnungen führen, die diese Anordnungen befolgen müssen.

Der EDSA begrüßt zwar das Fehlen einer Bestimmung, die eine Verpflichtung zur Entschlüsselung verschlüsselter Daten vorsieht[35], ist jedoch besorgt, dass die Vorschlagsentwürfe keine spezifischen Anforderungen an die Adressaten vorsehen, die Authentizität der so erhaltenen Daten zu bewerten, und betont, dass diese Bewertung auch ein Mehrwert traditioneller Instrumente ist, die sich auf die justizielle Zusammenarbeit stützen, und warnt vor den erhöhten Risiken, die sich für die betroffenen Personen ergeben, wenn eine solche Bewertung nicht erfolgt.

Schlussfolgerungen

Auf der Grundlage dieser Bewertung möchte der EDSA die folgenden Empfehlungen an die beiden gesetzgebenden Organe richten:

1) Rechtsgrundlage der Verordnung sollte nicht Artikel 82 Absatz 1 AEUV sein.
2) Die Notwendigkeit eines neuen Instruments im Vergleich zur bestehenden EEA-Richtlinie oder zum MLAT sollte besser nachgewiesen werden, auch durch eine detaillierte Analyse weniger in Grundrechte eingreifender Mittel wie Änderungen der bestehenden Instrumente oder die Beschränkung des Anwendungsbereichs dieses Instruments auf Sicherungsanordnungen in Kombination mit anderen bestehenden Verfahren für den Zugang zu den Daten.
3) Die Verordnung sollte eine längere Frist vorsehen, damit der ausführende Dienstleister sicherstellen kann, dass die Garantien in Bezug auf den Schutz der Grundrechte eingehalten werden können.
4) Das Prinzip der beidseitigen Strafbarkeit sollte beibehalten werden, insbesondere wenn der Standort der Daten als Kriterium keine Bedeutung mehr zukommt, um die Pflicht aufrechtzuerhalten, die in beiden betroffenen Staaten (d.h. im Staat der ersuchenden Behörde und in dem Staat, in dem der Dienstleister ansässig ist) vorgesehenen Garantien zu berücksichtigen.
5) Der Anwendungsbereich der Verordnung sollte auf die Verantwortlichen im Sinne der DSGVO beschränkt werden, oder die Verordnung sollte eine Bestimmung enthalten, die den Auftragsverarbeiter verpflichtet, den Verantwortlichen zu informieren, wenn der betroffene Dienstleister nicht der Verantwortliche, sondern der Auftragsverarbeiter ist.

[35] Siehe Erwägungsgrund 19 und Seite 240 der Folgenabschätzung.

6) Die Verordnung sollte Garantien für die Datenübermittlung in Fällen enthalten, in denen der Dienstleister ohne Angemessenheitsentscheidung für diesen Bereich in einem Drittland niedergelassen ist, oder auf die Richtlinie 2016/680 verweisen, da deren Garantien anwendbar wären.
7) Da die Verordnung in dem Punkt der obligatorischen Benennung eines gesetzlichen Vertreters von der DSGVO abweicht, sollte in der Verordnung präzisiert werden, dass der nach der Verordnung über elektronische Beweismittel benannte gesetzliche Vertreter von dem nach Artikel 3 Absatz 2 der DSGVO benannten Vertreter zu unterscheiden ist.
8) Die Verordnung sollte eine umfassendere Definition der elektronischen Kommunikationsdaten enthalten, um sicherzustellen, dass die noch festzulegenden angemessenen Garantien und Zugangsbedingungen sowohl Nichtinhaltsdaten als auch Inhaltsdaten umfassen.
9) In der Verordnung sollten die Schwellenwerte für den Erlass von Anordnungen angehoben werden, und Anordnungen sollten von Gerichten erlassen oder genehmigt werden müssen, wobei Teilnehmerdaten hiervon ausgenommen werden sollten, sofern die Definition dieser Datenkategorie auf sehr grundlegende Informationen eingegrenzt wird, die nur die Identifizierung einer Person ohne Zugang zu Kommunikationsdaten ermöglichen.
10) Die Verordnung sollte den Zugang zu Teilnehmer- und Zugangsdaten auf eine Liste eng definierter Straftaten oder zumindest auf „schwere Straftaten“ beschränken.
11) Die Frist für die Bereitstellung von Daten, insbesondere in Dringlichkeitsfällen, sollte in der Verordnung besser begründet werden, und die Möglichkeit, auf ein Schnellverfahren von sechs Stunden zurückzugreifen, sollte die damit einhergehende Pflicht der ersuchenden Behörden einschließen, die Dringlichkeit der Anwendung dieses Verfahrens - auch nachträglich - nachzuweisen, um eine Kontrolle der Nutzung dieser Ausnahmebefugnisse zu ermöglichen.
12) Von dem vorgeschlagenen Verfahren, das die Herausgabe von Inhaltsdaten ohne Beteiligung der zuständigen Behörden des Mitgliedstaats, in dem sich die betroffene Person befindet, ermöglichen soll, sollte abgesehen werden.
13) Die Garantien im Zusammenhang mit der Erteilung von Europäischen Sicherungsanordnungen in der Verordnung sollten verbessert werden.
14) Die Verordnung sollte zumindest die klassische Mindestausnahmebestimmung enthalten, dass bei Vorliegen substanzieller Gründe für die Annahme, dass die Vollstreckung einer Anordnung zu einer Verletzung eines Grundrechts des Betreffenden führen würde, die den Vollstreckungsstaat veranlassen würde, seine Pflicht zum Schutz der in der Charta anerkannten Grundrechte zu vernachlässigen, die Vollstreckung der Anordnung verweigert werden sollte.
15) Um subjektive Auslegungen durch ein einziges Gericht zu vermeiden, sollte die Verordnung eine umfassendere Pflicht vorsehen, die zuständigen Behörden eines Drittlandes zu konsultieren, wenn sich der mit der Datenübermittlung beauftragte Dienstleister in einem Konflikt befindet.
16) Die Gültigkeit und die Dauer der Sicherungsanordnungen sollten stärker an die sie begleitenden Herausgabeanordnungen gebunden werden.
17) Es sollte eine bessere Sicherheit der Datenübermittlung gewährleistet werden.
18) Insbesondere für Fälle, in denen verschlüsselte Daten bereitgestellt werden, sollte vorgesehen werden, dass die Echtheit der Daten überprüft werden muss.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)