DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins vorbereitet durch die Ausschüsse Recht der Inneren Sicherheit, Informationsrecht und Strafrecht

zur öffentlichen Konsultation der Europäischen Kommission über eine Vorratsdatenspeicherung durch Diensteanbieter für Strafverfahren

Stellungnahme Nr.: 57/2025 Berlin/Brüssel, September 2025

Mitglieder des Ausschusses Recht der Inneren Sicherheit

- Rechtsanwältin Lea Voigt, Bremen (Vorsitzende)
- Rechtsanwalt Wilhelm Achelpöhler, Münster (Berichterstatter)
- Rechtsanwalt Dr. David Albrecht, Berlin
- Rechtsanwalt Dr. Eren Basar, Düsseldorf
- Rechtsanwältin Prof. Dr. Annika Dießner, Berlin (ständiges Gastmitglied im Ausschuss)
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Andreas Grözinger, Köln
- Rechtsanwalt Dr. Mayeul Hieramente, Hamburg (Berichterstatter)
- Rechtsanwalt Dr. Saleh Ihwas, Frankfurt am Main
- Rechtsanwältin Dr. Regina Michalke, Frankfurt am Main
- Rechtsanwältin Dr. Vivien Veit, Mönchengladbach
- Rechtsanwalt Prof. Dr. Mark A. Zöller, München (ständiges Gastmitglied im Ausschuss)

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwalt Max Gröning, Geschäftsführer, Berlin
- Rechtsanwältin Katharina Schmidt-Matthäus, Referentin, Berlin

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Prof. Niko Härting, Berlin (Vorsitzender und Berichterstatter)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Prof. Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwalt Dr. Helmut Redeker, Bonn
- Rechtsanwältin Dr. Kristina Schreiber, Köln
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Nicole Narewski, Geschäftsführerin

Mitglieder des Ausschusses Strafrecht

- Rechtsanwalt Dr. Rainer Spatscheck, München (Vorsitzender)
- Rechtsanwalt Stefan Conen, Berlin
- Rechtsanwältin Dr. Gina Greeve, Frankfurt
- Rechtsanwalt Kai Kempgens, Berlin
- Rechtsanwalt Prof. Dr. Stefan Kirsch, Frankfurt am Main
- Rechtsanwältin Dr. Jenny Lederer, Essen
- Rechtsanwalt Prof. Dr. Bernd Müssig, Bonn
- Rechtsanwalt Prof. Dr. Ali B. Norouzi, Berlin
- Rechtsanwältin Dr. Anna Oehmichen, Berlin
- Rechtsanwältin Gül Pinar, Hamburg
- Rechtsanwalt Martin Rubbert, Berlin
- Rechtsanwältin Dr. Heide Sandkuhl, Potsdam

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Tanja Brexl, Geschäftsführerin

Ansprechpartnerinnen in Brüssel:

- Rechtsanwältin Dorothee Wildt, LL.M.
- Myra Jockisch, LL.M.

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt ca. 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

I. Erwägungen zum Konsultationsfragebogen

Der Deutsche Anwaltverein begrüßt die Möglichkeit der Stellungnahme im Rahmen der öffentlichen Konsultation durch die Europäische Kommission.

Die Fragestellungen der Europäischen Kommission innerhalb des Konsultationsfragebogens begegnen jedoch umfassenden Bedenken, die auf den Inhalt der späteren Gesetzgebung durchzuschlagen drohen. Die Fragen sind einseitig und suggestiv zugunsten einer EU-weit einheitlichen Regulierung von Vorratsdatenspeicherung formuliert. Dabei handelt es sich um ein Problem, das die Kommission selbst in ihrer „Better Regulation Toolbox“ von 2023 als „Backward Engineering“ bezeichnet und als Problem für evidenzbasiertes Policymaking identifiziert[1]. Eine Konsultation sollte immer, jedoch insbesondere in einem derart grundrechtssensiblen Bereich wie der Vorratsdatenspeicherung, zunächst ergebnisoffen ausgestaltet sein. Wünschenswert wäre es, dass zunächst der grundsätzliche Regelungsbedarf evaluiert wird.

Auch die geschlossene Fragestellung schränkt die Antwortmöglichkeiten auf ein nicht akzeptables Maß ein. Die Möglichkeit, andere Antwortoptionen unter „Other“ anzugeben, ist nicht gleichwertig wie die originäre Aufnahme dieser Antwortoptionen in den Katalog möglicher Antworten[2].

---

[1] “Backward engineering” refers to situations where the problem analysis is performed with a specific policy option in mind. This not only undermines the quality of the analysis, but it also hurts the credibility of the whole impact assessment process“, vgl. Better Regulation Toolbox (Juli 2023), S. 88.

[2] „When used to collect opinions, the questions and range of answers should be carefully reflected upon to avoid bias“, Better Regulation Toolbox (S. 472). Questions in consultation questionnaires should be

Einige Beispiele:

Gleich zu Beginn der Konsultation wird mehrfach betont, dass eine effektive Kriminalitätsbekämpfung ohne Speicherung von Metadaten nicht möglich sei. Während die Vorteile der Vorratsdatenspeicherung und die Nachteile des Fehlens einer EU-weiten Regelung umfassend dargestellt werden, werden ihren Risiken kaum bis keine Beachtung geschenkt[3].

Es wird von einem Strafverfolgungsdefizit in der EU ausgegangen, nämlich dass „in der heutigen digitalen Gesellschaft die meisten Straftaten, insbesondere solche, die ausschließlich online begangen werden, in der EU nicht erfolgreich untersucht und strafrechtlich verfolgt werden“ können, was dann mit drei möglichen Gründen dekliniert wird. Zwar ist es möglich, diesen Aussagen nicht zuzustimmen, eine anderslautende Grundaussage wird von der EU-Kommission jedoch nicht als Alternative vorgeschlagen.

Die Speicherung von Metadaten zu Strafverfolgungszwecken wird stellenweise verharmlost. Dies wird insbesondere bei der Frage deutlich, bei der die Ermittlungsmethoden danach sortiert werden sollen, wie stark diese in die Privatsphäre des Betroffenen eingreifen. Es werden vor allem Optionen genannt, die zumindest auf den ersten Blick stärker in die Privatsphäre eingreifen als die Vorratsdatenspeicherung, offenbar mit dem Ziel, dass diese Option als am wenigsten eingreifend eingeordnet wird. Diese Ordnung der Maßnahmen suggeriert eine Simplizität der Problematik, die dem Anlass nicht gerecht wird und die nach über zehn Jahren Reflektionsprozess und Rechtsprechungshistorie nach dem Urteil „Digital Rights Ireland“[4] in ihrer Schlichtheit erstaunt[5]. Zumal in nicht wenigen Fällen eine Hausdurchsuchung etwa weniger eingriffsintensiv sein dürfte, als im Rahmen von Vorratsdatenspeicherung sichergestellte persönliche Daten.

---

relevant, short and simple, and be designed in a neutral manner. The right balance between open and closed questions should be struck. (S.471)

[3] So sollen die Vorteile einer Metadatenvorratsdatenspeicherung alle mit „ja“ oder „nein“ bewertet werden, während bei den Risiken lediglich fünf von zwölf Antwortoptionen angekreuzt werden können.

[4] EuGH v. 8.4.2014 - C-293-12 „Digital Rights Ireland“.

[5] Beispielhaft dafür sind auch Fragen zum Wissensstand über Metadatenspeicherung oder dazu ob es unterschiedliche Vorgaben für Speicherdauer bzw. je nach Datentypus geben sollte, was nach gefestigter Rechtsprechung des EuGH gar nicht infrage gestellt werden kann

Auch sollen die Vorteile einer Metadatenvorratsdatenspeicherung alle mit „ja“ oder „nein“ bewertet werden, während bei den Risiken lediglich fünf von zwölf Antwortoptionen angekreuzt werden können.
Während die Erforderlichkeit der Speicherung „für eine längere Dauer oder von zusätzlichen Datenkategorien“ lediglich mit „ja“ oder „nein“ zu beantworten ist, werden für andere ebenso geeignete weniger eingriffsintensive Maßnahmen keine konkreten Alternativen vorgeschlagen, denen man mit „ja“ zustimmen könnte. Die Folge: Dass die Neuregelung für erforderlich gehalten wird ist fast sicher, da die Alternativen unterschiedlich umschrieben sein werden.

Schließlich ist ebenfalls zu beanstanden, dass die Beantwortung aller Fragen zwingend ist und nur bei Beantwortung aller Fragen der Upload einer Freitextstellungnahme möglich ist. Bei einer derart tendenziösen Fragestellung ist die Beantwortung des Fragebogens nicht möglich, wenn der Konsultationsteilnehmer die Grundprämisse der Nützlichkeit der Vorratsdatenspeicherung nicht unterstützt. Dadurch dass der Call for Evidence der Konsultation zeitlich vorgeschaltet war, ist es ihm auch nicht möglich, sein Dokument im Rahmen des Calls for Evidence hochzuladen, ohne auf den Fragebogen zu antworten.

II. Unzureichender Schutz der Berufsgeheimnisträger

Das Anwaltsgeheimnis ist nach der Rechtsprechung des EuGH[6] und des EGMR[7] ein hohes Gut und genießt den besonderen Schutz des Art. 7 GRCh und des Art. 8 Abs. 1 EMRK. Rechtsanwälten wird in einer demokratischen Gesellschaft die Aufgabe der Verteidigung des Rechtsunterworfenen übertragen. Sie können dieser Funktion nur gerecht werden, wenn die Loyalität und Vertraulichkeit gegenüber der Mandantschaft gewährleistet sind.

Art. 6 EMRK begründet zudem für jede Person das Recht auf ein faires Verfahren, insbesondere auf eine effektive Verteidigung. Die essentielle Grundlage hierfür sind Vertrauen und Vertraulichkeit. Die anlasslose Massenspeicherung von Metadaten ist geeignet, eben dieses Vertrauen gegenüber Anwälten zu gefährden. Sobald Daten

[6] EuGH v. 8.12.2022 – C-694/20 Rz. 27f.; EuGH v. 30.5.2024 – C-432/23 Rz. 49f.
[7] EGMR v. 6.12.2012, Michaud/Frankreich, Application no. 12323/11, Rz. 117f; EGMR v. 9.4 2019, Altay/Türkei, Application no. 11236/09, Rz. 49.

gespeichert werden, ist auch die Grundlage für die Gefahr einer Verwendung dieser Informationen gesetzt[8].

Werden Telekommunikationsdienstleister verpflichtet, alle Metadaten zu speichern, wird zwangsläufig auch Anwaltskommunikation im Datenpool erfasst. Ein uneingeschränkter Personenkreis veranlasste den EuGH in seiner Entscheidung zur rechtswidrig erklärten Richtlinie 2006/24/EG, den Eingriff mit *besonderer Schwere* und von *großem Ausmaß* einzustufen[9]. Dabei leitete der EuGH die besondere Schwere des Eingriffs ausdrücklich auch daraus ab, dass die Richtlinie auch für Personen galt, deren Kommunikationsvorgänge dem Berufsgeheimnis unterliegen[10]. Diese Linie bestätigte der EuGH in seiner Entscheidung bezüglich nationaler Vorratsdatenspeicherungsgesetze Schwedens und des Vereinigten Königreichs[11].

Ähnlich wie bei der Bestandsdatenauskunft[12] gilt es, zwischen den Eingriffsformen der Speicherung der Metadaten und der Verwendung dieser Daten zu differenzieren. Der DAV fordert geeignete Schutzvorschriften auf den beiden Eingriffsebenen.

1. Datenspeicherung

Durch Einschränkung der Speicherpflichten muss das Anwaltsgeheimnis bestmöglich geschützt werden. Zu diesem Zweck müssen Vorkehrungen getroffen werden, die die Speicherung geschützter Kommunikation von vornherein ausschließt. Eine solche Vorkehrung kann die Einführung eines „Whitelisting“-Verfahrens sein. Anwaltskanzleien müssen die Möglichkeit erhalten, E-Mail-Adressen und IP-Adressen als geschützt registrieren zu lassen. Telekommunikationsprovider sind sodann zu verpflichten, durch geeignete Filtermaßnahmen Kommunikation, die über registrierte Kanzleiadressen geführt wird, von der Speicherung auszunehmen[13].

2. Datenabfrage

[8] Vgl. Stellungnahme des DAV v. 15.5.2015 Nr.: 25/2015 S. 14.
[9] EuGH v. 8.4.2014 - C-293/12, C-594/12 Rz. 65.
[10] EuGH v. 8.4.2014 - C-293/12, C-594/12 Rz. 58.
[11] EuGH v. 21.12.2016 – C-203/15, C-698/15 – Tele2 Sverige/Watson Rz. 105.
[12] Vgl. BVerfG v. 27.5.2025 -- 1 BvR 1873/13 und 1 BvR 2618/13 Rz. 55.
[13] Vgl. auch Stellungnahme der DAV v. 15.5.2015 Nr.: 25/2015 S. 14.

Ergänzend bedarf es Einschränkungen bei den Abfrage- und Verwendungsbefugnissen staatlicher Behörden, da anderenfalls der Verhältnismäßigkeitsgrundsatz nicht gewahrt bleibt. Im Hinblick auf den vom EuGH geforderten besonderen Schutz des Anwaltsgeheimnisses bedarf es einer Zugangsbeschränkung, die deutlich über Art. 4 der vom EuGH für rechtswidrig erklärten Richtlinie 2006/24/EG hinausgeht und lauten könnte:

> *„Die Mitgliedstaaten erlassen Maßnahmen, um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden. Die Weitergabe von Daten, die dem Anwaltsgeheimnis unterliegen, muss ausgeschlossen werden."*

III. Kompetenzgrundlage

1. Zuständigkeit

Die Rechtsgrundlage für Regelungen zur Vorratsdatenspeicherung ist vor allem in der **Binnenmarktkompetenz aus Art. 114 Abs. 1 AEUV** zu sehen. Der Inanspruchnahme der Binnenmarktkompetenz aus Art. 114 Abs. 1 AEUV steht nicht entgegen, dass das Ziel der Vorratsdatenspeicherung auch in der Strafverfolgung liegt. Auch nach Art. 1 der Richtlinie 2006/24 war es das Ziel der Richtlinie (Art. 1) mit einer Harmonisierung der Vorschriften über die Speicherung, *„sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen*". Da sich die Richtlinie aber darauf beschränkte, Regelungen zur Speicherung aufzustellen, verwarf der EuGH den auf dieses Ziel der Vorratsdatenspeicherung gestützten Einwand Irlands, die Richtlinie könne ebenso wenig wie Fluggastdatenrichtlinie[14] auf die Binnenmarktkompetenz gestützt werden. Hierzu der EuGH:

[14] EuGH v. 30.5.2006, C 317/04 und C 318/04, Rn. 67.

„Angesichts dieses materiellen Gehalts ist zu schlussfolgern, dass die Richtlinie 2006/24 in überwiegendem Maß das Funktionieren des Binnenmarkts betrifft"[15].

In seinem Urteil vom 8. April 2014 **Digital Rights Ireland Ltd -C-293/12**- beanstandete der EuGH nicht prinzipiell eine auf die Binnenmarktkompetenz gestützte Verpflichtung zur Speicherung von Daten, sondern verlangte, dass der mit der Speicherung verbundene Eingriff auf das absolut notwendige Maß beschränkt wird.

2. Unionsrechtliche Beschränkung des Zugangs

Anhaltspunkte dafür, dass der EuGH der Ansicht wäre, die von ihm beanstandeten fehlenden Einschränkungen einer (national begründeten) Verpflichtung zur Übermittlung der Daten hätten mangels Kompetenz gar nicht durch die Richtlinie festgelegt werden können, lassen sich aus dem Urteil nicht herleiten. Das Urteil nimmt zu Kompetenzfragen nicht Stellung.

Alle folgenden Entscheidungen des EuGH zur Vorratsdatenspeicherung betrafen nationale Regelungen und ihre Vereinbarung mit Art. 15 Abs. 1 der Richtlinie 2002/58 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation). Auch die Richtlinie 2002/58 ist auf die Binnenmarktkompetenz Art. 95 EGV/Art. 114 Abs. 1 AEUV gestützt.

Der EuGH hat insoweit festgestellt, dass der Geltungsbereich der auf die **Binnenmarktkompetenz** gestützten Richtlinie auch (nationale) Regelungen erfasst, die „*Tätigkeiten des Staates im strafrechtlichen Bereich, der die öffentlichen Sicherheit, der Landesverteidigung und die Sicherheit des Staates"*[16] betreffen. Denn nationale Regelungen, die eine Verpflichtung der Betreiber elektronischer Kommunikationsdienste vorschreiben, den zuständigen nationalen Behörden Zugang zu diesen Daten zu gewähren, haben zwangsläufig eine Verarbeitung der betreffenden Daten durch die

[15] EuGH 10.2.2009 C-301/06, Rn 83ff.
[16] EuGH v. 21.12.2016 – C 203/15, C 698/15 – Tele2 Sverige/Watson Rn. 69.

Betreiber zur Folge und betreffen folglich den Geltungsbereich der Richtlinie[17]. Zudem ermächtigt Art. 15 Abs. 1 der Richtlinie die Mitgliedstaaten nur in dem dort genannten Rahmen zum Erlass solcher Regelungen.
Der EuGH geht davon aus, dass durch Regelungen einer Richtlinie, die auf die Binnenmarktkompetenz gestützt ist, nationale Regelungen des Zugriffs auf Daten aus Gründen der Sicherheit, Strafverfolgung etc. beschränkt werden kann.
Daraus folgt, dass durch eine Richtlinie, gestützt auf die Binnenmarktkompetenz, den Betreibern elektronischer Kommunikationsdienste eine Vorratsdatenspeicherung vorgeschrieben werden kann, wenn **zugleich** Regelungen getroffen werden, die eine (im nationalen Recht begründete) Verpflichtung der Betreiber elektronischer Kommunikationsdienste zur Übermittlung der Daten beschränken.

Mit diesen **Regelungen der Beschränkung der Übermittlung der Daten** müssen auch Regelungen verbunden sein, die im Hinblick auf die Speicherung der Daten differenzieren, sowohl im Hinblick auf die Art der Daten, der Personen, sowie die Zeit der Speicherung. Ebenso sind Regelungen der Sicherung des ordnungsgemäßen Zugriffs auf die Daten unerlässlich.

Gestaltet man diese vom EuGH vorformulierten Regelungen nicht als eine Regelung der Speicherung und des Zugriffs, sondern allein als **eine Regelung der Speicherung und der Begrenzung einer etwaigen (national geregelten) Pflicht zur Übermittlung**, dann kann sie nach der bisherigen Rechtsprechung des EuGH auf die Binnenmarktkompetenz gestützt werden und wäre zugleich mit den Art. 7, 8 und 11 der Charta vereinbar.

3. Materielle Grenzen der Speicherpflicht

Der EuGH hat sich zu einer mögliche Vorratsdatenspeicherung im Hinblick auf **IP-Adressen** dezidiert geäußert:

> *,,Um sicherzustellen, dass eine solche, genaue Schlüsse auf das Privatleben der betreffenden Person ermöglichende Kombination von Daten ausgeschlossen ist, müssen die Modalitäten der Vorratsspeicherung die Struktur der Speicherung als*

[17] EuGH v. 6.10.2020 C-511/18 und C-512/18, La Quadrature du Net I Rn 93ff.

*solche betreffen, die im Wesentlichen so gestaltet sein muss, dass eine **wirksame strikte Trennung der verschiedenen Kategorien auf Vorrat gespeicherter Daten** gewährleistet ist.“*[18]

Der EuGH postuliert einen wichtigen **Zweckbindungsgrundsatz**. Daten, die für die einen gewichtigen Zweck (vorrats-) gespeichert werden, dürfen nicht zur Verfügung gestellt werden, wenn die mit dem Abruf verfolgten Ziele eine geringere Bedeutung haben. Dies setzt praktisch voraus, dass (vorrats-) gespeicherte Daten in einer Weise gespeichert werden, die den ursprünglichen Speicherzweck erkennen lassen. Hierfür ist eine **Kennzeichnungspflicht** unerlässlich.

Für **Verkehrs- und Standortdaten** hat der EuGH eine **anlasslose** Vorratsdatenspeicherung für unzulässig erklärt und einzig eine behördliche Anordnung, die zwar unterschiedslos wirkt aber anlassbezogen erfolgt, für zulässig erachtet. Der EuGH führt insoweit zum **Schutz der nationalen Sicherheit** aus:

*„sofern **hinreichend konkrete Umstände** die Annahme zulassen, dass sich der betreffende Mitgliedstaat einer als **real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung** für die nationale Sicherheit im Sinne der Rn. 135 und 136 des vorliegenden Urteils gegenübersieht. (…)*

***Die Anordnung, die Daten aller Nutzer elektronischer Kommunikationsmittel präventiv auf Vorrat zu speichern, muss jedoch in zeitlicher Hinsicht auf das absolut Notwendige beschränkt werden**. (…) **Die Speicherung darf somit keinen systematischen Charakter haben**.“*[19]

Da eine solche Regelung jedoch eine behördliche Anordnung im Einzelfall erfordert und eine gesetzliche Speicherpflicht gerade nicht zulässig ist, dürfte insoweit eine unionsrechtliche Regelung nicht zielführend sein.

[18] EuGH v. 30.4.2024 C 470/21, La Quadrature du Net II Rn. 84.
[19] EuGH v. 6.10.2020 C-511/18 und C-512/18, La Quadrature du Net I Rn. 137f.

4. Ergebnis

Die Rechtsgrundlage für Regelungen zur Vorratsdatenspeicherung ist vor allem in der **Binnenmarktkompetenz aus Art. 114 Abs. 1 AEUV** zu sehen. Soweit mit einer Richtlinie daher eine **Verpflichtung der Betreiber** elektronischer Kommunikationsdienste **zur Speicherung** von Bestand- und Kommunikationsdaten vorgesehen wird, ist aus Gründen der Vereinbarkeit mit den Art. 7, 8 und 11 der Charta **zugleich die Verpflichtung der Betreiber** elektronischer Kommunikationsdienste zur Übermittlung der Daten zu beschränken. Auch eine solche **Beschränkung dieser Übermittlungspflichten** kann auf die Binnenmarktkompetenz gestützt werden, sie ist im Hinblick auf den Grundrechtsschutz auch erforderlich.

Durch eine Beschränkung der Übermittlungspflichten und eine **Einschränkung der Speicherpflichten** muss zudem das **Anwaltsgeheimnis** bestmöglich geschützt werden. Durch die Einführung eines **„Whitelisting"-Verfahrens** müssen Anwaltskanzleien die Möglichkeit erhalten, E-Mail-Adressen, IP-Adressen und andere Kontaktdaten als geschützt registrieren zu lassen. Telekommunikationsprovider sind zu verpflichten, durch geeignete Filtermaßnahmen Kommunikation, die über registrierte Kanzleiadressen geführt wird, von der Speicherung auszunehmen.

Mit dieser Beschränkung der Verpflichtung zur Übermittlung der Daten wird der Zugriff auf diese Daten beschränkt, ohne dass damit eine nicht auf die Binnenmarktkompetenz gestützte Regelung des Zugangs zu den Daten aus Gründen der Strafverfolgung und der Sicherheit getroffen würde.

Ein denkbares Regelungsfeld wäre die anlasslose Speicherung von IP-Adressen.

Verteiler

Europa

- Europäische Kommission
  - Generaldirektion Inneres
  - Generaldirektion Justiz
- Europäisches Parlament
  - Ausschuss Bürgerliche Freiheiten, Justiz und Inneres
- Rat der Europäischen Union
- Ständige Vertretung der Bundesrepublik Deutschland bei der EU
- Justizreferenten der Landesvertretungen
- Rat der Europäischen Anwaltschaften (CCBE)
- European Digital Rights (EDRi)

Deutschland

- Bundesministerium der Justiz und für Verbraucherschutz
- Bundesministerium des Innern
- Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages
- Innenausschuss des Deutschen Bundestages
- Arbeitsgruppe Recht der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppe Inneres der im Deutschen Bundestag vertretenen Parteien
- Rechts- und Innenausschüsse der Landtage
- Justizministerien und Justizverwaltungen der Bundesländer
- Landesministerien und Senatsverwaltungen des Innern
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Bundesrechtsanwaltskammer
- Deutscher Richterbund
- Bundesverband der Freien Berufe
- Verdi
- Gewerkschaft der Polizei
- Deutsche Polizeigewerkschaft im DBB
- Europäische Kommission - Vertretung in Deutschland
- stiftung neue verantwortung e.V.
- Deutsches Institut für Menschenrechte
- Gesellschaft für Freiheitsrechte
- Institut für Deutsches und Europäisches Strafprozessrecht
- Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen e. V. – ABV
- Mitglieder des Vorstandes des Deutschen Anwaltvereins
- Vorsitzenden der Landesverbände des Deutschen Anwaltvereins
- Vorsitzenden der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Mitglieder des Ausschusses Recht der Inneren Sicherheit des Deutschen Anwaltvereins
- Mitglieder des Ausschusses Informationsrecht des Deutschen Anwaltvereins
- Mitglieder des Ausschusses Strafrecht des Deutschen Anwaltvereins

Presse

- NJW
- Frankfurter Allgemeine Zeitung
- Süddeutsche Zeitung
- Berliner Verlag GmbH
- Hamburger Abendblatt
- Der Tagesspiegel
- Der Spiegel
- Juris Newsletter
- JurPC
- Netzpolitik.org
- Heise
- LTO
- Neue Zürcher Zeitung
- Frankfurter Rundschau
- Zeit
- beck-online
- Neue Zeitschrift für Verwaltungsrecht
- Die Öffentliche Verwaltung