Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Prof. Dr. Aden, HWR Berlin • Alt-Friedrichsfelde 60 • 10315 Berlin

An den
Finanzausschuss des
Deutschen Bundestages

Per E-Mail an: finanzausschuss@bundestag.de

Prof. Dr. Hartmut Aden
Fachbereich 5
Polizei und
Sicherheitsmanagement
Professur für Öffentliches Recht,
Europarecht, Politik- und
Verwaltungswissenschaft

Stv. Direktor, Forschungsinstitut
für Öffentliche und Private
Sicherheit (FÖPS Berlin)

Behördlicher
Datenschutzbeauftragter der
HWR Berlin

Alt-Friedrichsfelde 60
D-10315 Berlin
T +49 (0)30 30877-2868

privat:
Postfach 580601
D-10415 Berlin

E-Mail: Hartmut.Aden@
hwr-berlin.de

www.hwr-berlin.de/prof/hartmut-aden

www.foeps-berlin.org

Datum: 23. November 2019

Stellungnahme zu dem Gesetzentwurf der Bundesregierung: „Entwurf eines Gesetzes zur Neustrukturierung des Zollfahndungsdienstgesetzes“ (BT-Drucksache 19/12088), vorgelegt zur Anhörung des Finanzausschusses des Deutschen Bundestags am 25. November 2019 in Berlin

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur Mitwirkung an der Anhörung. Wegen des erheblichen Umfangs des Gesetzentwurfs beschränkt sich meine Stellungnahme auf grundsätzliche Defizite des vorliegenden Gesetzentwurfs und ausgewählte Einzelfragen.

Der vorliegende Entwurf verfolgt laut Begründung zwei Hauptziele: Die Grundsätze, die das Bundesverfassungsgericht (BVerfG) in seiner Entscheidung vom 20. April 2016 zum Bundeskrimalamtgesetz (BKAG)[1] aufgestellt hat, sollen nun auch für den Zoll umgesetzt werden. Das Zollfahndungsdienstgesetz (ZFdG) soll außerdem an das neue EU-Datenschutzrecht angepasst werden, hier insbesondere an die Richtlinie (EU) 2016/680,[2] die für die Verfolgung von Straftaten und die auf die Straftatenverhütung gerichtete Gefahrenabwehr maßgeblich ist.

1. Vermeidbare (Über-)Komplexität

Die im vorliegenden Gesetzentwurf gewählte Gesetzgebungstechnik ist wenig überzeugend. Die Regelungen sind unnötig komplex. Dies dürfte die

1 BVerfGE 141, 220.

2 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 Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung […], ABl. L 119 vom 4.5.2016, S. 89.

Verständlichkeit für Normadressat*innen und Zollbedienstete beeinträchtigen und zu Anwendungsfehlern führen.

Besonders augenfällig ist dies bei den zahlreichen Dopplungen in dem sehr umfangreichen Kapitel 3 (§§ 26 bis 83 des Entwurfs). Die Regelungen zum Zollkriminalamt (ZKA) sind unterteilt in Befugnisse als Zentralstelle (Abschnitt 1) und „besondere Befugnisse“ des ZKA (Abschnitt 3, §§ 71ff.). Dazwischen sind in Abschnitt 2 die Befugnisse der Behörden des Zollfahndungsdienstes geregelt. Sehr ähnliche Regelungen kommen sowohl in Abschnitt 1 als auch in Abschnitt 2 vor. Für eine rechtssichere Anwendung wäre es sinnvoller gewesen, die Befugnisse zum ZKA in einem Abschnitt zu bündeln und darüber hinaus einen „allgemeinen Teil“ mit gemeinsamen Befugnissen voranzustellen, wobei bei Bedarf im Detail zwischen dem ZKA und den Behörden des Zollfahndungsdienstes hätte unterschieden werden können. Dies gilt für zahlreiche Vorschriften, u.a. für die Bestandsdatenauskunft (§§ 10 und 30 des Entwurfs), die zugelassen Adressaten der Datenerhebung (§§ 11 bis 12 und 31 bis 32), für die Datenverarbeitung zu Forschungszwecken (§§ 19 und 37 des Entwurfs) sowie für den Schutz des Kernbereichs privater Lebensgestaltung (§§ 49 und 73 des Entwurfs).

Die Strukturierung der bisherigen Gesetzesfassung aus dem Jahr 2002 ist unter diesen Aspekten überzeugender gelungen.

2. Verspätete und unzulängliche Umsetzung der EU-Datenschutzrichtlinie 2016/680

Die Absicht, die Richtlinie 2016/680 nun auch für den Zollbereich umzusetzen, ist zu begrüßen. Die Umsetzungsfrist ist gemäß Art. 63 dieser Richtlinie bereits am 6. Mai 2018 abgelaufen; Gründe, die nach dieser Vorschrift ausnahmsweise eine längere Umsetzungsphase rechtfertigen, liegen nur bei den Teilen der Datenverarbeitung vor, die als automatisierte Abrufsysteme betrieben werden.

Gemäß Art. 288 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) sind Richtlinien für die Mitgliedstaaten hinsichtlich des zu erreichenden Ziels verbindlich. Die mitgliedstaatlichen Regelungen werden folglich bei einer Nachprüfung durch die EU-Datenschutzaufsicht, die Europäische Kommission oder den Gerichtshof der EU (EuGH) daran gemessen, ob diese Ziele erreicht werden. Die Gesetzgebung sollte sich daher nicht darauf beschränken, den zuständigen Behörden die abstrakte Aufgabe zuzuweisen, diese Ziele zu erreichen, sondern sie sollte hierfür

konkrete materiell-rechtliche Vorgaben machen. In dieser Hinsicht enthält der vorliegende Entwurf nur wenig brauchbare Substanz.

a) Privacy by Design und by Default

Hier sei beispielhaft der Grundsatz *Privacy by Design* und *by Default* genannt, dessen Umsetzung Art. 20 RL 2016/680 vorschreibt. Das Ziel dieser Vorschrift besteht darin, dass die Befolgung von Datenschutzvorschriften nicht von den Anwender*innen abhängen soll. Denn bei ihnen bestünde das Risiko, dass sie die Vorschriften nicht oder nicht richtig anwenden, z.B. weil sie diese nicht korrekt kennen oder weil sie mit anderen Aufgaben überlastet sind. *Privacy by Design* und *by Default* verlagert die Verantwortung dagegen auf die Ebene der Ausgestaltung von Hard- und Software. Bereits hier sind die technischen Weichenstellungen so vorzunehmen, dass eine Nutzung der Systeme ohne Einhaltung der Vorgaben zum Schutz der betroffenen Personen nicht möglich ist. Demnach haben die mitgliedstaatlichen Gesetze Maßnahmen zum Schutz der Rechte Betroffener durch Technikgestaltung vorzusehen. Der vorliegende Entwurf konkretisiert diese Zielsetzung indes nicht, sondern delegiert dieses zentrale Element der Richtlinie ohne nähere Konkretisierung an die Zollbehörden (§§ 3 Abs. 9, 19 Abs. 6, 27 Abs. 3, 37 Abs. 6, 99 Abs. 1 des Entwurfs). Damit überlässt der Entwurf der Verwaltung das Erreichen dieses wichtigen Ziels, ohne dafür konkrete Maßstäbe zu festzulegen. Konkrete Ansätze lägen bei einer teil-automatisierten Rechtmäßigkeitskontrolle bei Datenbankeingaben und -abfragen sowie bei technisch voreingestellten Löschungen. Auch die Nachverfolgbarkeit von Datenübermittlungen könnte durch entsprechende Programmierung unterstützt werden.

b) Fairness und Transparenz der Datenverarbeitung

Gemäß Art. 4 Abs. 1 lit. a RL 2016/680 ist der Grundsatz der rechtmäßigen Verarbeitung „nach Treu und Glauben“ in den mitgliedstaatlichen Fachgesetzen umzusetzen. Der Terminus „Treu und Glauben“ in der deutschen Übersetzung ist hier missverständlich. Klarer ist der Begriff „fair“ in der englischen Fassung. Er umfasst das Gebot der Rücksichtnahme auf die Belange der Betroffenen und ein immanentes Gebot transparenter Datenverarbeitung. Hieraus folgt auch für die Arbeit von Sicherheitsbehörden der Vorrang offener gegenüber verdeckter Datenerhebung. Auch müssen die Abläufe für Betroffene nachvollziehbar sein, soweit dadurch das jeweilige

Sicherheitsziel nicht gefährdet wird.[3] Gerade in Sicherheitsbehörden, die eine Kultur von Geheimhaltung und Intransparenz pflegen, werden die Potentiale erhöhter Transparenz, die auch zu mehr Vertrauen und Legitimität ihres Handelns beitragen könnte, häufig unterschätzt.[4]

Der vorliegende Entwurf wird diesen Grundsätzen allenfalls in ersten Ansätzen gerecht. Bereits auf Gesetzesebene sollten grundlegende Entscheidungen getroffen werden, die das Rücksichtnahme- und Transparenzgebot umsetzen. Die ausdrückliche Normierung des Vorrangs offener Datenerhebung wäre hier nur der Mindeststandard.

c) Mangelhafte Regelungen zur Datenqualität und zur Sicherstellung der Korrektur und Löschung übermittelter Daten

Nach der Richtlinie (EU) 2016/680 müssen die Mitgliedstaaten Maßnahmen ergreifen, um die Qualität der verarbeiteten Daten sicherzustellen. Dies liegt nicht nur im Interesse der Betroffenen, sondern auch der Sicherheitsbehörden, für die zutreffende und aktuelle Daten essentiell sind, um effektiv zu arbeiten und unnötigen Arbeitsaufwand zu vermeiden.

Besonders relevant ist die Sicherung der Datenqualität im Zusammenhang mit der Datenübermittlung, die auch im vorliegenden Gesetzentwurf sehr weitreichend zugelassen wird (§§ 21 bis 24 und §§ 65 bis 68 des Entwurfs). Die Vorschriften der Richtlinie (EU) 2016/680 wurden hier nicht bzw. nur unzulänglich umgesetzt. So heißt es in Art. 7 Abs. 3 der Richtlinie:

> „Wird festgestellt, dass unrichtige personenbezogene Daten übermittelt worden sind oder die personenbezogenen Daten unrechtmäßig übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. In diesem Fall ist gemäß Artikel 16 eine Berichtigung oder Löschung oder die Einschränkung der Verarbeitung der personenbezogenen Daten vorzunehmen."

§ 21 Abs. 6 und § 65 Abs. 6 des Entwurfs enthalten Regelungen, basierend auf § 33 Abs. 5 der bisherigen Gesetzesfassung, die dieser Vorschrift zuwider laufen. Diese Vorschriften verpflichten die jeweils zuständigen Stellen, bei Datenübermittlungen an nicht-öffentliche Stellen Übermittlungsnachweise im Regelfall am Ende des Kalenderjahres nach der Übermittlung zu löschen. Dies ist mit Art. 7 Abs. 3 der Richtlinie unvereinbar. Wird erst später bekannt, dass eine übermittelte Information fehlerhaft war

---

3 So auch Johannes/Weinhold, Das neue Datenschutzrecht bei Polizei und Justiz, Baden-Baden 2018, S. 64f.

4 Näher hierzu: Aden, Information Sharing, Secrecy and Trust among Law Enforcement and Secret Service Institutions in the European Union. In: West European Politics (WEP) 2018, 41(4), S. 981-1002

oder nicht mehr aktuell ist, so kann die empfangende Stelle nicht mehr informiert werden, wenn der Übermittlungsnachweis gelöscht wurde. Die Löschung der Übermittlungsnachweise ist vielmehr im Interesse der Datenqualitätssicherung an die Löschung der übermittelten Ausgangsdaten zu koppeln, am besten im Rahmen von technischen Voreinstellungen (s.o., Abschnitt 2a). Dies ist im Interesse der Qualitätssicherung nicht nur für die Datenübermittlung an nicht-öffentliche Stellen, sondern für jegliche Form der Datenübermittlung geboten.

3. Fehlende Begrenzung der Datenverarbeitung in der Substanz

Der Entwurf vermittelt den Eindruck, dass er in erster Linie darauf ausgerichtet ist, die Datenverarbeitungsbefugnisse so wenig wie unbedingt nötig zu beschränken. Die Grenzen des gerade noch Zulässigen werden „ausgereizt".

a) Problematische Datenverarbeitungs-Generalklausel

Problematisch ist die Beibehaltung der Datenverarbeitungsgeneralklausel in § 8 Abs. 1 und § 26 Abs. 1 des Entwurfs, die eine Datenverarbeitung ausschließlich an die *Erforderlichkeit für die Aufgabenerfüllung* knüpft. Nach der alten bundesdeutschen Rechtslage war die Erhebung von Daten hiervon nicht umfasst. Der Entwurf beabsichtigt die Umsetzung der Richtlinie (EU) 2016/680, der ein weiter Verarbeitungsbegriff zugrunde liegt und daher auch die Datenerhebung einschließt. Art. 2 Nr. 2 der Richtlinie definiert die Verarbeitung wie folgt:

> „'Verarbeitung' jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung."

Ausweislich der Entwurfsbegründung[5] soll dem vorliegenden Gesetzentwurf – unionsrechtlich zutreffend – der weite Verarbeitungsbegriff der EU-Richtlinie zugrunde liegen. Damit ist die Datenverarbeitungs-Generalklauseln zugleich eine Datenerhebungsgeneralklausel, ohne dass die Erhebung noch an materielle Voraussetzung wie die Verhütung von Straftaten

[5] BT-Drs. 19/12088, S. 87.

von erheblicher Bedeutung gebunden wäre.[6] Bereits in der bisher geltenden Fassung der §§ 24 Abs. 2 und 27 Abs. 1 ZFdG sind sehr weitreichende Befugnisse zur Informationsbeschaffung mit nur schwach definierten Tatbestandsvoraussetzungen enthalten. Sogar der in Polizeigesetzen übliche Grundsatz des Vorrangs offener Datenerhebung fehlt. Der Verzicht auf materiell-rechtliche und prozedurale Eingrenzungen für die Datenerhebungsgeneralklausel dürfte kaum mit dem verfassungsrechtlichen Bestimmtheitsgebot vereinbar sein.

b) Bestandsdatenauskunft

Die §§ 10 und 30 des vorliegenden Entwurfs regeln die Bestandsdatenauskunft. Diese ermöglicht einen weitreichenden Zugriff auf Telekommunikations-Vertragsdaten und dazugehörige Identifikationsmerkmale wie Internet-Protokolladressen (§§ 95 und 111 Telekommunikationsgesetz, TKG).

Die vorliegende Entwurfsfassung ermöglicht die Bestandsdatenauskunft bereits bei ihrer Erforderlichkeit für die Aufgabenerfüllung. Substantiierte Eingriffsvoraussetzungen, die hier aufgrund des Bestimmtheits- und Verhältnismäßigkeitsgrundsatzes erforderlich wären, fehlen.

c) Quellen-Telekommunikationsüberwachung

Die §§ 72ff. des Entwurfs regeln weitreichende Eingriffe des Zollkriminalamts in das Telekommunikations- und Postgeheimnis (Art. 10 GG). Im Gegensatz zu den allgemeinen Datenverarbeitungsvorschriften sind die Voraussetzungen für diese schwerwiegenden Grundrechtseingriffe hier substantiierter geregelt. Die Anwendungskontrolle durch die Datenschutzaufsicht wird zu überprüfen haben, ob diese Regelungen eine Nutzung der Befugnisse unter Beachtung des Verhältnismäßigkeitsgrundsatzes sicherstellen.

§ 72 Abs. 3 des Entwurfs ermöglicht zusätzlich die Quellen-Telekommunikationsüberwachung. Diese ist beim heutigen Stand der Technik mit einem schweren Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verbunden, vom BVerfG abgeleitet aus Art. 2 Abs. 1 i.v.m. Art. 1 Abs. 1 GG. Die Auffassung, dass sich die Kommunikationsinhalte säuberlich von den übrigen Inhalten des

---

6 Zur Parallelproblematik in der noch nicht angepassten Fassung des § 29 Abs. 1 BPolG: Arzt, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Aufl., München 2019, § 29 Rn. 6.

im Rahmen der Überwachung angegriffenen Systems trennen ließen und daher „nur“ Art. 10 GG betroffen sei,[7] ist jedenfalls beim heutigen Stand der Technik kaum überzeugend. Die Erstreckung auf „Inhalte und Umstände der Kommunikation […], wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können“ (§ 72 Abs. 3 S. 2 des Entwurfs) geht über die Parallelvorschrift in § 51 BKAG hinaus, deren frühere Fassung Gegenstand der Überprüfung durch das BVerfG war.[8]

Die Erweiterung in § 72 Abs. 3 S. 2 des Entwurfs erhöht das Risiko unverhältnismäßiger Eingriffe in die Grundrechte der Betroffenen.

d) Risikomanagement

Basierend auf Art. 46 EU-Zollkondex[9] weist § 3 Abs. 2 des vorliegenden Entwurfs dem Zollkriminalamt Aufgaben im Zusammenhang mit dem Risikomanagement zu. Im Interesse effektiver und effizienter Aufgabenwahrnehmung ist die Orientierung von Kontrolltätigkeiten des Zolls im Allgemeinen und auch der Zollfahndung an Risikoanalysen grundsätzlich zu begrüßen. Problematisch ist indes das Zusammenwirken dieser Aufgabenzuweisung mit der unbestimmt weit gefassten Befugnisnorm zur Erhebung personenbezogener Daten in § 8 Abs. 1 des Entwurfs. Hier wäre klarzustellen, welche zu rechtmäßigen Zwecken bereits erhobenen personenbezogenen Daten neben Informationen aus offenen Quellen im Rahmen des Risikomanagements verwendet werden dürfen. Ziel des Risikomanagements gemäß Art. 46 EU-Zollkodex ist ein effizienter Einsatz von Prüfressourcen, um die ordnungsgemäße Erhebung von Zöllen sicherzustellen. Zusätzliche Überwachungsbefugnisse sind damit nicht verbunden.

e) Kernbereich privater Lebensgestaltung

Der Entwurf enthält zudem längst überfällige Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung (§§ 49 und 73). Ihre Notwendigkeit geht nicht auf die BVerfG-Entscheidung zum BKA-Gesetz aus dem Jahr 2016 zurück,[10] sondern bereits auf die Entscheidung vom 3. März

---

7 S. Entwurfsbegründung, BT-Drs. 19/12088, S. 112.
8 Seinerzeit § 20l BKAG: BVerfGE 141, 220 (Abs. 234).
9 VO (EU) 952/2013.
10 BVerfGE 141, 220.

2004 zur Änderung des Art. 13 GG.[11] Diese Regelungen sind folglich bereits seit 15 Jahren überfällig. Ob die nun getroffenen Regelungen tatsächlich zu einem wirksamen Kernbereichsschutz führen, wird die laufende Überprüfung durch die Datenschutzaufsicht erweisen müssen.

4. Abgrenzung zwischen Strafverfolgung und Gefahrenabwehr

Die Behörden des Zollfahndungsdienstes nehmen Aufgaben wahr, die sowohl gefahrenabwehrend im Vorfeld von Straftaten und Ordnungswidrigkeiten angesiedelt sind – als auch bei deren Verfolgung. Dies kommt bereits in der Überschrift des 2. Abschnitts in Kapitel 3 (vor § 26 des Entwurfs) zum Ausdruck. Folglich vermischt der Entwurf wie die bisherige Gesetzesfassung die Eingriffsbefugnisse zur Gefahrenabwehr und zur Strafverfolgung. Dabei ist zu beachten, dass die strafverfolgende Tätigkeit unter der Verfahrensleitung der zuständigen Staatsanwaltschaft steht. Vorrangig gelten hier die Vorschriften der Strafprozessordnung – das ZFdG hat hier nur ergänzende oder klarstellende Funktionen, kann aber keinesfalls Befugnisse außerhalb der staatsanwaltschaftlichen Verfahrensleitung etablieren. Folglich sollten Gefahrenabwehr- und Strafverfolgungsbefugnisse im Gesetz klarer getrennt werden.

5. Fehlende Regelungen zur Europäischen Staatsanwaltschaft

Die Europäische Staatsanwaltschaft (EUStA) soll Ende 2020 ihre Tätigkeit aufnehmen, basierend auf Verordnung (EU) 2017/1939.[12] Die EUStA wird auch für Straftaten zuständig sein, die in die Zuständigkeit der Zollfahndung fallen, insbesondere für Straftaten zum Nachteil der EU-Einnahmen. Hierzu zählen Straftaten im Zusammenhang mit der Pflicht zur Zahlung von Zöllen und Verbrauchsteuern, soweit das Aufkommen jedenfalls teilweise der EU zusteht.[13] Die EUStA-Verordnung enthält nur zu wenigen Fragen Vollregelungen. Insbesondere die Regelungen zur Zusammenarbeit mit den mitgliedstaatlichen Strafverfolgungsbehörden bedürfen der

---

11 BVerfGE 109, 279; unzutreffend insofern die Entwurfsbegründung, BT-Drs. 19/12088, S. 103.

12 VO (EU) 2017/1939 des Rates zur Durchführung einer Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft (EUStA), ABl. L 283 v. 31.10.2017, S. 1.

13 Art. 22 VO (EU) 2017/1939 i.V.m. Art. 3 Richtlinie (EU) 2017/1371 (Richtlinie zum Schutz der finanziellen Interessen der EU).

weiteren Konkretisierung im mitgliedstaatlichen Recht, auch für die Zollfahndung. Solche Regelungen fehlen in dem vorliegenden Entwurf, so dass zu befürchten ist, dass die deutschen Regelungen nicht rechtzeitig verabschiedet werden, bevor die EUStA ihre Arbeit aufnimmt.[14]

6. Zusammenfassende Empfehlungen

Die genannten Defizite geben **Anlass, den Entwurf zurückzuziehen und das Gesetzgebungsverfahren mit einem neuen Entwurf erneut zu beginnen.** Hierfür sollte – jenseits der vermeidbaren Wiederholungen und anderer „handwerklicher" Schwächen – insbesondere Folgendes berücksichtigt werden:

- Die §§ 8 Abs. 1 und 26 Abs. 1 sind verfassungskonform so umzuformulieren, dass die Datenerhebung (nach der heute maßgeblichen Terminologie als Unterfall der Datenverarbeitung) nicht von der Datenverarbeitungsgeneralklausel umfasst wird. Alle Datenerhebungen sind an substantiierte materiell-rechtliche Voraussetzungen zu binden, z.B. die Aufklärung einer Straftat von erheblicher Bedeutung oder die Abwehr von Gefahren für gewichtige Rechtsgüter, insbesondere auch die Bestandsdatenauskunft (§§ 10 und 30 des Entwurfs). Die Erhebung zusätzlicher personenbezogener Daten im Rahmen des vorgelagerten Risikomanagements ist auszuschließen.
- Bereits im Gesetz sollten klare Vorgaben für technikbasierten Datenschutz (*Privacy by Design* und *by Default*) gemacht werden. Dies betrifft u.a. Vorgaben für die technische Kontrolle der Rechtmäßigkeit von Datenbankeingaben und –abfragen und für die Datenlöschung. Das Fairness- und das Transparenzgebot sind in konkreten gesetzlichen Regelungen auszugestalten.
- Im ZFdG sollten die nötigen Anpassungen für die Zusammenarbeit mit der Europäischen Staatsanwaltschaft (EUStA) vorgenommen werden, damit diese auch in Deutschland planmäßig ihre Arbeit aufnehmen kann.

Gez. Prof. Dr. Hartmut Aden

---

[14] Zu diesem und weiteren Problemen bei der Arbeitsaufnahme der EUStA. H. Aden, M.-L. Sánchez-Barrueco and P. Stephenson, The European Public Prosecutor's Office. Strategies for coping with complexity. Brussels: European Parliament 2019 (Online: http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2019)621806).