ÖRAK-Stellungnahme anlässlich der öffentlichen Konsultation der Europäischen Kommission zu einer EU-Initiative zur Vorratsdatenspeicherung durch Diensteanbieter für Strafverfahren

Der Österreichische Rechtsanwaltskammertag (ÖRAK) ist die gesetzlich eingerichtete Vertretung der Rechtsanwälte in Österreich und als solche zur Wahrung der Rechte und Angelegenheiten sowie zur Vertretung der österreichischen Rechtsanwälte auf nationaler, europäischer und internationaler Ebene berufen. Als solcher obliegen ihm besonders die Erstattung von Gesetzesvorschlägen und Stellungnahmen zu Gesetzesentwürfen sowie die Anzeige von Mängeln der Rechtspflege und Verwaltung bei der zuständigen Stelle und die Erstattung von Vorschlägen zur Verbesserung von Rechtspflege und Verwaltung.

I. Einleitung

Der ÖRAK versteht, dass die Auswertung von Daten von Dienstleistungsanbietern entscheidend für die Strafverfolgung sein kann und sieht auch ein Spannungsfeld im Falle der verfrühten Löschung von – ggf sogar entlastenden – Daten.

Grundsätzlich sieht der ÖRAK allerdings den **Aufbau und Inhalt des Konsultationsfragebogens** zu einer EU-Initiative zur Vorratsdatenspeicherung durch Diensteanbieter für Strafverfahren kritisch. Dieser ist nicht neutral formuliert und lässt in großem Umfang lediglich bestimmte Antworten zu. Aus Sicht des ÖRAK wird der Konsultationsfragebogen daher den Ansprüchen der Europäischen Kommission zur sog besseren Rechtsetzung insbesondere im Hinblick auf die

Beteiligung von Interessenvertretern, einschließlich der Zivilgesellschaft, und Folgenabschätzungen, nicht gerecht.

Der ÖRAK kann den Konsultationsfragebogen daher nicht ausfüllen und erstattet stattdessen die vorliegende Stellungnahme.

II. Anmerkungen zu den Konsultationsfragen

1. Regelungsmaterien einer möglichen Gesetzgebungsmaßnahme

Zu bemerken ist zunächst, dass ausweislich der Konsultationsfragen grundsätzlich **zwei Regelungsmaterien zu unterscheiden** sind: die **Vorratsdatenspeicherung** von Daten auf Seiten von Anbietern und der **Zugang** zu den gespeicherten Daten durch Strafverfolgungsbehörden. Die Fragen vermischen diese beiden Materien teilweise.

2. Falsche allgemeine Annahme, dass Zugang zu Metadaten nicht intensiver Eingriff

Die Konsultation scheint ausweislich der Fragestellungen in der Konsultation davon auszugehen, dass das Speichern von und der Zugriff auf **Metadaten allgemein einen nicht intensiven Eingriff** in die Grundrechte bedeuten, insbesondere im Vergleich zu sog content data (sog Inhaltsdaten). Dies entspricht nicht dem Stand der Diskussionen zu Datensicherheit und Privacy. Richtig ist, dass Metadaten wie in der Konsultation genannt zB Nutzer-/Teilnehmerinformationen bzw IP-Daten, Sende-/Empfangsdaten einer Nachricht, Standort eines Geräts, Datum, Uhrzeit, Dauer, Größe einer Nachricht oder andere Interaktionsarten, aus denen der Inhalt der Kommunikation nicht hervorgeht beinhalten. Allerdings handelt es sich nicht um „Kommunikationsdaten, die nicht den Inhalt einer Kommunikation betreffen", da **Metadaten eben genau auf den Inhalt einer Kommunikation oder andere sensible**

Daten schließen lassen können.[1] Auch Metadaten sind geschützte Daten; die Intensität des Eingriffs ihrer Speicherung und/oder Nutzung lässt sich nicht allgemein-abstrakt, sondern nur individuell-konkret unter Zugrundelegung eines konkreten Sachverhalts- und Regelungskontexts bestimmen.

Beispiele:

- **Standortdaten** bei einer Rechtsanwaltskanzlei bedeuten wohl eine Konsultation eines Rechtsanwalts oder einer Rechtsanwältin – dabei ist bereits die **Identität von Mandantinnen und Mandanten in Österreich vom Verschwiegenheitsgebot gedeckt**. Dasselbe gilt für übereinstimmende Daten von Mandanten und Rechtsanwältinnen oder Rechtsanwälten bei Treffen außerhalb der Büroräume; **genauso: übereinstimmende Verbindungsdaten bei Telekommunikation**.
- **Tätigkeitsschwerpunkte der genannten Berufsträger können den Anlass des Kontakts vermuten lassen,** dieser wird allerdings erst recht durch ein Verschwiegenheitsgebot geschützt.
- **Gewohnheitsabbildungen** durch einzelne oder Zusammenschau von Daten, die **höchstpersönliche Informationen** über das Familienleben, die sexuelle Orientierung, Abhängigkeit von Drogen etc, sichtbar machen.

[1] Auch die Recommendations der High Level Group on Access to Data for Effective Law Enforcement sowie deren Abschlussbericht, die von der Kommission in ihrer Roadmap aufgenommen worden sind, deuten an, dass sich sehr weitgehende Erkenntnisse erhofft werden.

3. Bedenken im Hinblick auf Regelungen zur Vorratsdatenspeicherung einschließlich Abrufmöglichkeiten für Strafverfolgungsbehörden

Die Konsultation fragt nach Bedenken im Hinblick auf eine geplante Regelung zur Vorratsdatenspeicherung und gibt dabei auch richtig folgende Bedenken *im Fragebogen* an:

- *Beeinträchtigung bestimmter Grundrechte wie des Rechts auf freie Meinungsäußerung,*
- *Risiko, dass mehr Daten aufbewahrt werden als für die Ermittlung einer Straftat erforderlich,*
- *Risiko, dass Daten über einen längeren Zeitraum gespeichert werden als für die Ermittlung einer Straftat erforderlich,*
- *Risiko der Offenlegung sensibler Daten gegenüber Behörden (z. B. im Fall von Anrufen bei medizinischen Diensten oder Hotlines),*
- *Risiko, dass Daten fehlinterpretiert werden,*
- *Risiko, dass unbefugte Dritte auf Daten zugreifen (Datenschutzverletzungen),*
- *Risiko des Missbrauchs der Daten für andere als die ursprünglich vorgesehenen Zwecke,*
- *Risiko eines Eingriffs in die Privatsphäre der Nutzer*innen,*
- *Risiken im Zusammenhang mit der Informationssicherheit,*
- *Höhere Kosten im Zusammenhang mit der Datenspeicherung sowie technischen und organisatorischen Anforderungen,*
- *Vertrauen der Kund*innen in die Dienste.*

Die Kommission bittet sodann um **Auswahl der fünf wichtigsten Bedenken, was zwangsweise zu einer Verzerrung der Antworten der Interessenträger führen wird**. Im Umkehrschluss werden dann automatisch valable Bedenken als nicht so wichtig ausgewertet, was falsch ist.

Die Vorratsdatenspeicherung geht mit komplexen grundrechtlichen und gesellschaftlichen Fragestellungen herein, die alle einer Diskussion und Beantwortung bedürfen. Fast alle der genannten Bedenken gehen auch mit Verletzungen von grundrechtlich geschützten Gütern überein, sodass eine Listung von fünf Bereichen (und Nichtlistung der anderen) die schlicht rechtlich erforderliche Einhaltung von Grundrechten bzw die vorgeschriebene rechtliche Rechtfertigung von Eingriffen dem Eindruck nach negieren.

4. „Abstimmung" zu Grundrechtseingriffen im Rahmen einer Konsultation wirft Fragen auf

Die Kommission fragt weiters in ihrer Konsultation „**welche Ermittlungsmethode**, für die die vorherige Anordnung eines Gerichts oder einer unabhängigen Verwaltungsbehörde erforderlich ist, **würde Ihrer Ansicht nach stärker in die Privatsphäre eingreifen**?"

Mögliche Antworten *ausweislich des Fragebogens* sind:

- *Zugriff auf Metadaten aller Nutzer*innen eines Kommunikationsdienstes, die vom Diensteanbieter gespeichert werden,*
- *Live-Überwachung der Kommunikation von Zielpersonen,*
- *Hausdurchsuchungen bei Verdächtigen,*
- *Extraktion von Daten aus beschlagnahmten Geräten wie Mobiltelefonen oder Laptops von Verdächtigen,*
- *Maßnahmen zur verdeckten Überwachung von Verdächtigen.*

Die angegebenen Antworten sind so zugeschnitten, dass der Zugriff auf Metadaten wohl am wenigsten eingriffsintensiv erscheint, denn wer möchte schon live überwacht werden oder sich eine Hausdurchsuchung vorstellen. Dasselbe gilt wohl auch für den Zugriff auf alle Daten eines digitalen Geräts, dh sowohl Meta- als auch Inhaltsdaten.

Der Frage fehlt allerdings der Kontext, diese ist daher sehr verzerrend und auch unrichtig.

Beispiel:

Ein Schüler kommt aus einem sogenannten Problemviertel, in dem ua Drogenkriminalität eine Rolle spielt. Der Schüler ist 15 Jahre alt und begeht keinerlei Straftaten.

In seiner Klasse sind verschiedene Jugendliche, die Drogen verkaufen, mit diesen spielt er auch Fußball an den Wochenenden. Ein Sportverein besteht nicht, man spricht sich über Handy ab.

Der Schulweg des Schülers geht durch einen Bereich, in dem Drogen verkauft werden. Der Fußballplatz ist dank einer engagierten Sozialarbeiterin drogenfreies Gebiet.

Eine Live-Überwachung der verfolgten Drogendeals, dh verdächtiger Personen, hätte nichts ergeben im Hinblick auf den Schüler. Eine Analyse der Metadaten seiner Freunde – auf Vorrat gespeichert durch den Anbieter und an die Ermittlungsbehörden übergeben - hat ihn aber direkt als potenziellen Verdächtigen identifiziert (eingeloggt im Bereich der Drogengeschäfte, Chatkontakte mit jugendlichen Drogendealern).

Noch ein Schritt weiter: Der Schüler hat nun ein Date in einem Café. Die Polizei führt eine Razzia in diesem durch. Alle Betroffenen schmeißen ihre Drogen auf den Boden, einiges liegt unter dem Stuhl des Schülers.

Analyse des Beispiels:

In dieser Situation kann ein potenzielles Misstrauen der Ermittlungsbehörden gegen den Schüler befürchtet werden, denn er ist ja „bekannt" in den Ermittlungen. Ein Verstoß gegen die Unschuldsvermutung ist möglich. Natürlich kann auch zur Entlastung ermittelt werden, die Situation stellt sich für den Schüler aber zunächst schwierig dar. Sein völlig legales und gesellschaftlich gewünschtes Verhalten, dh Schule, Sport, normales Freizeitverhalten, hat ihn alleine aufgrund seiner Wohn- und Lebenssituation auf dem Radar der Polizei als möglichen Drogendealer erscheinen lassen.

Bei einer Live-Überwachung der Drogengeschäfte, Übergaben etc wäre der Name des Schülers nicht in Ermittlungsakten aufgetaucht und er müsste sich nun keine Sorgen machen, dass bereits ein Vorverdacht gegen ihn besteht.
Das Beispiel zeigt, dass **eine Verhältnismäßigkeitsprüfung einer Maßnahme, insbesondere die Frage nach einem milderen Mittel niemals im Allgemeinen beantwortet werden kann** – anders als die Frage in der Konsultation zu unterstellen scheint. Es ist nicht auszuschließen, dass aufgrund anderer Umstände eine Abfrage von Metadaten gerechtfertigt gewesen und tatsächlich das mildere Mittel dargestellt hätte. Solche Umstände sind aber im Einzelfall genau zu ermitteln und zu prüfen, **eine schematische Betrachtungsweise zur Eingriffsintensität ist faktisch und rechtlich falsch**.

Im Ergebnis liefert die Fragestellung der Konsultation kein geeignetes Substrat für eine Grundrechtsprüfung. Vielmehr wäre es notwendig, ein konkretes Regelungsvorhaben in den Blick zu nehmen, das insgesamt auf seine Verhältnismäßigkeit beurteilt werden kann (wobei dafür zudem in der Regel auch eine fachliche Grundlage notwendig ist). Die hier gewählte fragmentarische Art der Fragestellung verleitet zu grundrechtsdogmatisch unzulässigen Verallgemeinerungen.

5. Maßstab des geringeren, gleich wirksamen Eingriffs

Weiters stellt die Kommission die Frage, ob es „Maßnahmen [gebe], die weniger in die Privatsphäre eingreifen und trotzdem eine wirksame Ermittlung und Verfolgung von Straftaten ermöglichen würden?". Diese allgemeine Frage ist im Hinblick auf die zuvor geäußerten Hinweise zur Notwendigkeit einer individuellen Abwägung irreführend. Es ist auch anzumerken, dass die **Tatsache, dass kein milderes Mittel denkbar ist** (bezüglich einer *konkreten* Regelung, nicht allgemein, siehe Ausführungen zuvor) **zwar deren Erforderlichkeit iSd Verhältnismäßigkeit stützt, dies bedeutet aber nicht, dass ein Eingriff im Sinne der Verhältnismäßigkeitsprüfung des EuGH dadurch gerechtfertigt ist**.

Ein Eingriff in ein Grundrecht ist nur gerechtfertigt und damit rechtmäßig, wenn es sich nicht um ein absolutes Recht handelt und dieser verhältnismäßig erfolgt. Die Verhältnismäßigkeitsprüfung beinhaltet ua auch die Frage nach einer Angemessenheit von Maßnahmen, die unabhängig von der Frage nach einem möglichen milderen Mittel zu beantworten ist. Auch die Eingriffe in Grundrechte anderer als des Adressaten – was bei einer Vorratsdatenspeicherung – ja zwangsläufig der Fall ist und bei Herausgabe von Daten fast immer der Fall sein wird, sind zu berücksichtigen.

Im Ergebnis liefert die Fragestellung der Konsultation auch hier kein geeignetes Substrat für eine Grundrechtsprüfung. Ohne ein konkretes Regelungsvorhaben verleitet die fragmentarische Fragestellung zu unrichtigen Verallgemeinerungen, siehe hierzu auch unter II. 4..

III. Weitere Analysepunkte zu möglichen Regelungen

1. Eingriff in Grundrechte nicht verdächtiger Bürgerinnen und Bürger

Zu unterstreichen ist, dass eine Vorratsdatenspeicherung auf alltägliche Kommunikationsmittel und sonstige digitale Tools zielt. Fast alle Nutzerinnen und Nutzer derselben stehen in keinerlei Verdacht, eine Straftat begangen zu haben.

Gleichzeitig befindet sich die Gesellschaft in einem Zeitalter zunehmender Digitalisierung, sodass Menschen und Unternehmen auf diese Technologien angewiesen sind bzw keine anderen, nicht Daten produzierenden Produkte zur Verfügung stehen.

2. Eingriff in Grundrechte von verdächtigen Personen

Auch ein Eingriff in zB das Grundrecht auf Privatsphäre einer verdächtigen Person ist nicht automatisch gerechtfertigt und damit rechtmäßig. Hier ist zum einen der Umfang der Datenspeicherung zu begrenzen, insbesondere bzgl sensibler Daten wie des rechtsanwaltlichen Verschwiegenheitsgebots, siehe unter II.3., und zum anderen ist die Möglichkeit des Abrufens verschiedener Datenkategorien und -mengen klar zu definieren. Auch *fishing expeditions* sind aus rechtstaatlichen Gründen abzulehnen.

Zusammengefasst heißt das, bestimmte Daten dürfen aus grundrechtlichen Erwägungen bereits nicht gespeichert, andere zwar gespeichert, aber nicht unbegrenzt abgerufen werden.

3. Gefährdung von Grundrechten, einschließlich des Justizgrundrechts auf rechtsanwaltliche Verschwiegenheit

Aus Sicht des ÖRAK ist insbesondere die mit dem Vorschlag einhergehende **ständige Möglichkeit der Verletzung des rechtsanwaltlichen Verschwiegenheitsgebots** und damit eines **rechtsstaatlichen Grundprinzips besorgniserregend**.
Die Geltung des rechtsanwaltlichen Verschwiegenheitsgebots ist für viele Mandantinnen und Mandanten eine **Grundvoraussetzung für die Inanspruchnahme rechtsanwaltlicher Beratung und damit auch für den Zugang zum**

Recht.[2] Es besteht keine Technologie, die derzeit oder in Zukunft vom Verschwiegenheitsgebot geschützte Daten von anderen unterscheiden könnte.
Es ist richtig, dass Eingriffe in Grundrechte unter bestimmten Voraussetzungen zulässig sind. **Artikel 8 EMRK, der das rechtsanwaltliche Verschwiegenheitsgebot nach ständiger Rechtsprechung[3] streng schützt**, legt dazu etwa fest, dass eine Behörde in dieses Recht eingreifen darf, wenn der Eingriff gesetzlich vorgesehen und 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. Ein Eingriff hat daher nicht nur einem bestimmten, definierten Zweck zu diesen, der unter eine der angeführten Ziele zu subsumieren ist, er hat auch das Verhältnismäßigkeitsgebot zu wahren. Diese Kriterien gelten im Wesentlichen für jeden Eingriff in die nachstehenden Grundrechte, soweit diese nicht ohnedies schrankenlos garantiert werden.
Nach Auffassung des ÖRAK gefährden Vorratsdatenspeicherung und mögliche Herausgaben der Daten an Ermittlungsbehörden kumulativ ua folgende **Grundrechte:**

- 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), 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),
- Freiheit der Meinungsäußerung und Informationsfreiheit (Art 11 GRC)

[2] Vorsorglich ist klarzustellen, dass eine Berufung auf das Verschwiegenheitsgebot nie möglich ist, wenn ein Rechtsanwalt oder eine Rechtsanwältin selber in kriminelle Aktivitäten involviert sind.

[3] Siehe ua Factsheet EGMR, abrufbar hier: https://www.echr.coe.int/documents/d/echr/fs_legal_professional_privilege_eng .

Es ist anzumerken, dass auch andere Berufe Verschwiegenheitspflichten unterliegen, die grundrechtlich geschützt sind, so Ärztinnen und Ärzte sowie Journalisten (siehe hierzu Art. 11 Abs. 2 GRC, Freiheit der Medien, unter dem Gesichtspunkt des Quellenschutzes).

Vor diesem Hintergrund ist eine Vorratsdatenspeicherung – wenn überhaupt – nur dann zulässig, wenn vielfältige Differenzierungen insbesondere nach Art der gespeicherten Datenkategorien sowie nach den Anlässen und der Reichweite von Abfragebefugnissen erfolgen, Ausnahmen für besonders sensible Bereiche geschaffen werden (wie insbesondere die Wahrung der rechtsanwaltlichen Verschwiegenheit) und effektive Maßnahmen zum Schutz vor Missbrauch einschließlich effektiver Rechtsschutzgarantien das Regelungssystem komplettieren.

4. Risiko von falschen Verdächtigungen

Nach Auffassung des ÖRAK ist das Risiko falscher Verdächtigungen heute noch höher als zur Zeit der ersten Diskussionen um Vorratsdatenspeicherung. Durch Digitalisierung und vor allem die Nutzung von Smartphones werden schier unendlich viele Daten erzeugt. Der klassische Sozialraum scheint sich ins Digitale zu verlagern, so zB Absprachen unter Eltern, im Sportverein, unter Nachbarn, Arbeitskollegen, Absprachen von handwerklichen Leistungen, Reservierungen, Unterstützung im sozialen Bereich und Selbsthilfegruppen, Kleinanzeigen etc etc. Diese Verbindungen können zu vielen falsch-positiv verdächtigen Metadaten führen.

Aus statistischer Sicht ist zu erwarten, dass sich die Anzahl falsch-positive Treffer besonders an Orten mit erhöhter Kriminalität ebenfalls erhöht, was spezifische soziale und diskriminierende Folgen haben kann.

Falsch-positiv verdächtige Metadaten können mit negativen Konsequenzen für Betroffene einhergehen. Neben den direkten Belastungen für eine hiervon betroffene Person kann auch das familiäre und gesellschaftliche Leben nachhaltig geschädigt werden.

Es bedarf daher auch effektiver technischer und rechtlicher Maßnahmen zum Schutz vor jeglicher Form eines ‚Bias'. Zu betonen ist zudem, dass eine Abfrage und Nutzung von Vorratsdaten ohnehin immer nur anlassbezogen bei schwerer Kriminalität (siehe EuGH 30.4.2024, Rs C-470/21, Rn 95) durch die Strafverfolgungsbehörden erfolgen dürfte und diese aus rechtsstaatlichen Notwendigkeiten die volle Verantwortung dafür zu tragen haben. Ein allgemeines ‚Ausforschen' möglicher Verdachtslagen (vielleicht sogar durch eine KI) wäre nicht grundrechtskonform; ebenso wenig, wenn die Letztverantwortung nicht auf eine/n konkrete/n Organwalter/in zurückgeführt werden könnte.

5. Gefahr der Absenkung von Schutzstandards für Rechtssuchende

Der ÖRAK weist daraufhin, dass es bei Situationen zu Datenspeicherung oft zu grenzüberschreitenden Sachverhalten mit mehreren Mitgliedstaaten oder sogar Drittstaaten kommt.

Es wird eine große Herausforderung des angedachten Rechtsrahmens, dass es in diesen Situationen zu keiner Absenkung der bisherigen rechtlichen Schutzstandards, insbesondere im grundrechtlichen Bereich kommt.

Im Hinblick auf das rechtsanwaltliche Verschwiegenheitsgebot ist darauf hinzuweisen, dass dieses national eingepasst ist in die jeweilige Rechtstradition. Vorsichtshalber ist darauf hinzuweisen, dass die **sog E-Evidence-Verordnung hier <u>kein</u> geeignetes Modell** ist sobald mehr als zwei Mitgliedstaaten betroffen sind. Wenn massenhaft geschützte Daten von zB einem Anbieter von Kanzleisoftware in einem Mitgliedstaat A in einem zweiten Mitgliedstaat B gespeichert werden und sodann Behörden aus Mitgliedstaat C , D, E, … Daten abfragen können, ist **absolut unerlässlich, dass die Daten, die aus Mitgliedstaat A stammen auch entsprechend dem Erwartungshorizont der Rechtssuchenden durch das Verschwiegenheitsgebot des Mitgliedstaats A geschützt sind.**

Im Angesicht der obigen Ausführungen fordert der ÖRAK die Europäische Kommission nachdrücklich dazu auf, sich für den Schutz der Grund- und Freiheitsrechte, sowie insbesondere des Mandatsgeheimnisses einzusetzen und rechtsstaatliche Grundwerte bereits in der Vorbereitung einer eventuellen Gesetzgebung zur Vorratsdatenspeicherung zu beachten.

Wien, am 11. September 2025

Der Österreichische Rechtsanwaltskammertag