BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 44
September 2025
Registernummer: 25412265365-88

Öffentliche Konsultation zu einer EU-Initiative zur Vorratsspeicherung von Daten durch Diensteanbieter für Strafverfahren

Mitglieder des Ausschusses Datenschutzrecht

RA Klaus Brisch, LL.M.
RA Malte Dedden
RA Michael Dreßler
RA Peter Hense,
RA Prof. Dr. Armin Herb, (Vorsitzender)
RAin Heike Kraus, MLE, LL.M
RA Jörg Martin Mathis
RAin Simone Rosenthal
RA Dr. Hendrik Schöttle
RA Sebastian Schulz
RA Dr. Volker Schumacher

RA André Haug, Vizepräsident, Bundesrechtsanwaltskammer
RA Sebastian Aurich, LL.M., Bundesrechtsanwaltskammer
Ass. jur. Frederic Boog, LL.M., Bundesrechtsanwaltskammer, Brüssel

Mitglieder des Ausschusses Europa

RA Dr. Sebastian Cording
RA Dr. Hans-Joachim Fritz
RA Marc André Gimmy
RAin Dr. Margarete Gräfin von Galen (Vorsitzende)
RA Andreas Max Haak
RA Dr. Frank J. Hospach
RA Dr. Christian Lemke
RA Maximilian Müller
RAin Dr. Kerstin Niethammer-Jürgens
RA Dr. Hans-Michael Pott
RA Jan K. Schäfer, LL.M.

RAin Stefanie Schott
Prof. Dr. Gerson Trüg
RA Andreas von Máriássy

RA Dr. Christian Lemke, Vizepräsident, Bundesrechtsanwaltskammer
RAin Astrid Gamisch, LL.M., Bundesrechtsanwaltskammer, Brüssel
Ass. jur. Nadja Wietoska, Bundesrechtsanwaltskammer, Brüssel
Ass. jur. Frederic Boog, LL.M., Bundesrechtsanwaltskammer, Brüssel
Ass. jur. Sarah Pratscher, Bundesrechtsanwaltskammer, Brüssel

Mitglieder des Ausschusses Strafrecht (Strauda)

RAin Dr. Carolin Arnemann
RA Prof. Dr. Jan Bockemühl
RA Prof. Dr. Alfred Dierlamm
RA Prof. Dr. Björn Gercke
RA Dr. Mayeul Hiéramente
RA Thomas C. Knierim
RA Dr. Daniel M. Krause
RAin Theres Kraußlach
RA Prof. Dr. Holger Matt (Vorsitzender)
RA Prof. Dr. Ralf Neuhaus
RA Prof. Dr. Tido Park
RAin Dr. Hellen Schilling
RA Dr. Jens Schmidt
RAin Dr. Annette von Stetten

RAin Leonora Holling, Schatzmeisterin, Bundesrechtsanwaltskammer

Mitglieder des Ausschusses Strafprozessrecht

RA Dr. Matthias Dann
RA Prof. Dr. Michael Gubitz
RAin Dr. Vera Hofmann
RA Prof. Dr. Christoph Knauer (Vorsitzender)
RA Dr. jur. Andreas Minkoff
RA Maximilian Müller, LL.M.
RA Jürgen Pauly
RAin Anette Scharfenberg
RAin Dr. Alexandra Schmitz
RAin Stefanie Schott
RA Prof. Dr. Gerson Trüg

RAin Leonora Holling, Schatzmeisterin, Bundesrechtsanwaltskammer
RAin Eva Melina Buchmann, Bundesrechtsanwaltskammer

Verteiler: Europäische Kommission
Bundeskanzleramt
Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium des Innern und für Heimat
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Rechtsausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesnotarkammer
Bundessteuerberaterkammer
Bundesverband der Freien Berufe
Deutscher Anwaltverein
Deutscher Juristinnenbund
Deutscher Notarverein
Deutscher Richterbund
Neue Richtervereinigung e.V.
Patentanwaltskammer
Bundessteuerberaterkammer
Deutscher Steuerberaterverband e.V.
Wirtschaftsprüferkammer
Gesellschaft für Datenschutz und Datensicherheit e. V.
Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Deutsche Vereinigung für Datenschutz e. V.
Bitkom e. V.
davit – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.
eco – Verband der Internetwirtschaft e. V.
VAUNET – Verband Privater Medien e. V.
Stiftung Datenschutz
Datenschutzberater
Computer und Recht
Netzpolitik.org
Redaktionen der NJW, ZAP, AnwBl, DRiZ, FamRZ, FAZ, Süddeutsche Zeitung, Die Welt, taz, PinG, Tagesspiegel, Table.Media, Handelsblatt, dpa, Spiegel, Focus, Deubner Verlag Online Recht, Beck aktuell, Jurion Expertenbriefing, Juris Nachrichten, Otto Schmidt Verlag

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Sie bezieht zur Öffentliche Konsultation zu einer EU-Initiative zur Vorratsspeicherung von Daten durch Diensteanbieter für Strafverfahren auf Basis des von der EU-Kommission ausgegebenen Fragebogens wie folgt Stellung:

The German Federal Bar (Bundesrechtsanwaltskammer, BRAK) is the umbrella organisation of the self-regulatory bodies of the German Rechtsanwälte. It represents the interests of the 28 German Bars and thus of the entire legal profession in the Federal Republic of Germany, which currently consists of approximately 166,000 lawyers, vis-à-vis authorities, courts and organisations at national, European and international level.

Based on the questionnaire issued by the European Commission, the BRAK submits the following remarks on the public consultation on an EU initiative on data retention by service providers for criminal proceedings:

Stellungnahme / Position Paper

Methodik

Bei künftigen Konsultationen sollte stärker auf eine hinreichend offene Fragestellung und eine breitere Auswahl an Antwortmöglichkeiten geachtet werden. Insbesondere die Gestaltung der Fragen 10 („Was versprechen Sie sich von einer EU-Initiative zur Vorratsdatenspeicherung, was auf nationaler Ebene nicht erreicht werden kann?“) und 11 („Welche Bedenken könnte eine EU-Initiative im Bereich der Vorratsdatenspeicherung Ihrer Meinung nach hervorrufen? Wählen Sie die fünf wichtigsten Bedenken aus“) erscheint tendenziös und schließt berechtigte und naheliegende Kritik aus.

Methodology

In future consultations, it has to be ensured that questions are sufficiently open-ended and that there is a wider range of possible answers. In particular, the wording of questions 10 ('What do you expect to be achieved by an EU initiative on data retention that cannot be achieved at national level?') and 11 ("Which concerns could an EU initiative in the area of data retention raise in your view? Pick the five main concerns") appears biased and excludes legitimate and obvious criticism.

Inhaltlich

Zu Frage 1) Wie sind Sie von Gesetzgebung in diesem Bereich betroffen?
(“*How are you affected by legislation in this area?”)*

Antwortauswahl:

- Als Bürger/Nutzer digitaler Dienste
  (“As a citizen/user of digital services”)

- Als Mitarbeiter einer Strafverfolgungs- oder Justizbehörde (Richter, Staatsanwalt, Polizei)
  (“As staff of a law enforcement or judicial authority (judge, prosecutor, police)”)

- Als Beamter einer Behörde oder Verwaltung
  (“As a civil servant of a public authority or administration”)

- ✓ **Als Anwalt/Anwältin**
  („as a lawyer“)

- ○ Als Mitarbeiter eines Anbieters elektronischer Kommunikationsdienste im Sinne von Art. 2 Abs. 4 der Richtlinie (EU) 2018/1972 zur Festlegung des Europäischen Kodex für elektronische Kommunikation
  (“As an employee of an electronic communication service provider as defined in Art. 2 (4) of Directive (EU) 2018/1972 establishing the European Electronic Communications Code”)

- ○ Als Mitarbeiter eines Anbieters von Diensten der Informationsgesellschaft (z. B. OnlineDienste, Cloud-Dienste, soziale Netzwerke, Plattformen usw.)
  (“As an employee of an information society service provider (e.g. online services, cloud services, social networks, platforms etc) »)

- ○ Als Mitarbeiter einer Nichtregierungsorganisation (NGO)
  (“As an employee of a non-governmental organisation (NGO)”)

- ○ Als Wissenschaftler
  („As an academic“)

- ✓ **Sonstige**
  („other“)

Erläuterung zu dieser Antwort:

Die Vorratsdatenspeicherung würde alle **Rechtsanwältinnen und Rechtsanwälte** betreffen, die im Anwendungsbereich der zu erwartenden Vorschriften elektronisch kommunizieren. Potenziell sind davon nicht nur die Kommunikationsmetadaten umfasst, sondern häufig sekundär auch die Korrespondenz der Anwaltschaft – namentlich solche mit Mandantinnen und Mandanten sowie mit Gerichten, (Ermittlungs-)behörden und anderen Anwaltskanzleien. Die Anwaltschaft wäre also in erheblichem Umfang betroffen. Sofern durch die Speicherpflichten - wie zu erwarten steht - Mandatskontakte (oder bei einer strengeren Regulierung sogar Mandatsinhalte) über längere Zeiträume nachvollziehbar würden, wäre die Anwaltschaft und vor allem ihre Mandantschaft auch qualitativ und in rechtsstaatlich mindestens bedenklicher Weise betroffen. Dies kann durch ein Verbot von direkt gegen Anwältinnen und Anwälte oder die Bundesrechtsanwaltskammer gerichtete Maßnahmen sowie durch nachträgliche Aussonderungspflichten von anwaltlichen Verbindungs-, Bestands- (oder gar Inhalts)-Daten nicht hinreichend begrenzt werde. Denn um Daten als zu einem Anwalt gehörend zu identifizieren, muss bereits eine Auseinandersetzung mit den Daten erfolgen und zumindest die Tatsache, dass es sich um einen Anwalt oder eine Anwältin handelt, erfasst werden. Dies reicht aus, um Mandatskontakte oder sonstige anwaltliche Korrespondenz als solche zu identifizieren und ist geeignet, Mandantinnen und Mandanten von der Inanspruchnahme rechtlichen Rates oder rechtlicher Vertretung abzuhalten. Eine Technologie, die von der Verschwiegenheit umfasste Daten von anderen unterscheiden kann, gibt es nicht. Die Anwaltschaft wäre insoweit an der Erfüllung ihres rechtsstaatlichen Auftrags gehindert. Neben den Vertraulichkeitsgrundrechten aller betroffenen Anwältinnen und Anwälte, Mandantinnen und Mandanten sowie sonstiger Beteiligter litten folglich auch der Zugang zum Recht und damit die Rechtsstaatlichkeit in der EU im Allgemeinen.

Anwaltliche Kommunikation unterliegt dem Verschwiegenheitsgebot, welches, wie vom EGMR in ständiger Rechtsprechung betont, dem Schutz des Art. 8 EMRK unterfällt. Eingriffe in dieses Recht sind zwar möglich, unterliegen aber den strengen Voraussetzungen dessen, was in einer demokratischen

Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer. Eingriffe müssen daher verhältnismäßig sein und was insbesondere verhältnismäßig ist. Aus einer Gesamtschau der Antworten des vorliegenden Fragebogens ergibt sich, dass diesbezüglich mit Blick auf die Vorratsdatenspeicherung enorme Zweifel bestehen, s. auch Rechtsprechung des EuGH. Die Vorratsdatenspeicherung gefährdet nach unserer Ansicht kumulativ das Recht auf Achtung des Privatlebens sowie die Vertraulichkeit elektronischer Kommunikation (Art 8 Abs 1 EMRK und Art 7 GRC), den Anspruch auf ein faires Verfahren inklusive einer Verteidigung (Art 6 Abs 1 Satz 1, Abs 3 lit c EMRK), die Unschuldsvermutung (Art 6 Abs 2 EMRK), das Recht auf einen wirksamen Rechtsbehelf inklusive der Beratung, Verteidigung und Vertretung (Art 47 Abs 1 und Abs 2 Satz 2 GRC), sowie die Freiheit der Meinungsäußerung und die Informationsfreiheit (Art 11 GRC)

Als Betreiberin des besonderen elektronischen Anwaltspostfachs(beA) und Teilnehmer am elektronischen Rechtsverkehr wären auch die **BRAK und ihre 28 Mitglieds-Rechtsanwaltskammern** umfänglich und eingriffsintensiv von entsprechenden Regelungen betroffen. Die Rechtsanwaltskammern führen unter anderem sensible, dem Berufsgeheimnis bzw. Amtsgeheimnis unterliegende elektronische Korrespondenzen etwa zu berufsrechtlichen Verfehlungen, Anwalts- und Strafgerichtsverfahren sowie gegebenenfalls Mandatsinhalten über das beA.

Die Bundesrechtsanwaltskammer steht Bestrebungen zu einer allgemeinen Speicherpflicht daher ablehnend gegenüber. Sollte eine solche gleichwohl eingeführt werden, könnte sich eine zusätzliche Betroffenheit daraus ergeben, dass die Eintragung einer Person im von der Bundesrechtsanwaltskammer betriebenen Bundesweiten Amtlichen Anwaltsverzeichnis (BRAV) und / oder deren Authentifizierung mittels Log-ins ins beA-System als Grundlage für die in einem solchen Fall zwingend erforderliche Aussonderungen von anwaltlichen Daten dienen könnte. Für Gespräche über Aussonderungsmechanismen steht die BRAK jederzeit zur Verfügung.

"How are you affected by legislation in this area?"

Data retention affects all lawyers who communicate electronically within the scope of the planned legal acts. Potentially, this will not only cover communication metadata, but often also, secondarily, correspondence between lawyers – namely correspondence with clients, courts, (investigative) authorities and other law firms. The legal profession will therefore be significantly affected. If, as expected, the retention obligations mean that client contacts (or, in the case of stricter rules, even client content) could be traced over longer periods of time, the legal profession and, above all, its clients will also be affected in a way that is at least questionable in terms of quality and the rule of law. This cannot be sufficiently limited by a ban on measures aimed directly against lawyers or the German Federal Bar, or by subsequent obligations to separate lawyers' contact, inventory (or even content) data.

In order to identify data as belonging to a lawyer, the data must first be examined and at least the fact that it relates to a lawyer must be recorded. This is sufficient to identify client contacts or other legal correspondence as such and is likely to deter clients from seeking legal advice or representation. There is no technology that can distinguish data covered by confidentiality from other data. This would prevent the legal profession from fulfilling its constitutional mandate. In addition to the fundamental rights of confidentiality of all lawyers, clients and other parties involved, access to justice and thus the rule of law in the EU in general would also suffer.

Communication between lawyers and their clients is subject to confidentiality, which, as pointed out by the ECtHR in well-established case law, is protected under Article 8 of the ECHR. Interference with this right is possible, but it is subject to strict conditions imposed by what is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Any interference must therefore be proportionate. An overall view of our responses to the present questionnaire shows that there are enormous doubts with regard to data retention, see also the case law of the ECJ. In our opinion, data retention cumulatively jeopardises the right to respect for private life and the confidentiality of electronic communications (Art. 8(1) ECHR and Art. 7 CFR), the right to a fair trial, including a defence (Art. 6(1) sentence 1, para. 3(c) ECHR), the presumption of innocence (Art. 6(2) ECHR), the right to an effective remedy, including advice, defence and representation (Art. 47(1) and (2), second sentence, CFR), and freedom of expression and information (Art. 11 CFR).

As the operator of the special electronic lawyers' mailbox (beA) – and a participant in electronic legal transactions –, the BRAK and its 28 member bars would also be extensively and intensively affected by such a legislation. Among other things, the bars conduct sensitive electronic correspondence subject to professional secrecy or official secrecy via the beA, for example on professional misconduct, lawyer and criminal court proceedings and, where applicable, client matters.

The BRAK therefore opposes efforts to introduce a general retention obligation. Should such an obligation nevertheless be introduced, an additional impact could result from the fact that a person's registration in the Federal Official Lawyers' Directory (BRAV) operated by the German Federal Bar and/or their authentication by means of logins to the beA system could serve as the basis for the mandatory exclusion of lawyers' data in such a case. The BRAK is available at any time for discussions on exclusion mechanisms.

Zu Frage 2) Sind Sie der Meinung, dass die für die Ermittlung und Verfolgung von Straftaten zuständigen Behörden in der heutigen digitalen Gesellschaft über ausreichende Instrumente verfügen?

("Do you consider that, in today's digital society, public authorities in charge of investigating and prosecuting crimes have sufficient tools at their disposal?")

Antwortauswahl:

- Stimme voll und ganz zu („Fully agree'")
- ✓ **teilweise Zustimmung *(„somewhat agree")***
- Weder zustimmen noch ablehnen („Neither agree nor disagree")
- Eher nicht („Somewhat disagree")
- Völlig dagegen („Fully disagree")
- Ich weiß nicht („I don't know")

Erläuterung der Antwort:

Angesichts hoher Aufklärungsraten sieht die BRAK die Notwendigkeit zusätzlicher genereller Speicherpflichten als nicht überzeugend belegt. Die vorhandenen rechtlichen Instrumente sind

ausreichend. Es besteht stattdessen ein Umsetzungsdefizit, das primär auf die nicht ausreichende materielle und personelle Ausstattung der Ermittlungsbehörden zurückzuführen ist.

"Do you consider that, in today's digital society, public authorities in charge of investigating and prose-cuting crimes have sufficient tools at their disposal?"

In view of high detection rates, the BRAK does not consider the need for additional general retention obligations to be convincingly proven. The existing legal instruments are sufficient. Instead, there is an implementation deficit, which is primarily due to the insufficient material and personnel resources available to the investigating authorities.

Zu Frage 3) In der heutigen digitalen Gesellschaft können die meisten Straftaten, insbesondere solche, die ausschließlich online begangen werden, in der EU nicht erfolgreich untersucht und strafrechtlich verfolgt werden, da es an digitalen Beweisen mangelt, die unter anderem die Identifizierung und Lokalisierung von Verdächtigen ermöglichen würden. Inwieweit stimmen Sie dieser Aussage zu?

("In today's digital society, most crimes, especially those committed solely online, cannot be successfully investigated and prosecuted in the EU, because of a lack of available digital evidence which can enable, among other things, the identification and localisation of suspects. To what extent do you agree with this statement?")

Antwortauswahl:

- Stimme voll und ganz zu („Fully agree'")
- teilweise Zustimmung *(„somewhat agree")*
- Weder zustimmen noch ablehnen („Neither agree nor disagree")
- ✓ **Eher nicht („Somewhat disagree")**
- Völlig dagegen („Fully disagree")
- Ich weiß nicht („I don't know")

Erläuterung der Antwort:

Die Aufklärungsquoten sind bereits ohne flächendeckende Speicherpflichten hoch. Es werden derzeit mehr digitale Spuren erzeugt als je zuvor. Ein quantitatives Defizit liegt daher eher fern. Optimierungsbedarf könnte hingegen mit Blick auf die Datenqualität und personelle oder technische Auswertungsmöglichkeiten bestehen. Beides ließe sich durch flächendeckende Speicherpflichten jedoch nicht adressieren.

In today's digital society, most crimes, especially those committed solely online, cannot be successfully investigated and prosecuted in the EU, because of a lack of available digital evidence which can enable, among other things, the identification and localisation of suspects. To what extent do you agree with this statement?"

The clearance rates are already high without comprehensive retention obligations. More digital traces are currently being generated than ever before. A quantitative deficit is therefore unlikely. However, there may be a need for optimisation in terms of data quality and personnel or technical evaluation capabilities. Neither of these issues could be addressed by comprehensive retention obligations.

Zu Frage 4) In der heutigen digitalen Gesellschaft können die meisten Straftaten, insbesondere solche, die ausschließlich online begangen werden, in der EU aufgrund fehlender gesetzlicher Verpflichtungen oder Vorschriften nicht erfolgreich untersucht und strafrechtlich verfolgt werden. Inwieweit stimmen Sie dieser Aussage zu?

("In today's digital society, most crimes, especially those committed solely online, cannot be successfully investigated and prosecuted in the EU, due to lack of legal obligations or rules. To what extent do you agree with this statement")

Antwortauswahl:

- Stimme voll und ganz zu („Fully agree'")
- teilweise Zustimmung *(„somewhat agree")*
- Weder zustimmen noch ablehnen („Neither agree nor disagree")
- ✓ **Eher nicht („Somewhat disagree")**
- Völlig dagegen („Fully disagree")
- Ich weiß nicht („I don't know")

Erläuterung der Antwort:

Derzeit dürfte auch in den meisten grenzüberschreitenden Sachverhalten nach den bestehenden nationalen wie internationalen Regeln zur Rechtsanwendung und -auslegung klar ermittelbar sein, welche Rechtsvorschrift anzuwenden ist und wie diese – ggf. im Lichte des EU-Primärrechts, der Grundrechtecharta und der Rechtsprechung des Europäischen Gerichtshofs – auszulegen ist. Einzig, wo dies im Einzelfall nicht möglich sein sollte, könnte eine Harmonisierung helfen. Dieser eher theoretische Anwendungsfall wird zusätzlich dadurch begrenzt, dass derzeit nur einige EU-Mitgliedstaaten überhaupt Regelungen zur Vorratsdatenspeicherung haben oder anstreben.

Dieses allenfalls marginalen Harmonisierungsbedürfnis kann keine Ausweitung einer grund- und verfassungsrechtlich zweifelhaften allgemeinen Speicherpflichten rechtfertigen. Allenfalls könnte eine Harmonisierung im Sinne es Level-Downs bei der Speicherpflicht und einer Ausweitung des Grundrechtsschutzes befürwortet werden: nämlich einer EU-weiten Abschaffung von Mindestspeicherpflichten.

Sollte demgegenüber zweifelhafter Weise eine Harmonisierung überwiegend für erforderlich erachtet werden, dürfte diese eine Speicherpflicht allenfalls unter äußerst strengen Voraussetzungen und Schutzvorgaben vorsehen.

In today's digital society, most crimes, especially those committed solely online, cannot be successfully investigated and prosecuted in the EU, due to lack of legal obligations or rules. To what extent do you agree with this statement

At present, even in most cross-border cases, it should be possible to clearly determine which legal provisions apply and how they should be interpreted – where necessary in light of EU primary law, the EU- Charter of Fundamental Rights and the case law of the European Court of Justice – in accordance with existing national and international rules on the application and interpretation of law. Only where this is not possible in individual cases could harmonisation be of help. This rather theoretical application is

further limited by the fact that only a few EU Member States currently have or are seeking to introduce regulations on data retention.
This marginal need for harmonisation cannot justify the extension of general retention obligations that are questionable under fundamental and constitutional law. At most, harmonisation could be advocated in the sense of a level-down in retention obligations and an extension of fundamental rights protection: namely, the EU-wide abolition of minimum retention obligations.
If, on the other hand, harmonisation were deemed necessary, which is doubtful, it should only provide for retention obligations subject to extremely strict conditions and protection requirements.

Zu Frage 5) In der heutigen digitalen Gesellschaft können die meisten Straftaten, insbesondere solche, die ausschließlich online begangen werden, in der EU aufgrund fehlender personeller Ressourcen, Fähigkeiten, Schulungen usw. nicht erfolgreich untersucht und strafrechtlich verfolgt werden. Inwieweit stimmen Sie dieser Aussage zu?

("In today's digital society, most crimes, especially those committed solely online, cannot be successfully investigated and prosecuted in the EU, due to lack of human resources, skills, training, etc. To what extent do you agree with this statement?")

Antwort:

- *Stimme voll und ganz zu*
- *Stimme eher zu*
- ✓ ***Weder zustimmen noch ablehnen***
- *Eher nicht*
- *Stimme überhaupt nicht zu*
- *Ich weiß nicht*

Erläuterung der Antwort:

Die Statistiken weisen eher hohe Aufklärungsraten auf. Insofern trifft die Aussage nicht zu. Bezüglich verbleibender Aufklärungslücken liegen die in der Frage genannten Gründe aber nahe.

In today's digital society, most crimes, especially those committed solely online, cannot be successfully investigated and prosecuted in the EU, due to lack of human resources, skills, training, etc. To what extent do you agree with this statement?"
The statistics show rather high detection rates. In this respect, the statement is not accurate. However, the reasons mentioned in the question are likely to be the cause of the remaining gaps in detection rates.

Zu Frage 6) Wie gut kennen Sie sich mit Gesetzen und Richtlinien zur Speicherung von Metadaten durch Dienstleister zum Zwecke der Verhinderung, Aufdeckung, Untersuchung und Verfolgung von Straftaten aus?

("How familiar are you with laws and policies related to retention of metadata by service providers for the purpose of preventing, detecting, investigating and prosecuting crimes?")

Antwortauswahl:

- Ich bin damit nicht vertraut. *(„I am not familiar with it.")*
- Ich weiß, dass es solche Vorschriften und Richtlinien gibt, kenne aber keine Details. („*I am aware of the existence of such rules and policies, but I do not know details")*
- ✓ **Ich habe detaillierte Kenntnisse zu diesem Thema.** *(„I have detailed knowledge of the subject")*

Erläuterung der Antwort:

Die BRAK verfügt über hochkarätig besetzte Expertengremien aus der Rechtspraxis und hat mehrere Stellungnahmen (Nr. 7/2025, Nr. 39/2025, Nr. 52/2022, Nr. 35/2012) zu themenverwandten Gesetzesvorhaben verfasst.

How familiar are you with laws and policies related to retention of metadata by service providers for the purpose of preventing, detecting, investigating and prosecuting crimes?")

The BRAK has highly qualified expert committees consisting of legal practitioners and has issued several position papers (no. 7/2025, no. 39/2025, no. 52/2022, no. 35/2012) on related legislative proposals.

Zu Frage 7) Sind Sie der Ansicht, dass Dienstleister zur Gewährleistung der Strafverfolgung Metadaten länger aufbewahren sollten oder dass sie zusätzliche Arten von Metadaten, die für Ermittlungen und/oder Strafverfolgungsmaßnahmen relevant sein könnten, für den spezifischen Zweck der Strafverfolgung aufbewahren sollten?

("Do you consider that, to ensure criminal justice, service providers should retain metadata for longer periods, or that they should retain additional types of metadata that could be relevant for investigations and/or prosecutions, for the specific purpose of law enforcement?")

Antwortauswahl:

- Ja, Anbieter sollten verpflichtet werden, Daten speziell für Strafverfolgungszwecke länger aufzubewahren, als es für geschäftliche Zwecke erforderlich ist. *(„Yes, providers should be obliged to retain data specifically for law enforcement purposes longer than required for business purposes.")*

- ✓ **Nein , Anbieter sollten Daten ausschließlich für geschäftliche Zwecke und nicht länger aufbewahren dürfen. Die Strafverfolgung sollte sich nur auf solche Daten stützen.** *("No, providers should be allowed to retain data exclusively for business. Law enforcement should rely only on such data.")*

- Weiß nicht *(„I don't know")*

Erläuterung der Antwort:

Die BRAK lehnt generelle, anlassunabhängige Mindestspeicherpflichten aufgrund der damit verbundenen Risiken für die Vertraulichkeit von Mandatsverhältnissen sowie weitreichender Grundrechtsbeeinträchtigungen ab. Allenfalls eng begrenzte, anlassbezogene Instrumente mit starken Schutzmaßnahmen zur Wahrung der Persönlichkeits- und Datenschutz-Grundrechte sowie der anwaltlichen Verschwiegenheit kommen in Betracht.

Do you consider that, to ensure criminal justice, service providers should retain metadata for longer periods, or that they should retain additional types of metadata that could be relevant for investigations and/or prosecutions, for the specific purpose of law enforcement?

The BRAK rejects general, untargeted minimum retention obligations due to the associated risks for the confidentiality of lawyer-client relationships and far-reaching infringements of fundamental rights. At most, narrowly defined, targeted instruments with strong protective measures to safeguard fundamental rights of privacy and data protection as well as the lawyer's professional secrecy may be considered.

Zu Frage 8) Derzeit gibt es keine harmonisierten EU-Vorschriften, die Diensteanbieter dazu verpflichten oder dazu anhalten, Metadaten für Strafverfolgungszwecke aufzubewahren. Sehen Sie darin eine Herausforderung?

(„At present, there are no harmonised EU rules obliging or inciting service providers to retain metadata for law enforcement purposes. Do you consider that this brings any challenges?")

Antwortauswahl:

- Ja *(„Yes")*
- ✓ **Nein *(„No")***
- Keine Meinung *(„No opinion")*

***Erläuterung der Antwort*:**

Eine EU-weite Regelung könnte zwar möglicherweise die wirtschaftliche Tätigkeit der (potentiellen) Adressaten von Speicher- und Bereitstellungspflichten erleichtern. Ebenso könnte die Ermittlungstätigkeit dadurch etwas einfacher gestaltet werden. Weder die wirtschaftliche Tätigkeit etwaiger Adressaten noch die Ermittlungsarbeit werden durch derzeit bestehende Unterschiede jedoch derart behindert, dass eine EU-weite Harmonisierung zwingend erschiene. Eine solche müsste die Grund- und Verfassungsrechte achten und die rechtsstaatlich gebotene Vertraulichkeit des Verhältnisses der Bürgerinnen und Bürger zu ihrer Anwältin oder ihrem Anwalt sicherstellen. Dazu gehört auch die Möglichkeit, unerkannt bzw. unüberwacht Kontakt zu einem Anwalt oder einer Anwältin aufnehmen zu können. Eine Harmonisierung, die eine allgemeine EU-weite Speicherpflicht vorsieht, scheidet damit aus. In Betracht käme lediglich ein EU-weites Verbot von Mindestspeicherpflichten.

At present, there are no harmonised EU rules obliging or inciting service providers to retain metadata for law enforcement purposes. Do you consider that this brings any challenges?"

An EU-wide regulation could potentially facilitate the economic activities of (potential) addressees of data retention and provision obligations. It could also make investigative work somewhat easier. However, neither the economic activities of potential addressees nor investigative work are hindered by the current differences to such an extent that EU-wide harmonisation would appear imperative. Such harmonisation would have to respect fundamental and constitutional rights and ensure the confidentiality of the relationship between citizens and their lawyers, as required by the rule of law. This includes the possibility of contacting a lawyer anonymously and without surveillance. Harmonisation that provides

for a general EU-wide retention obligation is therefore out of the question. The only option would be an EU-wide ban on minimum retention obligations.

Zu Frage 9) Sollten Maßnahmen ergriffen werden, um die Kohärenz der Vorschriften zur Vorratsdatenspeicherung in der EU zum Zwecke der Ermittlung und Verfolgung von Straftaten zu verbessern?

(„Should measures be taken to increase coherence of the data retention rules in the EU for the purpose of investigating and prosecuting crimes?)

Antwortauswahl:

- Ja *(„Yes“)*
- ✓ **Nein *(„No“)***
- Keine Meinung *(„No opinion“)*

Erläuterung der Antwort:

Jegliche Harmonisierung müsste die Grund- und Verfassungsrechte achten und die rechtsstaatlich gebotene Vertraulichkeit des Verhältnisses der Bürgerinnen und Bürger zu ihrer Anwältin oder ihrem Anwalt sicherstellen. Dazu gehört auch die Möglichkeit, unerkannt bzw. unüberwacht Kontakt zu einem Anwalt oder einer Anwältin aufzunehmen. Eine Harmonisierung, die eine allgemeine EU-weite Speicherpflicht vorsieht, scheidet damit aus. In Betracht käme lediglich ein EU-weites Verbot von Mindestspeicherpflichten.

Sofern dennoch eine Mindest- oder Höchstspeicherpflicht vorgesehen wird, dürfte dies nur gekoppelt mit starken Garantien erfolgen; namentliche stark zweckgebundene Maßnahmen, strukturelle, nicht nur nachträgliche Aussonderungspflichten von Berufsgruppen, um besonders schützenswerte Informationen wie Mandatskontakte gar nicht erst zu erheben. Es bedarf richterlicher Kontrollen und technischer Garantien gegen Dauerbevorratungen. Zur Vermeidung letzterer sollten wiederholende Anordnungen allenfalls in begrenztem Umfang zulässig sein. Erforderlichenfalls sollten dazu ferner Möglichkeiten, unterschiedliche Ermittlungsbefugnisse zu kombinieren, begrenzt werden.

Should measures be taken to increase coherence of the data retention rules in the EU for the purpose of investigating and prosecuting crimes?

Any harmonisation would have to respect fundamental and constitutional rights and ensure the confidentiality of the relationship between citizens and their lawyers, as required by the rule of law. This also includes the possibility of contacting a lawyer anonymously or without supervision. Harmonisation that provides for a general EU-wide retention obligation is therefore out of the question. The only option would be an EU-wide ban on minimum retention obligations.

If a minimum or maximum retention obligation is nevertheless provided for, this would need to be combined with strong guarantees, namely measures that are strictly purpose-bound, structural, and not merely obligations to separate data of particular professional groups a posteriori, so that particularly sensitive information, such as client contacts, is not collected in the first place. Judicial controls and technical safeguards against permanent retention are required. To avoid the latter, repeated orders

should only be permitted to a limited extent. If necessary, the possibilities for combining different investigative powers should also be limited.

Zu Frage 10) Was versprechen Sie sich von einer EU-Initiative zur Vorratsdatenspeicherung, was auf nationaler Ebene nicht erreicht werden kann?

(„What do you expect to be achieved by an EU initiative on data retention that cannot be achieved at national level?")

- Effektivere strafrechtliche Ermittlungen und Strafverfolgungen *(„More effective criminal investigations and prosecutions"):*

  Antwort: Keine Meinung *(„No opinion")*
- Rechtssicherheit für die beteiligten Akteure *(„Legal certainty for stakeholders involved"):*

  Antwort: Keine Meinung *(„No opinion")*
- Gleiche Verpflichtungen für alle in der EU tätigen Diensteanbieter *(„Same obligations for all service providers operating in the EU"):*

  Antwort: Keine Meinung *(„No opinion")*
- Mehr Transparenz seitens der Diensteanbieter hinsichtlich der von ihnen gespeicherten Daten *(„More transparency from service providers about the data they retain):*

  Antwort: Keine Meinung *(„No opinion")*
- Einfachere Zusammenarbeit zwischen den Mitgliedstaaten *(„Easier cooperation among Member States"):*

  Antwort: Keine Meinung *(„No opinion")*
- Stärkerer Schutz der Grundrechte im Einklang mit der Charta der Grundrechte *(„Stronger protection of fundamental rights in accordance with the Charter of Fundamental Rights"):*

  Antwort: Nein *(„No")*
- Sonstiges *(„Others")*:

  Antwort: Keine Angabe

Erläuterung zu diesen Antworten:

Eine Stärkung des Grundrechtsschutzes dürfte EU-weit allenfalls im Wege eines EU-weiten Speicherverbots zu erreichen sein. Zu erzielende Zugewinne bei der Rechtssicherheit, der grenzüberschreitenden Zusammenarbeit oder einheitlicher Verpflichtungen dürften demgegenüber marginal ausfallen.
Die zu dieser Frage gegebenen Antworten beziehen sich auf die Gegenüberstellung nationaler und europäischer Regelungen und erfolgten im engen vorgegebenen Rahmen der Auswahlmöglichkeiten („Ja", „Nein", „Keine Meinung"). Keinesfalls dürfen diese Antworten dahingehend missverstanden werden, dass die BRAK zur Erreichung eines dieser Ziele eine EU-weite Regelung für geboten erachte. Die zu den anderen Antworten mitgeteilten Vorbehalte und Anforderungen der BRAK gelten auch diesbezüglich uneingeschränkt.

What do you expect to be achieved by an EU initiative on data retention that cannot be achieved at national level?

Strengthening the protection of fundamental rights across the EU is likely to be achieved – if at all - at best by means of an EU-wide ban on retention. In contrast, the gains to be made in terms of legal certainty, cross-border cooperation or uniform obligations are likely to be marginal.
The answers given to this question refer to a comparison of national and European rules and only were provided within the very limited range of possible options ('Yes', "No", 'No opinion'). Under no circumstances should these answers be misunderstood to mean that the BRAK considers EU-wide regulation to be necessary to achieve any of these objectives. The reservations and requirements expressed by the BRAK in relation to the other questions also apply without restriction in this regard.

Zu Frage 11) Welche Bedenken könnte eine EU-Initiative im Bereich der Vorratsdatenspeicherung Ihrer Meinung nach hervorrufen? Wählen Sie die fünf wichtigsten Bedenken aus

(„Which concerns could an EU initiative in the area of data retention raise in your view? Pick the five main concerns")

Antwortauswahl:

- ✓ **Risiko der Offenlegung sensibler Daten gegenüber Behörden** *("Risk of sensitive data being revealed to public authorities (e. g. in calls to medical services or help hotlines)")*
- ✓ **Einschüchterungseffekte auf bestimmte Grundrechte, wie beispielsweise die Meinungsfreiheit.** *("Chilling effects on certain fundamental rights, such as freedom of expression.")*
- ✓ **Risiken der Beeinträchtigung der Privatsphäre der Nutzer** *(„Risks of interference with the privacy of users„)*
- ✓ **Risiko des Missbrauchs der Daten für andere als die ursprünglich vorgesehenen Zwecke** *(„Risk of misuse of the data for other purposes than initially intended")*
- ✓ **Risiko der Speicherung von Daten über einen längeren Zeitraum als für die Aufklärung einer Straftat erforderlich** *(„Risk of retention of data for a longer period of time than necessary to investigate a crime")*
- o Risiko der Speicherung von mehr Daten als für die Ermittlung einer Straftat erforderlich *(„Risk of retention of more data than necessary to investigate a crime")*
- o Risiko einer Fehlinterpretation von Daten *("Risk of misinterpretation of data")*
- o Risiko des Zugriffs auf Daten durch unbefugte Dritte (Datenschutzverletzung) *("Risk of access to data by unauthorised third parties (data breaches)")*
- o Risiken im Zusammenhang mit der Informationssicherheit *(„Information security related risks")*
- o Erhöhte Kosten aufgrund von Speicher-, technischen und organisatorischen Anforderungen *(„Increased costs due to storage and technical and organisational requirements")*
- o Vertrauen der Kunden in die Dienstleistungen *(„Customer's trust in services")*

- Sonstige *(„Other“)*

Erläuterung zu dieser Antwortauswahl:

Anwaltskontakte stellen sensible Daten dar, deren mögliche Offenbarung mit Einschüchterungseffekten einhergehen kann. Bürgerinnen und Bürger könnten aus Furcht vor der Offenbarung ihrer Kontaktaufnahme zu einem Rechtsanwalt oder einer Rechtsanwältin (und einem darin vermeintlich zu erkennenden Schuldeingeständnis) von der Inanspruchnahme rechtlichen Rats bzw. rechtlicher Vertretung abgehalten werden. Das wäre rechtsstaatlich inakzeptabel. Informationen über die Kontaktaufnahme und Korrespondenz zu Kanzleien sind insbesondere vor einem Zugriff staatlicher Stellen, aber auch Dritter, zu schützen.
Jede Datenspeicherung birgt das Risiko eines Missbrauchs. Je umfassender die Datenspeicherung ausfällt, desto größer ist das abstrakte Risiko etwa eines Auslesens durch feindliche und keinen rechtsstaatlichen Regeln unterworfenen Geheimdienste. Die Offenbarung von Mandatskontakten oder anderen sensiblen Verbindungen muss daher bei einer massenhaften Vorratsspeicherung für wahrscheinlich erachtet werden.

Es bestünde nicht nur ein „Risiko“ einer Beeinträchtigung der Rechte der Nutzer. Derartige Beeinträchtigungen würden sich wegen der damit verbundenen Einschüchterungseffekte mit der Einführung von Speicherpflichten vielmehr unmittelbar, sofort und flächendeckend verwirklichen. Es gilt es zu verhindern, dass sich in der Bevölkerung das Gefühl der umfassenden Überwachung ausbreitet.

Sind Daten einmal erhoben, bestehen erfahrungsgemäß Begehrlichkeiten, diese länger und für andere Zwecke zu nutzen. In praktischer Hinsicht ist dies jedenfalls bei unzureichenden technisch-organisatorischen Schutzmaßnahmen und Kontrollen möglich. Ferner steht zu befürchten, dass im Nachgang gesetzlich die Verlängerung der Speicherung oder eine Änderung des Verwendungszwecks ermöglicht wird. Es darf insoweit nicht zu einem „Dammbruch“ kommen.

Dass die übrigen zur Auswahl gestellten Risiken nicht angekreuzt wurden, ist einzig der eingrenzenden Vorgabe („pick five“) geschuldet. Sie bestehen nach Ansicht der BRAK allesamt ebenfalls. Ferner muss darauf hingewiesen werden, dass Antwortmöglichkeiten zu einer Grundrechtsverletzung hinsichtlich der Verschwiegenheit und Verfahrensrechten fehlen.

Which concerns could an EU initiative in the area of data retention raise in your view? Pick the five main concerns

Lawyer contacts constitute sensitive data, the disclosure of which could have chilling effects. Citizens could be deterred from seeking legal advice or representation for fear that their contact with a lawyer (and the supposed admission of guilt that this implies) will be disclosed. This would be unacceptable under the rule of law. Information about contacts and correspondence with law firms must be protected, particularly from access by government agencies, but also by third parties.

Any data retention carries the risk of abuse. The more comprehensive the data retention, the greater the abstract risk of, for example, hostile secret services that are not subject to the rule of law reading the data. The disclosure of client contacts or other sensitive connections must therefore be considered likely in the case of mass data retention.

There would not only be a ‘risk’ of infringing on the rights of users. Rather, such infringements would become immediate, instantaneous and widespread due to the associated chilling effects of the introduction of retention obligations. It is important to prevent a feeling of comprehensive surveillance

among the general population. Once data has been collected, our experience shows that there is a tendency to want to use it for longer and for other purposes. In practical terms, this is certainly possible where technical and organisational protective measures and controls are inadequate. There is also a risk that the law will subsequently permit to extend the retention period or to change the purpose it is used for. In this respect, there must be no 'breach of the dam'.
The fact that we did not tick the other risks listed for selection is solely due to the fact that our options were restricted ('pick five'). In the opinion of the BRAK, they all exist as well. Furthermore, it should be noted that there are no response options for a violation of fundamental rights with regard to confidentiality and procedural rights.

Zu Frage 12) Welche Ermittlungsmethode, die einer vorherigen Genehmigung durch einen Richter oder eine unabhängige Verwaltungsbehörde bedarf, würden Sie als eingreifender betrachten? Bitte listen Sie die Optionen in der Reihenfolge ihrer Priorität auf.

("Which investigative method requiring prior authorisation by a judge or independent administrative authority would you consider more intrusive? Please list the options in order of priority")

Antwort:

Priorisierung wie folgt:

1. Zugriff auf Metadaten eines Kommunikationsdienstes, die vom Dienstanbieter für alle Nutzer gespeichert werden *(„Accessing metadata of a communication service stored by the service provider for all users")*

2. Live-Überwachung der Kommunikation bestimmter Nutzer *(„Live interception of communications of targeted users")*

3. Extrahieren von Daten aus beschlagnahmten Geräten wie Mobiltelefonen oder Laptops von Verdächtigen *(„Extraction of data from seized devices such as mobile phones or laptops of suspects")*

4. Verdeckte und/oder undercover Überwachungsmaßnahmen gegen Verdächtige *(„Covert and/or undercover surveillance measures of suspects")*

5. Hausdurchsuchung von Verdächtigen *(„House search of suspects")*

Erläuterung zu dieser Priorisierung:

Breit angelegte Metadatenzugriffe sind aufgrund ihrer großflächigen Erfassung Unbeteiligter und sensibler Informationen besonders eingriffsintensiv. Die anderen genannten Maßnahmen können im jeweiligen Einzelfall jedoch schwerer wiegen.

Which investigative method requiring prior authorisation by a judge or independent administrative authority would you consider more intrusive? Please list the options in order of priority"

Large scale metadata access is particularly intrusive due to its widespread collection of data pertaining to persons that are not involved and the access to sensitive information. However, the other measures mentioned may carry greater weight in individual cases.

Zu Frage 13) Gibt es Ihrer Meinung nach Maßnahmen, die weniger eingreifend sind und dennoch eine wirksame Ermittlung und Verfolgung von Straftaten ermöglichen?

(„In your opinion, are there measures which would be less intrusive and still allow for the effective investigation and prosecution of crimes?")

Antwort:

- ✓ **Ja *(„Yes")***
- Nein *(„No")*
- Keine Meinung *(„No opinion")*

Erläuterung dieser Antwort:

Wirksam und weniger eingreifend – aber ebenfalls nicht unproblematisch – wäre eine anlassbezogene Speicher-Anordnung (sog. Quick-Freeze). Auch insoweit wären jedoch ein begrenzter Anwendungsbereich und flankierende Schutzmaßnahmen essentiell. Problematisch wäre aber auch hier, dass Mandatskontakte praktisch kaum ohne deren vorherige Offenbarung ausgesondert werden könnte. Möglich ist allein eine Untersagung der Erhebung, also Speicherung bestimmter Daten. Daher steht die Bundesrechtsanwaltskammer auch diesem Ansatz kritisch gegenüber (vgl. BRAK-Stellungnahmen 7/2025 und 52/2022).

In your opinion, are there measures which would be less intrusive and still allow for the effective in-vestigation and prosecution of crimes?
A targeted retention order (known as a quick freeze) would be effective and less intrusive, but it would also be problematic. In this respect, too, a limited scope of application and accompanying protective measures would be essential. Another problem here is that it will practically be impossible to select contacts without first disclosing them. The only option would be to prohibit the collection, i.e. retention, of certain data. The German Federal Bar is therefore also critical of this approach (cf. BRAK position papers no. 7/2025 and no. 52/2022).

Zu Frage 14) Ihrer Meinung nach, für welche der folgenden Dienstleister sollten EU-Maßnahmen zur Vorratsdatenspeicherung gelten?

(*„In your opinion, to which of the following service providers should EU measures on retention of metadata be applicable?")*

Antworten:

- Anbieter elektronischer Kommunikationsdienste (die traditionelle Sprachtelefonie/Sprachkommunikationsdienste und Textnachrichten/SMS anbieten)
  („Electronic communications service providers (offering traditional voice telephony/voice communications services and text messages/SMS)")

Antwort: **Nein**

- Anbieter, die nummernuabhängige Dienste für die zwischenmenschliche Kommunikation anbieten (z. B. VoIP, Messaging, Videokonferenzen, E-Mail)
  („Providers offering number-independent interpersonal communications services (e.g., VoIP, messaging, video conferencing, electronic mail) services“)
  Nein

- Internet-Zugangsdienstanbieter
  („Internet Access Service Providers“)
  Nein

- Anbieter von Diensten, die ganz oder überwiegend aus der Übertragung von Signalen bestehen (z. B. Machine-to-Machine-Kommunikation (M2M) und Rundfunksignale)
  („Providers of services consisting wholly or mainly of the conveyance of signals (such as Machine-to-Machine (M2M) communications and broadcasting signals)“)
  Nein

- Anbieter von Social-Media-Plattformen
  („Providers of social media platforms“)
  Nein

- Cloud-Dienste
  („Cloud services“)
  Nein

- Digitale Marktplätze
  („Digital marketplaces“)
  Nein

- Anbieter von Internet-Infrastrukturdiensten (wie IP-Adressen und DomainnamenRegistrierungsstellen und -Registrare)
  (“Providers of internet infrastructure services (such as IP addresses and domain name registries and registrars)”)
  Nein

- Anbieter von Webhosting-Diensten
  („Web hosting service providers“)
  Nein

- Zukünftige und neu entstehende Technologien
  („Future and emerging technologies“)
  Nein

- Sonstiges
  (“Other”)
  Nein

Erläuterung der Antwort:

Die Antwort gilt unter der Annahme, dass Mindestspeicherpflichten eingeführt werden sollen – welche die BRAK ablehnt. Gegen ein EU-weites Verbot von Speicherpflichten, das für alle Anbietergruppen gleichermaßen gilt, wäre demgegenüber nichts einzuwenden.
Sollten Mindestspeicherpflichten ungeachtet der genannten Bedenken eingeführt werden, sollten diese auf klassische Telekommunikations-Anbieter und nummerngebundene Dienste beschränkt werden. Eine Erweiterung auf Cloud- bzw. Social-Media-Plattformen oder Messenger würde eine erhebliche Ausweitung der betroffenen Lebens- und Grundrechtsbereiche bedeuten. Sie bedürfte jedenfalls einer gesonderten Rechtfertigung und dürfte allenfalls bei (noch) strengerer technischer Notwendigkeit und in begrenztem Umfang erfolgen. Angesichts der Fülle der in Cloud-, Social-Media- und Messenger-Diensten anfallenden Daten müsste in diesem Fall besonders sorgfältig darauf geachtet werden, dass die Speicher- und Herausgabepflichten strikt auf die für erforderlich erachteten Daten begrenzt werden. Zudem wäre eine differenzierte Betrachtung der jeweiligen (typischen) Nutzergruppen und Inhalte sowie der damit einhergehenden Risiken und Schutzbedarfe erforderlich. Ein Einbezug künftiger oder neu entstehender Technologien verbietet sich, da insoweit die jedenfalls erforderlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit mangels Kenntnis der jeweiligen Technologie nicht möglich sind.

In your opinion, to which of the following service providers should EU measures on retention of metadata be applicable?

The answer is based on the assumption that minimum retention obligations are to be introduced – which the BRAK rejects. On the other hand, there would be no objection to an EU-wide ban on retention obligations that applies equally to all provider groups. If minimum retention obligations were introduced despite the concerns mentioned above, they should be limited to traditional telecommunications providers and number-based services. Extending them to cloud and social media platforms or messengers would mean a significant expansion of the areas of life and fundamental rights that would be affected. In any case, it would require separate justification and should only be implemented if there is an (even) stricter technical necessity and to a limited extent. Given the wealth of data generated by cloud, social media and messenger services, particular care would have to be taken in this case to ensure that the retention and disclosure obligations are strictly limited to the data deemed necessary. In addition, a differentiated consideration of the respective (typical) user groups and content, as well as the associated risks and protection requirements, would be necessary. Including future or newly emerging technologies is not permitted, as the necessary considerations regarding necessity and proportionality are not possible in this respect due to a lack of knowledge of the respective technology.

Zu Frage 15) Für welche Art von Straftaten sollte die Verpflichtung zur Vorratsspeicherung von Daten vorgesehen werden?
(*„In your view, to investigate which types of crimes should the obligation to retain data be required?“*)

Antwortauswahl:

- Nur für schwere Straftaten (wie Terrorismus, Menschenhandel und sexuelle Ausbeutung von Frauen und Kindern, illegaler Drogenhandel, illegaler Waffenhandel, Geldwäsche, Korruption, Fälschung von Zahlungsmitteln, Computerkriminalität und organisierte Kriminalität) - *(„Only for serious crimes (such as terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime)“)*

- Für allgemeine Straftaten (wie Diebstahl, Raub, Kleinkriminalität, Verstöße gegen das Recht des geistigen Eigentums usw.)
  („For general crimes (such as thefts, robberies, petty crimes, infringements of intellectual property, etc)")

- Für alle Arten von Straftaten - *("For all types of crimes")*

- ✓ **Keine - („None")**

- Ich weiß nicht - *(„I don't know)*

Erläuterung zu dieser Auswahl:

Wegen der damit einhergehenden Grundrechtsbeeinträchtigungen und Risiken sollte eine verpflichtende Vorratsdatenspeicherung überhaupt nicht vorgesehen werden. Falls dies doch erfolgen sollte, müsste eine solche Pflicht auf schwerste Straftaten begrenzt bleiben, wie es in Deutschland jüngst das Bundesverfassungsgericht hinsichtlich der Quellentelekommunikationsüberwachung (sog. Staatstrojaner) entschieden hat (BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 180/23).

Problematisch wäre dabei in praktischer Hinsicht, dass bei einer allgemeinen Speicherpflicht kaum zwischen verschiedenen Graden der Strafbarkeit unterschieden werden könnte, sondern vielmehr sogar überwiegend Unbeteiligte betroffen wären. Sofern eine Differenzierung nach unterschiedlichen Arten von Straftaten angestrebt wird, darf dies nicht zu einer Inhaltsüberwachung durch die Hintertür führen, bei der der Zugriff auf Kommunikationsinhalte oder weitergehende Teilnehmerdaten mit der Zielrichtung erlaubt wird, diese einer Kategorie von Straftaten zuzuordnen.

In your view, to investigate which types of crimes should the obligation to retain data be required?
Due to the infringements of fundamental rights and risks that come with such measures, mandatory data retention should not be envisaged at all. If this were to happen, such an obligation would have to be limited to the most serious crimes, as the Federal Constitutional Court recently ruled in Germany with regard to source telecommunications surveillance (so-called 'state Trojans') (BVerfG, decision of 24 June 2025 – 1 BvR 180/23).
The practical problem here would be that a general retention obligation would make it almost impossible to distinguish between different degrees of punishability, and would instead affect predominantly uninvolved parties. If the aim is to differentiate between different types of criminal offences, this must not lead to content monitoring through the back door, where access to communication content or further-reaching subscriber data is permitted with the aim of assigning it to a certain category of criminal offences.

Zu Frage 16) Sollten Ihrer Meinung nach die Anforderungen an die Vorratsdatenspeicherung (z. B. die Dauer der Speicherung) je nach Art der Daten und Zweck der Ermittlung unterschiedlich sein?

("In your view, should data retention requirements differ (for example the duration of the retention) depending on the type of data and the purpose of the investigation?")

Antwort:

- ✓ **Ja *(„Yes“)***
- ○ Nein *(„No“)*
- ○ Keine Meinung *(„No opinion“)*

Erläuterung der Antwort:

Sofern Speicherfristen vorgesehen werden, gebieten die europa- und verfassungsrechtlichen Prinzipien der Erforderlichkeit bzw. der Verhältnismäßigkeit differenzierte Regelungen. Diese müssen unter anderem den unterschiedlichen Zwecken der Speicherung sowie den jeweiligen Daten- und Betroffenenkategorien Rechnung tragen. Demgegenüber wäre eine generelle einheitliche Speicherpflicht mit rechtsstaatlichen Prinzipien unvereinbar.

In your view, should data retention requirements differ (for example the duration of the retention) de-pending on the type of data and the purpose of the investigation?

Where retention periods are provided for, the principles of necessity and proportionality under European and constitutional law require differentiated regulations. These must take into account, among other things, the different purposes of retention and the respective categories of data and data subjects. By contrast, a general uniform retention obligation would be incompatible with the principles of the rule of law.

****