



Ausschussdrucksache 21(6)122e
vom 5. Oktober 2026, 17:18 Uhr

Schriftliche Stellungnahme
des Sachverständigen Jürgen Bering

Öffentliche Anhörung

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und
Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren
BT-Drucksachen 21/6581, 21/7154



5. Oktober 2025

Stellungnahme

zum Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren

für die öffentliche Anhörung im Rechtsausschuss des Deutschen Bundestages

am 7. Oktober 2026

von Jürgen Bering

Leitung Schwerpunkt „Freiheit im Digitalen Zeitalter“, Gesellschaft für Freiheitsrechte e.V.

I. Vorbemerkung

Der Entwurf nimmt die jüngere Rechtsprechung zur anlasslosen Speicherung von IP-Adressen vor allem zum Anlass, rechtliche Spielräume möglichst weit auszuschöpfen. Eine eigenständige gesetzgeberische Abwägung von Nutzen, Alternativen und Grundrechtsbelastungen tritt dabei in den Hintergrund. Die Verantwortung von Bundesregierung und Bundestag für den Grundrechtsschutz erschöpft sich jedoch nicht darin, gerichtlich vorgegebene Grenzen gerade noch einzuhalten.

Auch die Gesamtbelastung durch staatliche Überwachung wird nicht hinreichend berücksichtigt. Neue Befugnisse müssen im Zusammenspiel mit bestehenden und geplanten Instrumenten bewertet werden. Die Verknüpfung und automatisierte Auswertung von Daten können weitreichende Rückschlüsse auf das Privatleben ermöglichen. Gerade bei Befugnissen mit einer solchen Streubreite müssen diese Wechselwirkungen bereits die gesetzliche Ausgestaltung bestimmen.

II. Allgemeine Bewertung

1. Eingriffsgewicht

a. Bedeutung von Internetprotokolladressen

Die IP-Vorratsdatenspeicherung ist auch nach dem Urteil des EuGH vom 30. April 2024 in der Rechtssache La Quadrature du Net II (C-470/21) kein grundrechtlich unbedenkliches Instrument. Der Gerichtshof hat die französische Regelung nicht vorbehaltlos gebilligt, sondern ihre Zulässigkeit an strenge Voraussetzungen geknüpft; deren Einhaltung hat das nationale Gericht zu prüfen. Soll die Speicherung der Bekämpfung allgemeiner Kriminalität dienen, müssen ihre Modalitäten schwere Eingriffe durch aussagekräftige Datenverknüpfungen tatsächlich ausschließen.¹

In der Vergangenheit wurden wiederholt IP-Adressen als „vergleichbar einem temporären digitalen Autokennzeichen“² bezeichnet. Insbesondere zusammen mit Zeitstempeln und Portnummern sind IP-Adressen aber wesentlich mehr als das. Sie ermöglichen die Zuordnung anderweitig dokumentierter Internetaktivitäten zu einem Anschluss. Erst die Verbindung mit diesen Informationen kann sensible Lebensumstände offenlegen. Umgekehrt darf die bloße Anschlusszuordnung nicht mit dem Nachweis gleichgesetzt werden, wer tatsächlich gehandelt hat.

Eine wirksame Datentrennung beim Anbieter beantwortet deshalb noch nicht die Frage, welche Rückschlüsse die empfangende Behörde durch Verknüpfung mit eigenen Erkenntnissen ziehen kann. Speicherung, Auskunft und weitere Verwendung sind jeweils gesondert zu rechtfertigen.³

b. Zusammenwirken mit weiteren Befugnissen

Das Eingriffsgewicht ist im Zusammenhang mit weiteren Datenbeständen und Befugnissen zu beurteilen:

- Die Nutzung vernetzter Mobilgeräte kann Internetaktivitäten in zahlreiche Alltagssituationen hineinragen. Daraus folgt allerdings nicht, dass die IP-Speicherung selbst ein Standortprotokoll erzeugt: Der Entwurf schließt die Speicherung von Kommunikationsinhalten und Daten über die Nutzung anderer Dienste ausdrücklich aus. Das Risiko liegt insbesondere in der späteren Zuordnung bereits anderweitig erfasster Aktivitäten (§ 177 Abs. 1 Satz 3 TKG-E).
- Der Entwurf kombiniert die anlasslose IP-Speicherung mit Sicherungsanordnungen („Quick Freeze“), die weitere Verkehrsdaten erhalten können (§ 100g Abs. 7 StPO-E; § 176 TKG-E). Ein anlassbezogenes Instrument tritt damit nicht an die Stelle der

¹ EuGH, Urt. v. 30. April 2024 – C-470/21, Rn. 82–94.

² BT-Drucksache 20/3687, S.1.

³ EuGH, Urt. v. 30. April 2024 – C-470/21, Rn. 95–97, 110–114, 130–146.

Vorratsspeicherung, sondern neben sie. Bei rechtlich zulässiger Zusammenführung können sich die Erkenntnismöglichkeiten erheblich erweitern.

- Die E-Evidence-Verordnung eröffnet zudem grenzüberschreitende Auskünfte. § 177 Abs. 4 Satz 1 Nr. 2 TKG-E erlaubt die Verwendung der Vorratsdaten zur Erlangung von Teilnehmerdaten. Das ist kein schrankenloser Zugriff ausländischer Behörden: Es gelten insbesondere die Voraussetzungen der Art. 4 bis 6 VO (EU) 2023/1543. Gleichwohl erweitert sich der Kreis möglicher Auskunftersuchen.
- Automatisierte Datenanalysen können den Aussagegehalt einzelner Informationen durch ihre Verknüpfung erhöhen. Das Bundesverfassungsgericht behandelt solche Analysen deshalb als eigenständigen Grundrechtseingriff.⁴ Eine zunächst begrenzte Identitätsauskunft darf nicht allein wegen ihrer ursprünglichen Einordnung für weitergehende Analysen verfügbar sein.
- Auch die Gefahr einer späteren Zweckerweiterung ist konkret: Der Referentenentwurf zum Schutz vor digitaler Gewalt sieht mit § 174 Abs. 5 Nr. 9 TKG-E die Nutzung vorsorglich gespeicherter Daten für gerichtlich angeordnete zivilrechtliche Identitätsauskünfte vor. Das verfolgt ein eigenständig zu bewertendes Schutzanliegen, zeigt aber zugleich, dass der Datenvorrat über die hier angeführten Strafverfolgungszwecke hinaus nutzbar gemacht werden soll.⁵

2. Geeignetheit und Erforderlichkeit

Die IP-Zuordnung kann einen Ermittlungsansatz liefern. Dieser mögliche Nutzen beantwortet jedoch weder die Frage nach der Erforderlichkeit einer flächendeckenden Speicherung noch nach ihrer Dauer. Nötig ist eine nachvollziehbare Bewertung des zusätzlichen Nutzens gegenüber kürzeren Fristen, zügigeren Ermittlungsabläufen und anlassbezogener Sicherung.

Die Begründung nennt Ermittlungsprobleme und Fallkonstellationen. Sie sollte jedoch belastbar ausweisen, wie häufig gerade fehlende Zuordnungsdaten die Aufklärung verhindern und welchen zusätzlichen Beitrag die vorgeschlagene Speicherung leistet.

Der EuGH verlangt keine dreimonatige Frist, sondern eine Begrenzung auf das absolut Notwendige. Die Bundesregierung begründet drei Monate mit verzögert bekannt werdenden Spuren und grenzt diese Fälle ausdrücklich vom optimierten NCMEC-Meldeverfahren ab. Das ist zu würdigen, ersetzt aber keine quantifizierte Gegenüberstellung kürzerer Fristen. Nach der Einschätzung des BKA

⁴ BVerfG, Urt. v. 16. Februar 2023 – 1 BvR 1547/19.

⁵ BMJV, Referentenentwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt, Bearbeitungsstand 16. April 2026, Art. 11 sowie Begründung S. 73–75.

könnten bereits zwei bis drei Wochen im NCMEC-Verfahren einen erheblichen Nutzen bringen.⁶ Wenn eine IP-Zuordnung überhaupt eingeführt werden sollte, dann wäre eine Orientierung an einer Frist in dieser Größenordnung zu bevorzugen.

3. Gesamtbelastung und Missbrauchsvorsorge

Die Ausweitung von Überwachungsbefugnissen verlangt auch eine Betrachtung ihrer kumulativen Wirkung. Unabhängig von der Entwicklung einzelner Kriminalitätsfelder darf die Rechtfertigung nicht auf ein allgemeines Sicherheitsversprechen verkürzt werden. Gerade mit Blick auf mögliche politische Machtverschiebungen müssen die Befugnisse gegen zweckwidrige Verwendung abgesichert sein. Polizei und Nachrichtendienste sind in exekutive Weisungsstrukturen eingebunden; auch die Staatsanwaltschaft ist weisungsgebunden (§§ 146, 147 GVG). Rechtsstaatlicher Schutz muss deshalb durch enge Zwecke, unabhängige Kontrolle und wirksamen Rechtsschutz gesichert werden und darf nicht vom Vertrauen in jeweils amtierende Personen abhängen.

III. Einzelne Regelungsbereiche

1. Vorratsspeicherung von Internetprotokolladressen

Der zentrale Einwand betrifft die Behandlung der IP-basierten Auskunft als regelmäßig begrenzten Identifizierungsvorgang. § 100j Abs. 1 und 2 StPO-E enthält keine ausdrückliche Sonderregel für Fälle, in denen Kontext, wiederholte Abfragen oder Datenverknüpfungen einen schweren Eingriff ermöglichen.

La Quadrature du Net II betraf ein spezialisiertes französisches Verfahren zur Verfolgung von Urheberrechtsverletzungen. Die dortigen Sicherungen lassen sich nicht ohne Prüfung auf Behörden mit anderen Aufgaben und Datenbeständen übertragen. Maßgeblich sind insbesondere folgende Anforderungen:

- Die gespeicherten Datenkategorien müssen technisch wirksam getrennt bleiben; auch die zulässige Identitätszuordnung darf diese Trennung nicht unterlaufen. Ihre Zuverlässigkeit ist regelmäßig durch eine andere öffentliche Stelle zu kontrollieren. Die Speicherdauer ist auf das absolut Notwendige zu begrenzen.⁷
- Der erleichterte Zugang muss auf die Identifizierung begrenzt bleiben und durch Garantien gegen weitergehende Rückschlüsse auf das Privatleben abgesichert werden.

⁶ Siehe BT-Rechtsausschuss, Protokoll 20/68 v. 11. Oktober 2023, S. 14 (Aussage Martina Link).

⁷ EuGH, Urt. v. 30. April 2024 – C-470/21, Rn. 93.

Die geringere Eingriffsintensität ist eine Voraussetzung dieser Erleichterung, keine unwiderlegliche Eigenschaft einer IP-Auskunft.⁸

- Droht der Zugang genaue Rückschlüsse auf das Privatleben zu ermöglichen, verlangt der EuGH eine vorherige Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle. Bei schweren Eingriffen reicht die Verfolgung allgemeiner Kriminalität als Rechtfertigung nicht aus.⁹

Daran gemessen besteht insbesondere folgender Nachbesserungsbedarf:

§ 177 Abs. 3 Nr. 2, Abs. 4 und 5 TKG-E enthält bereits gesetzliche Trennungs-, Verfahrens- und Kontrollvorgaben. Offen bleibt jedoch, wie die Trennung der einzelnen Kategorien, die zulässige Zuordnung und der Ausschluss sonstiger Verknüpfungen konkret abgesichert werden. Auch die offene Kategorie „weitere Verkehrsdaten“ (§ 177 Abs. 1 Satz 1 Nr. 2 TKG-E) sollte auf abschließend bestimmbare Identifizierungsdaten begrenzt werden. Wesentliche Schutzentscheidungen sollte das Gesetz selbst treffen; technische Details können Rechtsverordnung und Richtlinie regeln. Die Speicherpflicht darf praktisch erst greifen, wenn die notwendigen technischen Sicherungen verbindlich feststehen und umgesetzt sind. Auch die Schlussanträge in Académie Fiscale betonen die Bedeutung technischer Trennung und klarer Vorgaben.¹⁰

Die dreimonatige Speicherfrist (§ 177 Abs. 1 Satz 2 TKG-E) bedarf aus den oben genannten Gründen einer tragfähigeren empirischen Begründung. Eine verbindliche, regelmäßige Evaluation sollte den tatsächlichen Zusatznutzen, Fehlzuordnungen, Grundrechtsfolgen und Kosten erfassen; eine Überprüfungsklausel sollte die weitere Geltung an diese Erkenntnisse anknüpfen.

Der Verweis auf punktuelle Auskünfte genügt nicht, wenn die Behörde daraus zusammen mit vorhandenen Erkenntnissen sensible Lebensumstände erschließen kann. Es bedarf gesetzlich bestimmter Verwendungsgrenzen und eines Verfahrens, das solche Konstellationen vor dem eingriffsintensiven Zugriff oder der Verknüpfung erkennt. Die Problematik betrifft auch die vorgelagerte Identifizierungsabfrage bei Kommunikations- und digitalen Diensten (§ 100g Abs. 5, § 100k Abs. 4 StPO-E).

Für diese Fälle sollten erhöhte materielle Schwellen und eine unabhängige Vorabkontrolle ausdrücklich geregelt werden. § 101a Abs. 1 StPO-E erfasst die einfache IP-basierte Bestandsdatenauskunft sowie die genannten Identifizierungsabfragen nicht mit einem Richter*innenvorbehalt.

⁸ EuGH, Urt. v. 30. April 2024 – C-470/21, Rn. 95–114, 122 und Tenor.

⁹ EuGH, Urt. v. 30. April 2024 – C-470/21, Rn. 130–146, insbesondere Rn. 131, 145.

¹⁰ Schlussanträge von GA Szpunar v. 3. September 2026 – C-661/24, Académie Fiscale.

Wiederholte Abfragen sind in ihrer Gesamtheit zu bewerten. Nicht jede Wiederholung bildet ein Profil; entscheidend ist, welche Rückschlüsse die zusammengeführten Informationen zulassen. Dokumentation und technische Vorkehrungen müssen verhindern, dass eine Serie formal einzelner Abfragen die strengeren Voraussetzungen umgeht.¹¹

Schließlich ist zwischen der Kontrolle der Anbieter und der Kontrolle behördlicher Verarbeitung zu unterscheiden. Die regelmäßige Prüfung durch die Bundesnetzagentur (§ 177 Abs. 5 Satz 5 TKG-E) ersetzt keine Kontrolle der nachgelagerten behördlichen Systeme. Der Gesetzgeber sollte hierfür Prüfgegenstand, Zuständigkeit, Zugangs- und Protokollierungsrechte sowie regelmäßige Prüfindervalle nachvollziehbar absichern; allgemeine Datenschutzaufsicht ist auf ihre Eignung zur Erfüllung dieser Aufgabe zu prüfen.

2. Sicherungsanordnungen

Quick Freeze ist als anlassbezogenes Instrument gegenüber einer unterschiedslosen Vorratsspeicherung grundsätzlich vorzugswürdig. Seine konkrete Ausgestaltung muss jedoch eigenständig geprüft werden. Die Aussagen zu einer begrenzten IP-Identifizierung tragen keine pauschale Absenkung der Schwellen für sämtliche Verkehrs- und Standortdaten. Die bisherige EuGH-Rechtsprechung zur umgehenden Sicherung knüpft an die Bekämpfung schwerer Kriminalität oder den Schutz der nationalen Sicherheit und eine wirksame gerichtliche Kontrolle an.¹²

a. Gerichtliche Kontrolle

§ 101a Abs. 1 Satz 1 Nr. 3 Buchst. a StPO-E erlaubt die erste Sicherung für bis zu drei Monate durch die Staatsanwaltschaft, bei Gefahr im Verzug auch durch ihre Ermittlungspersonen. Gerichtliche Kontrolle ist für die Verlängerung und grundsätzlich für den späteren Abruf vorgesehen, nicht aber zwingend zeitnah nach der ersten Sicherung. Die Sicherung ist gegenüber dem Abruf ein weniger intensiver, aber eigenständiger Eingriff. Deshalb überzeugt ein pauschaler Verzicht auf zeitnahe unabhängige Kontrolle insbesondere bei umfangreichen Datenbeständen nicht. Ein regelhafter Richter*innenvorbehalt mit eng begrenzter Eilkompetenz und unverzüglicher Nachprüfung wäre vorzusehen.¹³

b. Eingriffsschwellen und Schutz unverdächtigter Personen

Sicherung und Abruf haben unterschiedliche Voraussetzungen: § 100g Abs. 7 StPO-E verlangt tatsächliche Anhaltspunkte für eine qualifizierende Straftat, einen persönlichen oder räumlichen Tatbezug und die mögliche Bedeutung der Daten. Die Voraussetzungen eines späteren Abrufs

¹¹ EuGH, Urt. v. 30. April 2024 – C-470/21, Rn. 135–143.

¹² EuGH, Urt. v. 5. April 2022 – C-140/20, Rn. 85–91.

¹³ Zum intensitätsabhängigen Kontrollgebot BVerfGE 141, 220, Rn. 117 f.

müssen noch nicht vollständig vorliegen. Nach der Begründung können zudem künftig anfallende Daten gesichert werden. Gerade insoweit geht die Regelung über das bloße Erhalten eines bereits vorhandenen Bestands hinaus und bedarf enger Grenzen.

Für mittels Telekommunikation begangene Straftaten genügt beim Abruf künftig, dass die anderweitige Sachverhaltsaufklärung aussichtslos oder wesentlich erschwert wäre (§ 100g Abs. 2 Nr. 2 StPO-E). Bisher war insoweit Aussichtslosigkeit erforderlich (§ 100g Abs. 1 Satz 2 StPO). Die Absenkung erweitert zugleich den Deliktsbereich der Sicherungsanordnung. Bei aussagekräftigen Verkehrsdaten bestehen unionsrechtliche Bedenken gegen die Einbeziehung nicht schwerer Straftaten. Standortdaten sind allerdings vom erleichterten Abruf nach Absatz 2 ausgenommen.

Die Einbeziehung Unverdächtiger ist nicht schlechthin unzulässig. Der bloße persönliche oder räumliche Bezug darf aber keine flächige Sicherung auf Vorrat legitimieren. Erforderlich sind objektive Kriterien für den konkreten Erkenntnisbezug sowie Grenzen für Personenkreis, Datenkategorien und Zeitraum. Bei tiefgreifenden heimlichen Maßnahmen verlangt das Bundesverfassungsgericht eine spezifische individuelle Nähe zum Ermittlungsziel.¹⁴

§ 101a Abs. 4 StPO-E sieht die Benachrichtigung nach einer Erhebung, nicht aber nach einer bloßen Sicherung gemäß § 100g Abs. 7 StPO-E vor. Unterbleibt der Abruf, erfahren Betroffene daher regelmäßig nichts von der Maßnahme. Die von der Bundesregierung als Ausgleich angeführte statistische Erfassung ersetzt die individuelle Kenntnisnahme nicht. Das erschwert effektiven Rechtsschutz gegen eine rechtswidrige Sicherung. Auch insoweit sollte eine grundsätzlich nachträgliche Benachrichtigung mit eng begrenzten Ausnahmen vorgesehen werden.¹⁵

3. Besonders eingriffsintensive Datenerhebungen

Bei Funkzellenabfragen und retrograden Standortdaten kommt es besonders auf Umfang, Dauer und die Möglichkeiten zur Profilbildung an.

a. Funkzellenabfrage

§ 100g Abs. 4 in Verbindung mit Abs. 3 und 1 StPO-E lässt die Funkzellenabfrage bei Straftaten von auch im Einzelfall erheblicher Bedeutung zu. Damit wird die geltende, vom BGH bestätigte Anknüpfung an den Katalog besonders schwerer Straftaten abgesenkt.¹⁶

Die erhebliche Streubreite erfordert gleichwohl besondere Sicherungen. Erfasst werden können zahlreiche Unverdächtige, etwa im Umfeld einer Versammlung; dort ist auch Art. 8 GG zu berücksichtigen. Nicht sämtliche Teilnehmenden werden zwangsläufig erfasst, doch können

¹⁴ BVerfGE 141, 220, Rn. 104, 114–116.

¹⁵ BVerfGE 141, 220, Rn. 134–141, insbesondere Rn. 136.

¹⁶ BGH, Beschl. v. 10. Januar 2024 – 2 StR 171/23.

Anwesenheits- und Kontaktzusammenhänge erschlossen werden. Das Bundesverfassungsgericht verlangt abgestufte, der Eingriffsintensität entsprechende Schwellen.¹⁷ Kritisch ist, ob die Eingriffsschwelle bei besonders breiten oder kumulierten Abfragen ausreicht. Geboten sind daher wirksame räumliche und zeitliche Begrenzungen, eine konkrete Begründung der Streubreite sowie frühzeitige Aussonderung und Löschung irrelevanter Daten.

b. Retrograde Standortdaten

Bereits angefallene Standortdaten können bei hinreichender Dichte Bewegungsprofile ermöglichen. Sie sind von bloßen Bestandsdaten zu unterscheiden: Die Identifizierung eines Anschlusses liefert für sich kein Bewegungsprofil; hierfür bedarf es zusätzlicher Standortinformationen. Umfangreiche, gegebenenfalls zuvor gesicherte Standortbestände können besonders sensible Rückschlüsse ermöglichen.

§ 100g Abs. 3 StPO-E sieht dafür eine eigene Schwelle vor: eine Straftat von auch im Einzelfall erheblicher Bedeutung und qualifizierte Subsidiarität. § 100k Abs. 3 StPO-E überträgt dies auf digitale Dienste. Gegenüber dem bisherigen Verweis für retrograde Standortdaten auf § 100g Abs. 2 StPO werden die Anforderungen gleichwohl abgesenkt. Die Gleichbehandlung rückblickender und künftig anfallender Daten ist kritisch zu sehen. Erforderlich ist jedenfalls eine Abstufung nach tatsächlicher Aussagekraft: Für umfassende Bewegungsprofile sollten strengere Voraussetzungen gelten als für einzelne Ortspunkte.¹⁸

4. Besondere Schutzbedarfe und Belastungen

Der Entwurf muss außerdem den unterschiedlichen Schutzbedarfen betroffener Personen und den Belastungen der verpflichteten Anbieter Rechnung tragen.

a. Berufsheimnisträgerinnen und Berufsheimnisträger

Mit der Neufassung entfällt die besondere Schutzregel des bisherigen § 100g Abs. 4 StPO für die dort erfassten Datenerhebungen. § 160a StPO bleibt anwendbar, bietet aber nicht allen Berufsgruppen denselben Schutz; insbesondere Journalist*innen unterfallen grundsätzlich der Abwägungsregel des Absatzes 2. Der Quellenschutz aus Art. 5 Abs. 1 Satz 2 GG verlangt besondere Aufmerksamkeit. Zusätzlich fordert Art. 4 Abs. 3 und 4 VO (EU) 2024/1083 (EMFA) für die dort erfassten Maßnahmen grundsätzlich eine unabhängige vorherige Zustimmung, in dringenden Ausnahmefällen unverzügliche nachträgliche Genehmigung. Diese Anforderungen müssen auch bei Identifizierungsabfragen und Sicherungen beachtet werden, soweit deren Anwendungsbereich

¹⁷ BVerfGE 141, 220, Rn. 103–107.

¹⁸ BVerfGE 141, 220, Rn. 105–107.

eröffnet ist. Der pauschale Hinweis auf § 160a StPO beantwortet diese Verfahrensfrage nicht. Näher hierzu die Stellungnahme von Christoph Brill.

b. Kleinere Anbieter und Kostentragung

Der Normenkontrollrat beanstandet eine unvollständige und nicht methodengerechte Darstellung der Regelungsfolgen, insbesondere der Anbieteraufwände.¹⁹ Zwar sieht der Entwurf Entschädigungen für einzelne Mitwirkungshandlungen vor; damit ist die Finanzierung der Speicher- und Sicherheitsinfrastruktur nicht geklärt. Gerade kleine, ehrenamtliche oder nicht kommerzielle Anbieter können dadurch besonders belastet werden. Die Begründung nimmt Freifunkvereine unter den dort beschriebenen Voraussetzungen von § 177 Abs. 1 TKG-E aus; dies ist keine allgemeine Freistellung von sämtlichen Mitwirkungspflichten. Der Kreis der Verpflichteten sollte gesetzlich klar abgegrenzt und die Belastung kleiner Anbieter nachvollziehbar ermittelt werden. Erforderlich sind verhältnismäßige Umsetzungspflichten und eine sachgerechte Kostenregelung, ohne das erforderliche Datensicherheitsniveau abzusenken.

¹⁹ NKR, Stellungnahme zum Entwurf, NKR-Nr. 7948.