Gesetzentwurf

der Bundesregierung

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

A. Problem und Ziel

Straftaten weisen häufig digitale Bezüge auf, zum Beispiel bei der Kommunikation von Tatverdächtigen über Messengerdienste, der Verbreitung von Kinderpornographie, bei kriminellen Handelsplattformen, die Betäubungsmittel oder Cybercrime-as-a-Service (CaaS) anbieten, sowie bei echt wirkenden Onlineshops, die Waren verkaufen, die gar nicht existieren (sogenannte Fakeshops). Die Täter hinterlassen dabei digitale Spuren, zum Beispiel die von ihnen verwendete Internetprotokoll-Adresse (IP-Adresse). Diese Spuren sind nicht selten flüchtig, da die Internetzugangsdiensteanbieter die IP-Adressen – wenn überhaupt – nur wenige Tage speichern. Eine Abfrage der Strafverfolgungsbehörden und anderer berechtigter Stellen bei den Internetzugangsdiensteanbietern hat deshalb nur dann Erfolg, wenn die abgefragten Daten noch gespeichert sind. Ferner ist nach einer Entscheidung des Bundesgerichtshofs eine Funkzellenabfrage nicht mehr bei Straftaten von erheblicher Bedeutung möglich.

Ziel des Entwurfs ist, die Erfolgsaussichten der Abfragen der Strafverfolgungsbehörden und anderer berechtigter Stellen zu verbessern und der Strafverfolgungspraxis die Funkzellenabfrage im Umfang wie vor der Entscheidung des Bundesgerichtshofs zu ermöglichen.

B. Lösung; Nutzen

Es wird erstens eine Pflicht zur Speicherung von IP-Adressen eingeführt, um den Strafverfolgungsbehörden und anderen berechtigten Stellen die zuverlässige Identifikation eines Anschlussinhabers anhand einer IP-Adresse zu ermöglichen. Die Behörden können damit ein Instrument nutzen, das es ihnen erlaubt, dem häufig einzigen, aber nahezu immer effizientesten Ermittlungsansatz zu folgen. Zweitens wird im Bereich der Strafverfolgung und der Gefahrenabwehr durch die Bundespolizei für Verkehrsdaten das Instrument der Sicherungsanordnung geschaffen. Damit können diese Behörden die Sicherung von Verkehrsdaten veranlassen, sofern und solange die rechtlichen oder tatsächlichen Voraussetzungen einer Datenerhebung noch nicht vorliegen. Drittens wird der Strafverfolgungspraxis wieder ermöglicht, bei Straftaten von erheblicher Bedeutung, insbesondere solchen nach § 100a Absatz 2 der Strafprozessordnung, eine Funkzellenabfrage durchzuführen.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Im Haushalt des Bundes entstehen durch die Neuregelungen folgende Bedarfe:

Im Haushalt des Bundesministeriums des Innern, Einzelplan 06, entstehen beim Bundesamt für Verfassungsschutz zusätzliche Personal- und Sachkosten. Für notwendige technische Anpassungen entstehen voraussichtlich im Haushaltsjahr 2027 rund 254 000 Euro einmalige Sachkosten. Für den laufenden Betrieb werden ab 2027 zusätzliche Sachkosten in Höhe von 177 000 Euro erwartet. Die erforderlichen technischen Anpassungen sind nach derzeitigen Schätzungen mit einem zusätzlichen Bedarf von vier (Plan-)Stellen (1 A14, 1 A12, 1 A11, 1 E9a) verbunden. Die zusätzlichen Personalkosten betragen 372 000 Euro.

Im Haushalt des Bundesministeriums der Justiz und für Verbraucherschutz, Einzelplan 07, werden beim Bundesgerichtshof und bei dem Generalbundesanwalt beim Bundesgerichtshof ab dem Jahr 2027 minimale zusätzliche Sachkosten für Sicherungsanordnungen entstehen, die nach aktuellen Prognosen deutlich unter 1 000 Euro pro Jahr liegen werden.

Im Haushalt des Bundesministeriums der Finanzen, Einzelplan 08, werden bei den Behörden der Zollverwaltung voraussichtlich keine zusätzlichen Personal- oder Sachkosten entstehen.

Der zuvor dargestellte Mehrbedarf sowie etwaiger sonstiger Mehrbedarf soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Im Haushalt des Bundesministeriums für Wirtschaft und Energie, Einzelplan 09, besteht bei der Bundesnetzagentur ab dem Haushaltsjahr 2027 geschätzt ein zusätzlicher Personalbedarf in Höhe von 26 Planstellen für die Fachaufgaben (1 A16, 1 A15, 1 A14, 1 A13gZ, 3 A13g, 5 A12, 5 A11, 1 A10, 1 A9mZ, 2 A9m, 3 A8, 1 A7, 1 A6m) mit jährlichen Personaleinzelkosten in Höhe von insgesamt 2,376 Mio. Euro, Sacheinzelkosten in Höhe von 891 000 Euro sowie Gemeinkosten in Höhe von 960 000 Euro. Für die zusätzlichen Querschnittsaufgaben sind weitere 7,8 Stellen erforderlich (jeweils 0,3 A16, A15, A14 und A13gZ, 0,9 A13g, jeweils 1,5 A12 und A11, jeweils 0,3 A10 und A9mZ, 0,6 A9m, 0,9 A8 und jeweils 0,3 A7 und A6m). Die zusätzlichen Personal- und Sachkosten für die Querschnittsaufgaben sind in den Gemeinkosten enthalten. Hinzu kommen ab dem Haushaltsjahr 2027 jährliche laufende Sachkosten in Höhe von 5 000 Euro sowie im Jahr 2027 einmalige Sachkosten in Höhe von 25 000 Euro für die Erweiterung einer bestehenden Laboranlage.

Im Haushalt des Bundesministeriums für Wirtschaft und Energie sind zusätzliche Einnahmen infolge zusätzlicher Bußgeldverfahren zu erwarten. Die Höhe der Einnahme hängt von der Anzahl der Verfahren und der Schwere der Verstöße ab und lässt sich nicht prognostizieren.

Der stellenmäßige Mehrbedarf soll im Einzelplan 09 ausgeglichen werden. Der finanzielle Mehrbedarf soll in den jeweiligen Einzelplänen ausgeglichen werden.

Für die Haushalte der Länder ist mit Minderbedarfen in Höhe von insgesamt 1,429 Mio. Euro zu rechnen. Auswirkungen auf die Haushalte der Gemeinden sind nicht zu erwarten.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Keiner.

E.3 Erfüllungsaufwand der Verwaltung

Keiner.

F. Weitere Kosten

Die Regelungen zur IP-Adressspeicherung und Einführung einer Sicherungsanordnung für Verkehrsdaten betreffen den justiziellen Kernbereich. Es ist davon auszugehen, dass die Auswirkungen sowohl für den Bund als auch für die Länder überwiegend kostenneutral sind. Für die Wirtschaft entstehen weitere Kosten. Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau für Telekommunikationsdienste, sind im Übrigen nicht zu erwarten.

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren[1]

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 7 des Gesetzes vom 20. März 2026 (BGBl. 2026 I Nr. 95) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angabe zu § 100j wird durch die folgende Angabe ersetzt:

   „§ 100j Erhebung von Bestandsdaten“.

   b) Die Angabe zu § 101a wird durch die folgende Angabe ersetzt:

   „§ 101a Verfahrensregelungen bei Erhebung von Verkehrs-, Nutzungs- und Bestandsdaten“.

2. § 100g wird durch den folgenden § 100g ersetzt:

„§ 100g

Erhebung von Verkehrsdaten

(1) Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes, mit Ausnahme der aufgrund von § 177 Absatz 1 des Telekommunikationsgesetzes gespeicherten Daten, des Beschuldigten dürfen bei demjenigen erhoben werden, der öffentlich zugängliche Telekommunikationsdienste anbietet oder daran mitwirkt,

1. wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat,

2. soweit die Erhebung der Verkehrsdaten für die Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts des Beschuldigten erforderlich ist und

[1] Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

3. soweit die Erhebung der Verkehrsdaten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

Satz 1 gilt entsprechend für die Erhebung von Verkehrsdaten von Personen, bei denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt. Die Sätze 1 und 2 gelten für die Erhebung von Verkehrsdaten nach § 2a Absatz 1 des BDBOS-Gesetzes bei der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben entsprechend.

(2) Besteht kein Verdacht hinsichtlich einer Straftat von auch im Einzelfall erheblicher Bedeutung, ist die Erhebung von Verkehrsdaten unter den übrigen Voraussetzungen von Absatz 1 mit folgenden Maßgaben zulässig:

1. bestimmte Tatsachen begründen den Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat mittels Telekommunikation begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, und

2. abweichend von Absatz 1 Satz 1 Nummer 2 wäre die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert; eine Erhebung zur Ermittlung des Aufenthaltsorts des Beschuldigten ist unzulässig.

(3) Standortdaten gemäß § 3 Nummer 56 des Telekommunikationsgesetzes dürfen unter den Voraussetzungen von Absatz 1 mit der Maßgabe erhoben werden, dass die Erhebung abweichend von Absatz 1 Satz 1 Nummer 2 nur zulässig ist, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(4) Die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten (Funkzellenabfrage) ist unter den Voraussetzungen von Absatz 3 zulässig.

(5) Abweichend von den Absätzen 1 und 2 darf die Strafverfolgungsbehörde bei einem nummernunabhängigen interpersonellen Kommunikationsdienst, wenn ihr der Inhalt der Nutzung des Dienstes bereits bekannt ist, zum Zweck der Identifikation des Beschuldigten Folgendes erheben:

1. die zu ihm gespeicherte öffentliche Internetprotokoll-Adresse,

2. das Datum und die sekundengenaue Uhrzeit der Speicherung der öffentlichen Internet-Protokoll-Adresse unter Angabe der jeweils zugrunde liegenden Zeitzone sowie

3. die der Internetprotokoll-Adresse zugehörigen Portnummern und weitere Verkehrsdaten, soweit diese für eine Identifizierung des Beschuldigten anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse erforderlich sind.

Absatz 1 Satz 2 gilt entsprechend.

(6) Erfolgt die Erhebung von Verkehrsdaten nicht beim Verpflichteten nach Absatz 1 Satz 1 oder 3, bestimmt sich ihre Zulässigkeit nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.

(7) Zum Zwecke einer etwaigen Erhebung nach den Absätzen 1 bis 4 darf angeordnet werden, dass Verpflichtete Verkehrsdaten von betroffenen Personen unverzüglich zu sichern haben (Sicherungsanordnung),

1. wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Straftat begangen worden ist, welche die Erhebung nach den Absätzen 1 bis 4 rechtfertigen würde,

2. wenn die betroffene Person in einem persönlichen oder räumlichen Bezug zu der Straftat nach Nummer 1 steht und

3. soweit die Daten für die in den Absätzen 1 bis 4 jeweils genannten Zwecke von Bedeutung sein können.

Die Erhebung der nach Satz 1 gesicherten Daten erfolgt nach den Absätzen 1 bis 4.“

3. Die §§ 100j und 100k werden durch die folgenden §§ 100j und 100k ersetzt:

„§ 100j

Erhebung von Bestandsdaten

(1) Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist, darf Auskunft verlangt werden

1. über Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 Absatz 1 des Telekommunikationsgesetzes erhobenen Daten bei demjenigen, der öffentlich zugängliche Telekommunikationsdienste anbietet oder daran mitwirkt, und

2. über Bestandsdaten gemäß § 2 Absatz 2 Nummer 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes bei demjenigen, der digitale Dienste anbietet.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden.

(3) Bezieht sich das Auskunftsverlangen nach Absatz 1 Nummer 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 174 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Bezieht sich das Auskunftsverlangen nach Absatz 1 Nummer 2 auf als Bestandsdaten erhobene Passwörter oder andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 23 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für ihre Nutzung zur Verfolgung einer besonders schweren Straftat nach § 100b Absatz 2 Nummer 1 Buchstabe a, c, e, f, g, h oder m, Nummer 3 Buchstabe b erste Alternative oder Nummer 5, 5a, 5b, 6, 9 oder 10 vorliegen.

§ 100k

Erhebung von Nutzungsdaten bei digitalen Diensten

(1) Nutzungsdaten gemäß § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes des Beschuldigten dürfen bei demjenigen, der digitale Dienste anbietet, unter den Voraussetzungen des § 100g Absatz 1 Satz 1 erhoben werden. § 100g Absatz 1 Satz 2 gilt entsprechend.

(2) § 100g Absatz 2 gilt für die Erhebung von Nutzungsdaten bei dem Verpflichteten nach Absatz 1 mit der Maßgabe entsprechend, dass eine Erhebung zulässig ist, wenn der Verdacht hinsichtlich einer mittels eines digitalen Dienstes begangenen Straftat besteht.

(3) Standortdaten dürfen bei dem Verpflichteten nach Absatz 1 unter den Voraussetzungen von § 100g Absatz 3 erhoben werden.

(4) Nutzungsdaten zum Zweck der Identifikation des Beschuldigten dürfen bei dem Verpflichteten nach Absatz 1 unter den Voraussetzungen des § 100g Absatz 5 erhoben werden.

(5) Die Erhebung von Nutzungsdaten nach den Absätze 1 bis 3 ist nur zulässig, wenn aufgrund von Tatsachen die Annahme gerechtfertigt ist, dass die betroffene Person den digitalen Dienst des Verpflichteten nutzt.

(6) Erfolgt die Erhebung von Nutzungsdaten eines digitalen Dienstes nicht bei dem Verpflichteten nach Absatz 1, bestimmt sich ihre Zulässigkeit nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.“

4. § 101a wird durch den folgenden § 101a ersetzt:

„§ 101a

Verfahrensregelungen bei Erhebung von Verkehrs-, Nutzungs- und Bestandsdaten

(1) § 100e Absatz 1, 3 Satz 1 und 2 Nummer 1 bis 5 und Absatz 5 Satz 1 und 2 gilt entsprechend hinsichtlich der folgenden Verfahren:

1. bei Erhebung von Verkehrsdaten nach § 100g Absatz 1 bis 4 mit der Maßgabe, dass

   a) in der Entscheidungsformel nach § 100e Absatz 3 Satz 2 auch die zu übermittelnden Daten und der Zeitraum, für den sie übermittelt werden sollen, eindeutig anzugeben sind und

   b) bei Funkzellenabfragen nach § 100g Absatz 4 in der Entscheidungsformel abweichend von § 100e Absatz 3 Satz 2 Nummer 5 eine räumlich und zeitlich eng begrenzte und hinreichend bestimmte Bezeichnung der Telekommunikation genügt,

2. bei Erhebung von Nutzungsdaten nach § 100k Absatz 1 bis 3 mit der Maßgabe, dass

   a) in der Entscheidungsformel abweichend von § 100e Absatz 3 Satz 2 Nummer 5 wenn möglich eine eindeutige Kennung des Nutzerkontos des

Betroffenen, andernfalls eine möglichst genaue Bezeichnung des digitalen Dienstes, auf den sich das Auskunftsverlangen bezieht, anzugeben ist und

b) in der Entscheidungsformel auch die zu übermittelnden Daten und der Zeitraum, für den sie übermittelt werden sollen, eindeutig anzugeben sind,

3. bei einer Sicherungsanordnung nach § 100g Absatz 7 mit der Maßgabe, dass

a) abweichend von § 100e Absatz 1 Satz 1 bis 3 die Maßnahme durch die Staatsanwaltschaft für höchstens drei Monate angeordnet werden kann, bei Gefahr im Verzug auch durch ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes), und die Maßnahme nur auf Antrag der Staatsanwaltschaft durch das Gericht um höchstens drei Monate verlängert werden kann,

b) in der Entscheidungsformel nach § 100e Absatz 3 Satz 2 auch die zu sichernden Daten und der Zeitraum, für den sie gesichert werden sollen, eindeutig anzugeben sind und

c) bei der Sicherung von Daten einer Funkzelle nach § 100g Absatz 3 in der Entscheidungsformel abweichend von § 100e Absatz 3 Satz 2 Nummer 5 eine räumlich und zeitlich eng begrenzte und hinreichend bestimmte Bezeichnung der Telekommunikation genügt.

§ 100e Absatz 1 Satz 1 bis 3 und Absatz 3 Satz 1 und 2 Nummer 1 bis 4 gilt entsprechend hinsichtlich der Verfahren bei Erhebung von Bestandsdaten nach § 100j Absatz 3 mit der Maßgabe, dass

1. anstelle von § 100e Absatz 1 Satz 2 die gerichtliche Entscheidung unverzüglich nachzuholen ist und

2. in der Entscheidungsformel nach § 100e Absatz 3 Satz 2 Nummer 3 Dauer und Endzeitpunkt der Maßnahme nicht anzugeben sind.

Satz 2 findet bei Auskunftsverlangen nach § 100j Absatz 3 Satz 1 keine Anwendung, wenn die betroffene Person vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird.

(2) Wird eine Maßnahme nach § 100g Absatz 1 bis 4 oder 7, § 100j Absatz 3 oder § 100k Absatz 1 bis 3 angeordnet oder verlängert, sind in der Begründung einzelfallbezogen insbesondere die wesentlichen Erwägungen zur Erforderlichkeit und Angemessenheit der Maßnahme, auch hinsichtlich des Umfangs der zu erhebenden Daten und des Zeitraums, für den sie erhoben werden sollen, darzulegen.

(3) Personenbezogene Daten, die durch Maßnahmen nach § 100g Absatz 1 bis 4, § 100j Absatz 3 oder § 100k Absatz 1 bis 3 erhoben wurden, sind entsprechend zu kennzeichnen und unverzüglich auszuwerten. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten. Für die Löschung personenbezogener Daten gilt § 101 Absatz 8 entsprechend.

(4) Die Beteiligten der betroffenen Telekommunikation und die betroffenen Nutzer des digitalen Dienstes sind von einer Erhebung nach § 100g Absatz 1 bis 5, § 100j Absatz 2 und 3 und nach § 100k Absatz 1 bis 4 zu benachrichtigen. § 101 Absatz 4 Satz 2 bis 5 und Absatz 5 bis 7 gilt entsprechend.

(5) Hinsichtlich der Mitwirkungspflicht von nach den §§ 100g, 100j und 100k Verpflichteten gilt § 100a Absatz 4 entsprechend.“

5. § 101b wird wie folgt geändert:

a) In Absatz 1 Satz 1 wird die Angabe „Absatz 1 und 2“ gestrichen.

b) Absatz 5 wird wie folgt geändert:

a%6) In Nummer 1 in der Angabe vor Buchstabe a wird die Angabe „§ 100g Absatz 1, 2 und 3“ durch die Angabe „§ 100g Absatz 1, 2, 3, 4 und 7“ ersetzt.

b%6) Nummer 2 wird wie folgt geändert:

a%7%7) Nach Buchstabe c werden die folgenden Buchstaben d und e eingefügt:

a) „ die Anzahl der Anordnungen nach § 100g Absatz 4;

b) die Anzahl der Anordnungen nach § 100g Absatz 7;“.

b%7%7) Die bisherigen Buchstaben d und e werden zu den Buchstaben f und g.

c) In Absatz 6 in der Angabe vor Nummer 1 wird die Angabe „nach den Absätzen 1 und 2“ durch die Angabe „nach den Absätzen 1, 2 und 3“ ersetzt.

6. § 160a Absatz 5 wird durch den folgenden Absatz 5 ersetzt:

(1) „ Die §§ 97 und 100d Absatz 5 bleiben unberührt.“

Artikel 2

Änderung des Einführungsgesetzes zur Strafprozessordnung

Das Einführungsgesetz zur Strafprozessordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 312-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 4 des Gesetzes vom 8. Dezember 2025 (BGBl. 2025 I Nr. 319) geändert worden ist, wird wie folgt geändert:

§ 12 wird durch den folgenden § 12 ersetzt:

§ 1„

Übergangsregelung zum Gesetz zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren

Übersichten nach § 101b Absatz 5 und 6 der Strafprozessordnung in der vom … [einsetzen: Datum des Inkrafttretens nach Artikel 13 dieses Gesetzes] geltenden Fassung sind erstmalig für das auf den … [einsetzen: Datum des Inkrafttretens nach Artikel 13 dieses Gesetzes] folgende Berichtsjahr zu erstellen. Für die vorangehenden Berichtsjahre ist § 101b Absatz 5 und 6 der Strafprozessordnung in der bis einschließlich … [einsetzen:

Datum des Tages vor dem Inkrafttreten nach Artikel 13 dieses Gesetzes] geltenden Fassung anzuwenden.“

Artikel 3

Änderung des Elektronische-Beweismittel-Umsetzungs-und-Durchführungsgesetzes

Das Elektronische-Beweismittel-Umsetzungs-und-Durchführungsgesetz vom 10. März 2026 (BGBl. 2026 I Nr. 64) wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 10 die folgende Angabe eingefügt:

   „§ 10a Verfahren bei Europäischen Sicherungsanordnungen“.

2. Nach § 10 wird der folgende § 10a eingefügt:

„§ 10a

Verfahren bei Europäischen Sicherungsanordnungen

(1) Die Zuständigkeit der Staatsanwaltschaften für den Erlass von Europäischen Sicherungsanordnungen zum Zwecke der Strafverfolgung nach Artikel 4 Absatz 3 Buchstabe a der Verordnung (EU) 2023/1543 in der Fassung vom 12. Juli 2023 und für die Übermittlung der dazugehörigen Bescheinigung richtet sich nach dem Achten Abschnitt des Ersten Buchs der Strafprozessordnung.

(2) In einem begründeten Notfall gemäß Artikel 4 Absatz 5 der Verordnung (EU) 2023/1543 in der Fassung vom 12. Juli 2023 sind unter den dort genannten Voraussetzungen für den Erlass von Europäischen Sicherungsanordnungen und die Übermittlung der dazugehörigen Bescheinigung die folgenden Stellen nach Artikel 4 Absatz 3 Buchstabe b der Verordnung (EU) 2023/1543 in der Fassung vom 12. Juli 2023 zuständig:

1. die Ermittlungspersonen der Staatsanwaltschaft (§ 152 des Gerichtsverfassungsgesetzes),

2. die Finanzbehörden in den Fällen des § 399 Absatz 1 und des § 386 Absatz 2 der Abgabenordnung,

3. die Behörden der Zollverwaltung in den Fällen der §§ 14a und 14b des Gesetzes zur Bekämpfung der Schwarzarbeit und illegalen Beschäftigung.

(3) In Fällen des Absatzes 2 übermitteln die Anordnungsbehörden die Europäische Sicherungsanordnung innerhalb der in Artikel 4 Absatz 5 Satz 2 der Verordnung (EU) 2023/1543 in der Fassung vom 12. Juli 2023 genannten Frist der Staatsanwaltschaft zur Ex-Post-Validierung. Die Übermittlung der Bescheinigung durch die Anordnungsbehörde und die Entscheidung über die Validierung durch die Staatsanwaltschaft sind aktenkundig zu machen.

(4) Örtlich zuständig für die Validierung ist die ermittlungsführende Staatsanwaltschaft. Wenn die Finanzbehörden oder die Behörden der Zollverwaltung nach nationalem Recht die Ermittlungen selbst führen, ist für die Validierung die

Staatsanwaltschaft bei dem Landgericht zuständig, in dessen Bezirk die Anordnungsbehörde ihren Sitz hat. Die Länder können die örtliche Zuständigkeit abweichend regeln.

(5) Zuständig für den Erlass Europäischer Sicherungsanordnungen zum Zwecke der Strafvollstreckung im Sinne von Artikel 4 Absatz 3 Buchstabe a der Verordnung (EU) 2023/1543 in der Fassung vom 12. Juli 2023 und für die Übermittlung der dazugehörigen Bescheinigung sind die Staatsanwaltschaften und der Jugendrichter als Vollstreckungsleiter.“

Artikel 4

Änderung des Justizvergütungs- und -entschädigungsgesetzes

Das Justizvergütungs- und -entschädigungsgesetz vom 5. Mai 2004 (BGBl. I S. 718, 776), das zuletzt durch Artikel 13 des Gesetzes vom 8. Dezember 2025 (BGBl. 2025 I Nr. 318) geändert worden ist, wird wie folgt geändert:

1. In § 23 Absatz 1 wird nach der Angabe „Telekommunikation“ die Angabe „oder Sicherungsanordnungen“ eingefügt.

2. Anlage 3 wird wie folgt geändert:

a) Absatz 2 der Allgemeinen Vorbemerkung wird durch den folgenden Absatz 2 ersetzt:

(1) „ Für Leistungen, die die Strafverfolgungsbehörden über eine zentrale Kontaktstelle des Generalbundesanwalts, des Bundeskriminalamtes, der Bundespolizei oder des Zollkriminalamtes oder über entsprechende für ein Land oder für mehrere Länder zuständige Kontaktstellen anfordern und abrechnen, ermäßigen sich die Entschädigungsbeträge nach den Nummern 100, 101, 200 bis 202, 300 bis 308 und nach den Abschnitten 4 bis 6 um 20 Prozent.“

b) Nummer 201 wird durch die folgende Nummer 201 ersetzt:

Nr.	Tätigkeit	Höhe
„201	Auskunft über Bestandsdaten, zu deren Erteilung auf Verkehrsdaten zurückgegriffen werden muss: für bis zu 3 in demselben Verfahren gleichzeitig angefragte Kennungen, die der Auskunftserteilung zugrunde liegen..... Bei mehr als 3 angefragten Kennungen wird die Pauschale für jeweils bis zu 3 weitere Kennungen erneut gewährt. Kennung ist auch eine IP-Adresse.	15,00 €“.

c) Die Überschrift des Abschnitts 3 wird durch die folgende Überschrift ersetzt:

„Abschnitt 3

Auskünfte über Verkehrsdaten ohne vorausgegangene Sicherungsanordnung“.

d) Nach der Überschrift des Abschnitts 3 wird die folgende Vorbemerkung 3 eingefügt:

„*Vorbemerkung 3:*

Leitungskosten werden nur entschädigt, wenn die betreffende Leitung mindestens einmal zur Übermittlung von Verkehrsdaten genutzt worden ist. Die Entschädigung erfolgt für den gesamten Übermittlungszeitraum.“

e) Die Überschrift des Abschnitts 4 wird durch die folgende Überschrift ersetzt:

„Abschnitt 4

Sonstige Auskünfte ohne vorausgegangene Sicherungsanordnung“.

f) Nach Nummer 402 werden die folgenden Abschnitte 5 und 6 eingefügt:

Nr.	Tätigkeit	Höhe
	„Abschnitt 5	
	Sicherung von Daten	
500	Sicherung von Verkehrsdaten: für jede Kennung, die der Sicherungsanordnung zugrunde liegt ..... Die Sicherung der die Kennung betreffenden Standortdaten ist mit abgegolten.	25,00 €
501	Sicherung von Verkehrsdaten für eine von der Strafverfolgungsbehörde benannte Funkzelle	40,00 €
502	Sicherung von Verkehrsdaten für mehr als eine von der Strafverfolgungsbehörde benannte Funkzelle: Die Pauschale 501 erhöht sich für jede weitere Funkzelle um	5,00 €
503	Sicherung von Verkehrsdaten in Fällen, in denen lediglich Ort und Zeitraum bekannt sind: Die Sicherung erfolgt für einen bestimmten, durch eine Adresse bezeichneten Standort	75,00 €
504	Die Sicherung erfolgt für eine Fläche: Die Entschädigung nach Nummer 503 beträgt	190,00 €
505	Die Sicherung erfolgt für eine bestimmte Wegstrecke: Die Entschädigung nach Nummer 503 beträgt für jeweils angefangene 10 Kilometer Länge	65,00 €
506	Sicherung der Daten des letzten dem Netz bekannten Standortes eines Mobiltelefons	85,00 €
507	Verlängerung der Speicherung gesicherter Daten für jeden der in den Nummern 500, 501 und 503 bis 506 genannten Fälle	25,00 €
	Abschnitt 6	
	Auskünfte nach vorausgegangener Sicherungsanordnung	
600	Auskunft über Daten, soweit eine nach Abschnitt 5 zu entschädigende Sicherungsanordnung vorausgegangen ist: je Auskunftsersuchen	20,00 €“.

Artikel 5

Änderung des Gesetzes über Ordnungswidrigkeiten

Das Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), das zuletzt durch Artikel 21 des Gesetzes vom 22. Dezember 2025 (BGBl. 2025 I Nr. 349) geändert worden ist, wird wie folgt geändert:

In § 46 Absatz 4a wird die Angabe „§ 100j Absatz 1 Satz 1 Nummer 2“ durch die Angabe „§ 100j Absatz 1 Nummer 2“ ersetzt.

Artikel 6

Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch … [Artikel 2 des Entwurfs eines Gesetzes zur Durchführung einer Verordnung der Europäischen Union zum Datenaustausch bei Kurzzeitvermietungen sowie zur Durchsetzung von Diskriminierungsverboten der Europäischen Union, Bundestagsdrucksache 21/3484] geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu den §§ 175 bis 181 durch die folgende Angabe ersetzt:

„§ 175 Auskunft über Verkehrsdaten an Strafverfolgungs- und Sicherheitsbehörden

§ 176 Verarbeitungsbefugnis von Verkehrsdaten aufgrund von Sicherungsanordnungen

§ 177 Speicherpflicht und Verwendungsbefugnis von Verkehrsdaten zur Identifizierung von Anschlussinhabern

§§ 178 bis 181 (weggefallen)“.

2. Die §§ 175 bis 181 werden durch die folgenden §§ 175 bis 177 ersetzt:

§ 1„

Befugnis zur Verarbeitung von Verkehrsdaten zur Auskunftserteilung an Strafverfolgungs- und Sicherheitsbehörden

(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt oder daran mitwirkt, darf Verkehrsdaten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verarbeiten. Der Bundesnetzagentur ist auf deren Verlangen unverzüglich mitzuteilen, wer diese Daten speichert. Für die Auskunftserteilung nach Satz 1 gilt § 32 der Rechtsverordnung nach § 170 Absatz 5 entsprechend.

(2) Die Auskunft nach Absatz 1 Satz 1 darf nur erteilt werden nach Maßgabe der nachfolgenden Absätze und soweit ein Auskunftsverlangen einer in Absatz 3 genannten Stelle vorliegt, das die gesetzliche Bestimmung enthält, die der Auskunft verlangenden Stelle eine Erhebung von Verkehrsdaten erlaubt. Die Verantwortung für die Rechtmäßigkeit des Auskunftsverlangens tragen die um Auskunft ersuchenden Stellen.

(3) Die Auskunft nach Absatz 1 Satz 1 darf nur erteilt werden an

1. die für die Verfolgung von Straftaten zuständigen Behörden unter den Voraussetzungen des § 100g der Strafprozessordnung,

2. die Gefahrenabwehrbehörden der Länder, soweit dies im Einzelfall erforderlich ist zur Abwehr einer konkretisierten Gefahr für ein Rechtsgut von zumindest erheblichem Gewicht oder zur Abwehr einer konkreten Gefahr für die öffentliche Sicherheit,

3. die Bundespolizei unter den Voraussetzungen des § 25 Absatz 1 des Bundespolizeigesetzes,

4. das Bundeskriminalamt unter den Voraussetzungen des § 52 Absatz 1 des Bundeskriminalamtgesetzes,

5. das Zollkriminalamt unter den Voraussetzungen des § 77 Absatz 1 des Zollfahndungsdienstgesetzes,

6. das Bundesamt für Verfassungsschutz unter den Voraussetzungen des § 8a Absatz 1 Satz 1 Nummer 4 des Bundesverfassungsschutzgesetzes,

7. die Verfassungsschutzbehörden der Länder, soweit dies aufgrund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten nach

   a) § 3 Absatz 1 des Bundesverfassungsschutzgesetzes oder

   b) einem zum Verfassungsschutz (§ 1 Absatz 1 des Bundesverfassungsschutzgesetzes) landesgesetzlich begründeten Beobachtungsauftrag der Landesbehörde, insbesondere zum Schutz der verfassungsmäßigen Ordnung vor Bestrebungen und Tätigkeiten der organisierten Kriminalität,

8. den Militärischen Abschirmdienst unter den Voraussetzungen des § 20 Absatz 1 Satz 1 Nummer 5 des MAD-Gesetzes sowie

9. den Bundesnachrichtendienst unter den Voraussetzungen des § 3 des BND-Gesetzes in Verbindung mit § 8a Absatz 1 Satz 1 Nummer 4 des Bundesverfassungsschutzgesetzes.

(1) § 174 Absatz 6 Satz 2 und Absatz 7 ist entsprechend anzuwenden.

§ 2

Befugnis zur Verarbeitung von Verkehrsdaten zur Erfüllung von Sicherungsanordnungen

(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt oder daran mitwirkt, darf Verkehrsdaten verarbeiten, soweit dies erforderlich ist zur Erfüllung

1. einer Sicherungsanordnung nach § 100g Absatz 7 der Strafprozessordnung,

2. einer Sicherungsanordnung nach § 10b Absatz 1 oder § 52 Absatz 3 des Bundeskriminalamtgesetzes oder

3. einer Sicherungsanordnung nach § 25a Absatz 1 des Bundespolizeigesetzes.

Verkehrsdaten, die allein aufgrund einer Sicherungsanordnung gemäß Satz 1 gesichert wurden, dürfen nur im Rahmen des jeweiligen Sicherungszwecks verwendet und unter den Voraussetzungen des § 175 beauskunftet werden. Der Bundesnetzagentur ist auf deren Verlangen unverzüglich mitzuteilen, wer diese Daten speichert.

(2) Verpflichtete einer Sicherungsanordnung gemäß Absatz 1 Satz 1 haben sicherzustellen, dass die nach Absatz 1 gesicherten Verkehrsdaten

1. durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden,

2. technisch wirksam getrennt von allen anderen beim Verpflichteten vorhandenen Daten zu Anschlussinhabern durch eine abgesicherte und zuverlässige Datenverarbeitungseinrichtung gespeichert werden,

3. so gespeichert werden, dass die Übermittlung an eine anordnende Stelle unverzüglich erfolgen kann, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung verlangt, und

4. nach dem Stand der Technik unverzüglich und irreversibel gelöscht werden:

   a) soweit sie an die anordnende Stelle in Erfüllung eines Auskunftsverlangens nach Absatz 1 Satz 2 übermittelt werden, nach dieser Übermittlung,

   b) im Übrigen nach Ablauf der in der Sicherungsanordnung genannten Frist.

(3) Verpflichtete einer Sicherungsanordnung gemäß Absatz 1 Satz 1 haben über das Vorliegen einer Sicherungsanordnung, eines darauf bezogenen Auskunftsverlangens und über die auf dieser Grundlage erfolgte Datenübermittlung gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren.

(4) In der Rechtsverordnung nach § 170 Absatz 5 können Regelungen zur näheren Ausgestaltung der Pflichten nach den Absätzen 2 und 3 sowie zur Übermittlung der aufgrund von Sicherungsanordnungen gemäß Absatz 1 Satz 1 gesicherten Verkehrsdaten getroffen werden. Technische Einzelheiten zur Umsetzung dieser Pflichten werden in der Technischen Richtlinie nach § 170 Absatz 6 festgelegt. Anbieter öffentlich zugänglicher Telekommunikationsdienste haben der Bundesnetzagentur unverzüglich nach Aufnahme des Dienstes unter Vorlage von Unterlagen mitzuteilen, wie die Vorgaben nach Absatz 2 sowie der Rechtsverordnung nach Satz 1 und § 170 Absatz 5 sowie der Technischen Richtlinie nach Satz 2 und § 170 Absatz 6 in ihren Anlagen umgesetzt werden. Änderungen sind der Bundesnetzagentur unverzüglich mitzuteilen. Die Bundesnetzagentur überprüft regelmäßig die Umsetzung der Vorgaben.

§ 3

Pflicht zur Speicherung und Befugnis zur Verwendung von Verkehrsdaten zur Identifizierung von Anschlussinhabern

(1) Wer Internetzugangsdienste erbringt, ist verpflichtet, mit der Zuweisung einer öffentlichen Internetprotokoll-Adresse an einen Anschlussinhaber folgende Daten zu speichern:

1. die dem Anschlussinhaber für eine Internetverbindung zugewiesene, öffentliche Internetprotokoll-Adresse,

2. die der Internetprotokoll-Adresse zugehörigen Portnummern und weitere Verkehrsdaten, soweit diese für eine Identifizierung des Anschlussinhabers anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse erforderlich sind,

3. eine eindeutige Kennung des Anschlusses, über den die Internetverbindung erfolgt, sowie eine zugewiesene Benutzerkennung und

4. das Datum und die sekundengenaue Uhrzeit von Beginn und Ende der Zuweisung der öffentlichen Internetprotokoll-Adressen sowie der zugehörigen Portnummern und weiterer Verkehrsdaten, soweit diese nach Nummer 2 zu

speichern sind, an einen Anschlussinhaber unter Angabe der jeweils zugrunde liegenden Zeitzone.

Die Daten nach Satz 1 sind jeweils für drei Monate zu speichern. Inhalte der Kommunikation sowie Daten über den Aufruf oder die Nutzung von anderen Telekommunikationsdiensten oder digitalen Diensten dürfen nicht aufgrund dieser Vorschrift gespeichert werden.

(2) Ein Anbieter nach Absatz 1 Satz 1, der nicht alle der nach Absatz 1 Satz 1 zu speichernden Daten selbst erzeugt oder verarbeitet, hat

1. sicherzustellen, dass die nicht von ihm selbst bei der Erbringung seines Dienstes erzeugten oder verarbeiteten Daten gemäß Absatz 1 gespeichert werden,

2. der Bundesnetzagentur auf deren Verlangen unverzüglich mitzuteilen, wer diese Daten speichert.

(3) Verpflichtete nach Absatz 1 haben sicherzustellen, dass die aufgrund des Absatzes 1 gespeicherten Daten

1. durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden,

2. technisch wirksam getrennt von allen anderen beim Verpflichteten vorhandenen Endnutzerdaten gespeichert werden,

3. so gespeichert werden, dass die Auskunft zum Anschlussinhaber an die berechtigten Stellen unverzüglich erfolgen kann, und

4. nach Ablauf der Speicherfrist des Absatzes 1 Satz 2 unverzüglich und nach dem Stand der Technik irreversibel gelöscht werden.

(4) Die aufgrund des Absatzes 1 gespeicherten Daten dürfen

1. für eine Auskunft nach § 174 Absatz 1 Satz 3 oder

2. zur Erlangung von Teilnehmerdaten gemäß der Verordnung (EU) 2023/1543

   a) für die Erfüllung einer Europäischen Herausgabeanordnung oder

   b) für eine die Herausgabe nach Buchstabe a vorbereitende Europäischen Sicherungsanordnung

verwendet werden, wobei ein leistungsfähiges technisches Verfahren einzusetzen ist, das die getrennte Speicherung nach Absatz 3 Nummer 2 nicht beeinträchtigt. Für andere Zwecke dürfen die aufgrund des Absatzes 1 gespeicherten Daten nicht verwendet werden. Für Auskünfte nach § 174 Absatz 1 Satz 3 ist das leistungsfähige technische Verfahren nach § 174 Absatz 7 zu verwenden.

(5) In der Rechtsverordnung nach § 170 Absatz 5 können Regelungen zur näheren Ausgestaltung der Pflichten nach Absatz 3, einschließlich Vorgaben zu den eingesetzten Systemen, Verfahren und technischen Einrichtungen zur Speicherung der Daten nach Absatz 1, getroffen werden. Technische Einzelheiten zur Umsetzung dieser Pflichten werden in der Technischen Richtlinie nach § 170 Absatz 6 festgelegt. Verpflichtete nach Absatz 1 haben der Bundesnetzagentur unverzüglich nach Aufnahme des Dienstes unter Vorlage von Unterlagen mitzuteilen, wie die Vorgaben

nach Absatz 3 sowie der Rechtsverordnung nach Satz 1 und § 170 Absatz 5 sowie der Technischen Richtlinie nach Satz 2 und § 170 Absatz 6 in ihren Anlagen umgesetzt werden. Änderungen sind der Bundesnetzagentur unverzüglich mitzuteilen. Die Bundesnetzagentur überprüft regelmäßig die Umsetzung der Vorgaben."

3. § 228 wird wie folgt geändert:

a) Absatz 2 wird wie folgt geändert:

a%6) In Nummer 38 wird die Angabe „oder § 181 Satz 2" gestrichen.

b%6) Nummer 39 wird durch die folgende Nummer 39 ersetzt:

„39. entgegen § 168 Absatz 1 Satz 1, § 170 Absatz 1 Nummer 3 Buchstabe a, Absatz 2 Nummer 2 oder Absatz 3 Satz 1, § 176 Absatz 4 Satz 3 oder 4 oder § 177 Absatz 2 Nummer 2 oder Absatz 5 Satz 3 oder 4 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,".

c%6) Die Nummern 56 bis 60 werden durch die folgenden Nummern 56 bis 60a ersetzt:

1. „ entgegen § 174 Absatz 6 Satz 1 Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

2. entgegen § 174 Absatz 6 Satz 2, auch in Verbindung mit § 175 Absatz 4, oder entgegen § 176 Absatz 3 Stillschweigen nicht wahrt,

1. entgegen § 176 Absatz 2 Nummer 1 oder § 177 Absatz 2 Nummer 1 oder Absatz 3 Nummer 1 nicht sicherstellt, dass Daten geschützt werden,

2. entgegen § 176 Absatz 2 Nummer 2 oder 3 oder § 177 Absatz 3 Nummer 2 oder 3 nicht sicherstellt, dass Daten in der dort genannten Weise gespeichert werden,

3. entgegen § 176 Absatz 2 Nummer 4 oder § 177 Absatz 3 Nummer 4 nicht sicherstellt, dass Daten gelöscht werden,

60a. entgegen § 177 Absatz 1 Satz 1 oder 2 Daten nicht oder nicht für die vorgeschriebene Dauer speichert,".

b) Absatz 6 wird wie folgt geändert:

a%6) In Nummer 2 wird die Angabe „54 und 57 bis 59" durch die Angabe „54, 56, 58, 60 und 60a" ersetzt.

b%6) In Nummer 3 wird die Angabe „50, 53 und 60" durch die Angabe „50, 53 und 59" ersetzt.

c%6) In Nummer 5 wird die Angabe „56" durch die Angabe „57" ersetzt.

4. Nach § 230 Absatz 16 wird der folgende Absatz 17 eingefügt:

(1) „ Die Vorgaben des § 177 sind spätestens ab dem … [einsetzen: sechs Monate nach dem Datum des Inkrafttretens nach Artikel 13 dieses Gesetzes] zu erfüllen.“

Artikel 7

Änderung der Telekommunikations-Überwachungsverordnung

Die Telekommunikations-Überwachungsverordnung in der Fassung der Bekanntmachung vom 11. Juli 2017 (BGBl. I S. 2316), die zuletzt durch Artikel 11 des Gesetzes vom 9. Januar 2026 (BGBl. 2026 I Nr. 7) geändert worden ist, wird wie folgt geändert:

1. § 2 wird wie folgt geändert:

   a) Nummer 1 Buchstabe b wird durch den folgenden Buchstaben b ersetzt:

      a) „im Sinne des Teils 4 die Anordnung zur Erteilung von Auskünften über Verkehrsdaten nach § 100g Absatz 1 bis 4 in Verbindung mit § 101a Absatz 1 Satz 1 Nummer 1 der Strafprozessordnung, § 20 Absatz 1 Satz 1 Nummer 5 des MAD-Gesetzes, § 8a Absatz 1 Satz 1 Nummer 4 des Bundesverfassungsschutzgesetzes, auch in Verbindung mit § 3 Absatz 1 des BND-Gesetzes, § 52 Absatz 1 des Bundeskriminalamtgesetzes, § 25 Absatz 1 des Bundespolizeigesetzes, § 77 Absatz 1 des Zollfahndungsdienstgesetzes oder nach Landesrecht;“.

   b) Nummer 3 Buchstabe b wird durch den folgenden Buchstaben b ersetzt:

      a) „im Sinne des Teils 4 die Stelle, die nach § 100g in Verbindung mit § 101a Absatz 1 und 5 sowie § 100a Absatz 4 Satz 1 der Strafprozessordnung, § 20 Absatz 1 Satz 1 Nummer 5 des MAD-Gesetzes, § 8a Absatz 1 Satz 1 Nummer 4 des Bundesverfassungsschutzgesetzes, auch in Verbindung mit § 3 des BND-Gesetzes, § 52 des Bundeskriminalamtgesetzes, § 25 Absatz 1 des Bundespolizeigesetzes, § 77 des Zollfahndungsdienstgesetzes oder nach Landesrecht aufgrund der jeweiligen Anordnung berechtigt ist, Auskunftsverlangen über Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes zu stellen;“.

2. In § 32 Absatz 1 Satz 1 wird nach der Angabe „Telekommunikationsgesetzes“ die Angabe „und des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes“ eingefügt.

3. § 35 wird wie folgt geändert:

   a) In Satz 2 wird nach der Angabe „Telekommunikationsgesetzes“ die Angabe „ oder des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes“ eingefügt.

   b) Satz 3 Nummer 4 wird durch die folgende Nummer 4 ersetzt:

      1. „die Angabe der Rechtsgrundlage, aufgrund der die beauskunfteten Verkehrsdaten gespeichert wurden,“.

Artikel 8

Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes

Das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 3 des Gesetzes vom 10. März 2026 (BGBl. 2026 I Nr. 64) geändert worden ist, wird wie folgt geändert:

§ 13a wird durch den folgenden § 13a ersetzt:

„§ 13a

Erfüllung von Pflichten gemäß den Artikeln 10 und 11 der Verordnung (EU) 2023/1543

(1) Anbieter von Telekommunikationsdiensten und die von ihnen gemäß § 3 Absatz 1 bis 3 des Elektronische-Beweismittel-Umsetzungs-und-Durchführungsgesetzes benannten Adressaten dürfen personenbezogene Daten verarbeiten, soweit dies zur Erfüllung einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung gemäß der Verordnung (EU) 2023/1543 in der Fassung vom 12. Juli 2023 erforderlich ist. Das Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes) wird insoweit eingeschränkt.

(2) § 176 Absatz 2 Nummer 2 bis 4 des Telekommunikationsgesetzes ist auf die nach Absatz 1 gesicherten personenbezogenen Daten entsprechend mit der Maßgabe anzuwenden, dass eine unverzügliche und irreversible Löschung der Daten zu erfolgen hat sobald die Datensicherung gemäß der Verordnung (EU) 2023/1543 nicht mehr erforderlich ist.“

Artikel 9

Änderung des Bundespolizeigesetzes

Das Bundespolizeigesetz … [Artikel 1 des Entwurfs eines Gesetzes zur Modernisierung des Bundespolizeigesetzes, Bundestagsdrucksache 21/3051] wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 25 die folgende Angabe eingefügt:

   „§ 25a Sicherung von Verkehrsdaten“.

2. § 25 wird wie folgt geändert:

   a) In Absatz 1 wird in der Angabe vor Nummer 1 nach der Angabe „Verkehrsdaten“ die Angabe „nach § 3 Nummer 70 des Telekommunikationsgesetzes“ eingefügt.

   b) Absatz 4 Nummer 2 wird durch die folgende Nummer 2 ersetzt:

      1. „die Rufnummer oder eine andere Kennung des betroffenen Anschlusses oder Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, oder bei der

Sicherung von Daten einer Funkzelle, sofern andernfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre, eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation,“.

c) Absatz 5 Satz 2 Nummer 2 wird durch die folgende Nummer 2 ersetzt:

1. „die Rufnummer oder eine andere Kennung des betroffenen Anschlusses oder Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, oder bei der Sicherung von Daten einer Funkzelle, sofern andernfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre, eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation,“.

d) Absatz 6 wird durch den folgenden Absatz 6 ersetzt:

(1) „ Der auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 Verpflichtete hat die zur Auskunftserteilung erforderlichen Daten unverzüglich und vollständig zu übermitteln. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung.“

3. Nach § 25 wird der folgende § 25a eingefügt:

„§ 25a

Sicherung von Verkehrsdaten

(1) Die Bundespolizei kann zum Zwecke einer etwaigen Erhebung von Verkehrsdaten nach § 25 Absatz 1 anordnen, dass Verpflichtete nach § 25 Absatz 1 Verkehrsdaten von betroffenen Personen unverzüglich zu sichern haben, wenn die betroffene Person in einem persönlichen oder räumlichen Bezug zu der Gefahr oder zu verhütenden Straftat nach § 25 Absatz 1 steht und

1. tatsächliche Anhaltspunkte dafür vorliegen, dass es sich um eine Person im Sinne des § 25 Absatzes 1 handelt und eine Erhebung nach § 25 Absatz 1 gerechtfertigt sein könnte, oder

2. tatsächliche Anhaltspunkte dafür vorliegen, dass es sich um eine Person handelt, die mit einer Person nach § 25 Absatz 1 Nummer 2 oder 3 in nicht nur flüchtigem oder zufälligem Kontakt und in einer Weise in Verbindung steht, welche die Annahme rechtfertigt, dass nach Gewinnung weiterer Erkenntnisse eine Erhebung nach § 25 Absatz 1 gerechtfertigt sein könnte.

Die Daten müssen für die in § 25 Absatz 1 jeweils genannten Zwecke von Bedeutung sein können.

(2) Die Anordnung nach Absatz 1 Satz 1 darf nur durch die Präsidentin oder den Präsidenten des Bundespolizeipräsidiums oder einer Bundespolizeidirektion, ihrer oder seiner Vertretung oder von der Leiterin oder dem Leiter einer Abteilung des Bundespolizeipräsidiums getroffen werden. Die Anordnung ergeht ohne Anhörung der betroffenen Person. Die Anordnung wird mit Erlass wirksam. Sie ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Namen und Anschrift,

2. die Rufnummer oder eine andere Kennung des betroffenen Anschlusses oder Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, oder bei der Sicherung von Daten einer Funkzelle, sofern andernfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre, eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation,

3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes,

4. Art der durch die Maßnahme zu erhebenden Daten und ihre voraussichtliche Bedeutung für den Zweck der Erhebung und

5. die wesentlichen Gründe.

Die Anordnung ist auf höchstens 3 Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als 3 weitere Monate durch das Gericht auf Antrag der nach Satz 1 Anordnungsberechtigten ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Zuständig ist das Amtsgericht, in dessen Bezirk die Behörde der Antragsberechtigten nach Satz 1 ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Buches 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit mit Ausnahme der § 23 Absatz 2, § 37 Absatz 2 und § 41 entsprechend. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(3) Der auf Grund einer Anordnung nach Absatz 1 Verpflichtete hat die von der Anordnung erfassten Daten unverzüglich und vollständig zu sichern. § 25 Absatz 6 Satz 2 und Absatz 7 gilt entsprechend.“

Artikel 10

Änderung des Vereinsgesetzes

Das Vereinsgesetz vom 5. August 1964 (BGBl. I S. 593), das zuletzt durch Artikel 5 des Gesetzes vom 30. November 2020 (BGBl. I S. 2600) geändert worden ist, wird wie folgt geändert:

§ 4 Absatz 4 wird wie folgt geändert:

1. Satz 1 wird durch den folgenden Satz ersetzt:

„Für die Beschlagnahme von Gegenständen, die als Beweismittel von Bedeutung sein können, gelten die §§ 94 bis 97, 98 Absatz 4 sowie die §§ 99, 100, 101 der Strafprozessordnung entsprechend.“

2. Satz 4 wird durch den folgenden Satz ersetzt:

„Die §§ 104, 105 Absatz 2 und 3, die §§ 106 bis 110, 111c, 111n bis 111p der Strafprozessordnung gelten entsprechend.“

Artikel 11

Änderung des Geldwäschegesetzes

Das Geldwäschegesetz vom 23. Juni 2017 (BGBl. I S. 1822), das zuletzt durch Artikel 53 des Gesetzes vom 4. Februar 2026 (BGBl. 2026 I Nr. 33) geändert worden ist, wird wie folgt geändert:

In § 29 Absatz 2a Satz 2 Nummer 2 wird die Angabe „100k Absatz 1 Satz 2, den §§“ durch die Angabe „100k,“ ersetzt.

Artikel 12

Einschränkung eines Grundrechts

Durch Artikel 1 Nummer 2 und 3, Artikel 6 Nummer 2 sowie Artikel 9 Nummer 3 wird das Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes) eingeschränkt.

Artikel 13

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

EU-Rechtsakte:

Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl. L 191 vom 28.7.2023, S. 118)

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Das gesellschaftliche Leben ist ohne den digitalen Raum nicht mehr zu denken. Diese Entwicklung betrifft auch die Kriminalität. Straftaten weisen häufig digitale Bezüge auf, etwa wenn zwei Tatverdächtige miteinander über einen Messengerdienst kommunizieren, um einen terroristischen Anschlag zu planen. Oder die Straftaten finden vollständig in digitaler Umgebung statt, etwa indem Täter Kinderpornographie verbreiten oder eine Handelsplattform betreiben, auf der Betäubungsmittel sowie Cybercrime-as-a-Service (CaaS) angeboten werden, oder indem sie in einem echt wirkenden Onlineshop Waren verkaufen, die gar nicht existieren (sogenannte Fakeshops).

Strafverfolgungs- und andere Ermittlungsbehörden verfügen bereits heute über Instrumente, um den Spuren nachzugehen, die Kriminelle im Internet hinterlassen. Sie können insbesondere bei Telekommunikationsdiensten – zum Beispiel Internetzugangsdiensten – und bei digitalen Diensten – zum Beispiel bei den Betreibern sozialer Netzwerke – Daten erheben.

Allerdings sind Daten nicht selten flüchtig. Bei Straftaten, die im oder mithilfe des Internets begangen werden, hinterlassen Täter zumeist die von ihnen verwendete Internetprotokoll-Adresse (IP-Adresse) als Spur. Diese Adresse einem Anschlussinhaber zuzuordnen stellt – insbesondere bei ausschließlich im Internet begangenen Straftaten – häufig den einzigen Ermittlungsansatz dar. Wenn eine Strafverfolgungsbehörde oder eine andere berechtigte Stelle den Anschlussinhaber zu einer IP-Adresse ermitteln möchte, dann wendet sie sich mit einer sogenannten Bestandsdatenabfrage an den Internetzugangsdiensteanbieter. Die Abfrage hat aber nur dann Erfolg, wenn der Anbieter die Zuordnung zwischen IP-Adresse und Anschlussinhaber noch gespeichert hat. Dies ist – wenn überhaupt – nur wenige Tage der Fall, da Internetzugangsdiensteanbieter bislang diese Daten nur speichern, soweit und solange dies für ihre betrieblichen Zwecke erforderlich ist. So verlaufen viele Ermittlungen ergebnislos, oder die Behörden müssen auf andere, sehr viel aufwändigere und teilweise auch eingriffsintensivere Ermittlungsmethoden zurückgreifen.

In der Vergangenheit hat es mehrere Versuche gegeben, eine Vorratsdatenspeicherung von Verkehrs- und Standortdaten zu Zwecken der Strafverfolgung und Gefahrenabwehr einzuführen, zuletzt mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218). Im Rahmen eines vom Bundesverwaltungsgericht angestrengten Vorabentscheidungsverfahrens hat der Europäische Gerichtshof mit Urteil vom 20. September 2022 – C-793/19 und C-794/19, Spacenet und andere – entschieden, dass Regelungen wie die 2015 in Deutschland eingeführten nicht mit dem Unionsrecht vereinbar sind. Daraufhin hat das Bundesverwaltungsgericht am 14. August 2023 – 6 C 6.22 – geurteilt, dass die maßgeblichen Regelungen des Telekommunikationsgesetzes mit europäischem Recht unvereinbar sind und nicht mehr angewendet werden dürfen. Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen hatte bereits mit Beschluss vom 22. Juni 2017 – 13 B 238/17 – zugunsten eines Internetzugangsdienstes vorläufig festgestellt, dass keine Verpflichtung bestand, Verkehrsdaten ihrer Kunden auf Grundlage des 2015 eingeführten Gesetzes zu speichern.

Um den Strafverfolgungsbehörden und anderen berechtigten Stellen zu ermöglichen, zuverlässig Anschlussinhaber anhand einer IP-Adresse zu identifizieren, ist es notwendig, aber auch ausreichend, eine Pflicht zur Speicherung von IP-Adressen einzuführen. Diese vorsorgliche IP-Adressspeicherung hält sich im Rahmen desjenigen, was der Europäische Gerichtshof in seinem Urteil vom 30. April 2024 (Rechtssache C-470/21, Quadrature du Net II – Hadopi) für zulässig erachtet hat. Die bereits heute mögliche Bestandsdatenabfrage wird damit um ein Vielfaches ergiebiger werden. Die Behörden können damit ein Instrument nutzen, das es ihnen erlaubt, dem häufig einzigen, aber nahezu immer ersten, effizientesten und schnellsten Ermittlungsansatz zu folgen.

Darüber hinaus wird für Verkehrsdaten das Instrument der Sicherungsanordnung geschaffen. Damit können Strafverfolgungsbehörden und die Bundespolizei die Sicherung von Verkehrsdaten veranlassen, sofern und solange die rechtlichen oder tatsächlichen Voraussetzungen einer Datenerhebung zu Zwecken der Strafverfolgung noch nicht vorliegen. Die Verordnung (EU) 2023/1543 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (E-Evidence-Verordnung) setzt voraus, dass es das Instrument der Sicherungsanordnung für Zwecke der Strafverfolgung im nationalen Recht gibt. Sie einzuführen ist daher auch für grenzüberschreitende Fälle von Relevanz.

Ferner besteht Bedarf für eine Klarstellung, welche Eingriffsschwelle für die sogenannte Funkzellenabfrage gilt. Der Bundesgerichtshof hat mit Beschluss vom 10. Januar 2024 – 2 StR 171/23 – entschieden, dass eine Funkzellenabfrage den Verdacht einer besonders schweren Straftat voraussetze. Die Schwelle wird nunmehr gesetzlich dahingehend bestimmt, dass eine Straftat von erheblicher Bedeutung genügt.

II. Wesentlicher Inhalt des Entwurfs

Mit dem Entwurf werden die Befugnisse der Strafverfolgungsbehörden in maßvoller Weise an die Erfordernisse der Gegenwart anpasst.

Nach dem Entwurf werden Internetzugangsdiensteanbieter erstens verpflichtet, für drei Monate die von ihnen an Endkunden vergebenen IP-Adressen und weitere Daten wie die Portnummer zu speichern, sofern dies für eine eindeutige Zuordnung der IP-Adresse zu einem Anschlussinhaber erforderlich ist. Dadurch können Strafverfolgungsbehörden und andere berechtigte Stellen anhand eines Zeitstempels, einer IP-Adresse und gegebenenfalls einer Portnummer die Bestandsdaten beim Internetzugangsdiensteanbieter abfragen, sofern die gesetzlichen Voraussetzungen dafür vorliegen. Der Entwurf deckt damit einen wesentlichen Bedarf der Behörden. Die Speicherpflicht betrifft zwar alle Nutzer von Internetzugangsdiensten in Deutschland. Allerdings lassen die Daten nichts anderes zu als die Identifizierung des Anschlussinhabers anhand einer IP-Adresse. Es handelt sich gerade nicht um eine Vorratsdatenspeicherung von allen Verkehrs- und Standortdaten. Aus den gespeicherten IP-Adressdaten lassen sich insbesondere keine Surf- oder Bewegungsprofile erstellen. Die Beeinträchtigung insbesondere der unbescholtenen Nutzer ist damit überschaubar. Zugleich werden die Behörden entlastet, denn bei der Bestandsdatenabfrage handelt es sich um ein Ermittlungsinstrument, das geeignet ist, mit verhältnismäßig geringem Aufwand einen werthaltigen Ermittlungsansatz zu erlangen. Ansonsten müssten sie deutlich aufwändigere Maßnahmen ergreifen, zum Beispiel Recherchen im offenen Internet durchführen (sogenannte OSINT-Suchen). Diese Maßnahmen verlaufen nicht nur häufig ergebnislos, sondern können auch unbescholtene Bürger betreffen und sind zum Teil eingriffsintensiver als die Bestandsdatenabfrage. Die Bestandsdatenabfrage wird mit dem vorliegenden Entwurf im Ermittlungsverfahren aussichtsreicher und kann zielgenau erfolgen.

Die Einführung einer Speicherpflicht steht in Einklang mit Verfassungsrecht. Die vorsorgliche Speicherung allein der Telekommunikationsverkehrsdaten, die erforderlich sind, um den Anschlussinhaber zu einer anderweitig ermittelten dynamischen IP-Adresse beauskunften zu können, hat ein erheblich weniger belastendes Eingriffsgewicht als eine nahezu vollständige Speicherung der Daten sämtlicher Telekommunikationsverbindungen (vergleiche Bundesverfassungsgericht, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, Randnummer 257). Der Entwurf ist so ausgestaltet, dass er dem Gewicht des mit der Speicherpflicht verbundenen Eingriffs Rechnung trägt.

Die Einführung der genannten Speicherpflicht ist mit dem Recht der Europäischen Union vereinbar. Bei der gewählten Ausgestaltung stellt sie keinen schwerwiegenden Eingriff dar und ist durch das Ziel, Straftaten zu bekämpfen, gerechtfertigt (vergleiche Europäischer Gerichtshof, Urteil vom 30. April 2024, Rechtssache C-470/21, Quadrature du Net II – Hadopi, Randnummern 82 f., 101 und 115).

Zweitens sieht der Entwurf die Einführung des Instruments der Sicherungsanordnung vor. Damit können Strafverfolgungsbehörden und die Bundespolizei gegenüber Telekommunikationsunternehmen die Sicherung von Verkehrsdaten anordnen, wenn die Erhebungsvoraussetzungen aus rechtlichen oder tatsächlichen Gründen (noch) nicht vorliegen. Da das Instrument schnell eingesetzt werden kann, besteht die Aussicht, dass die Behörden so die Löschung flüchtiger Daten in Zusammenhang mit einer konkreten, bekannt gewordenen Straftat verhindern und damit für ihre weiteren Ermittlungen künftig auf diese Daten zugreifen können.

Vorgesehen ist drittens die ausdrückliche Regelung, dass eine Funkzellenabfrage zulässig ist bei Straftaten von erheblicher Bedeutung, insbesondere solchen nach § 100a Absatz 2 der Strafprozessordnung (StPO). Hiervon war die überwiegende Praxis der Strafverfolgung bis zu einer Entscheidung des Bundesgerichtshofs von 10. Januar 2024 – 2 StR 171/23 – ausgegangen. Mit dem Entwurf wird diese Handhabung wieder ermöglicht.

Mit dem Entwurf werden außerdem die Regelungen der europarechtswidrigen Vorratsdatenspeicherung und hierauf bezogene Abrufbefugnisse gestrichen. Der Entwurf enthält ferner eine systematische Neuordnung der §§ 100g, 100j und 100k StPO sowie der in § 101a StPO enthaltenen hierauf bezogenen Verfahrensvorschriften.

Mit der Anpassung des Justizvergütungs- und -entschädigungsgesetzes (JVEG) wird sichergestellt, dass die zur Umsetzung einer Sicherungsanordnung verpflichteten Unternehmen für den ihnen im Einzelfall anfallenden Aufwand angemessen entschädigt werden.

Die Folgeänderungen im Telekommunikationsgesetz (TKG) und in der Telekommunikations-Überwachungsverordnung (TKÜV) dienen dazu, die aus der neuen Sicherungsanordnung folgenden Speicherungs-, Übermittlungs- und Löschungspflichten für die Anbieter von Telekommunikationsdiensten zu regeln.

Im Übrigen enthält das Gesetz vor allem Folgeanpassungen in weiteren Gesetzen.

III. Exekutiver Fußabdruck

In der Erarbeitungsphase sind die Internetzugangsdiensteanbieter mit eigenen Netzen (Deutsche Telekom AG, Telefónica Germany GmbH & Co. OHG, Vodafone GmbH und 1&1 Telecommunication SE) zur technischen Machbarkeit der in Ausblick genommenen Regelungen konsultiert worden. Der Inhalt des Entwurfs ist durch Äußerungen der Unternehmensvertreter nicht wesentlich beeinflusst worden.

IV. Alternativen

Keine.

V. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes ergibt sich aus Artikel 74 Absatz 1 Nummer 1 des Grundgesetzes (gerichtliches Verfahren), Nummer 3 (Vereinsrecht) sowie aus Artikel 73 Absatz 1 Nummer 5 (Grenzschutz), 6 (Luftverkehr), 6a (Eisenbahnen) und 7 (Telekommunikation).

VI. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Entwurf steht mit dem Recht der Europäischen Union und mit völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, im Einklang.

Die vorsorgliche IP-Adressspeicherung hält sich unter den im Entwurf genannten Voraussetzungen im Rahmen desjenigen, was der Europäische Gerichtshof in seinem Urteil vom 30. April 2024 (Rechtssache C-470/21, Quadrature du Net II – Hadopi) für zulässig erachtet hat.

Die Einführung einer Sicherungsanordnung passt außerdem das nationale Strafverfahrens-recht an die Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren an. Artikel 6 der Verordnung sieht eine Europäische Sicherungsanordnung vor. Gemäß Artikel 6 Absatz 3 ist für den Erlass Voraussetzung, dass sie in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen hätte erlassen werden können. Die Ausgestaltung im deutschen Recht berücksichtigt die Anforderungen des Europäischen Gerichtshofs an eine Sicherungsanordnung, wie er sie insbesondere in seinem Urteil vom 6. Oktober 2020 (verbundene Rechtssachen C-511/18, C-512/18 und C-520/18, Quadrature du Net I) niedergelegt hat. So erfolgt die Sicherungsanordnung insbesondere anlassbezogen und ist in sachlicher Hinsicht beschränkt.

Darüber hinaus enthält auch das von Deutschland unterzeichnete und ratifizierte Übereinkommen des Europarats über Computerkriminalität, die sogenannte Budapest-Konvention, in Artikel 16 eine Verpflichtung der Vertragsstaaten, die zuständigen Behörden zu ermächtigen, die umgehende Sicherung von Verkehrsdaten anzuordnen. Diese Verpflichtung wird mit Einführung der Sicherungsanordnung umgesetzt.

VII. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Im Telekommunikationsgesetz werden die Vorschriften zur Vorratsdatenspeicherung, die mit europäischem Recht unvereinbar sind, aufgehoben. Dies gilt auch für die hierauf bezogene Abrufbefugnis in der Strafprozessordnung. Dies führt zur Vereinfachung des Rechts. Außerdem werden die in der Strafprozessordnung geregelten Befugnisse der Strafverfolgungsbehörden für den Abruf von Bestands-, Verkehrs- und Nutzungsdaten insgesamt neu gefasst und damit praktisch besser handhabbar.

2. Nachhaltigkeitsaspekte

Die beabsichtigte Einführung der Sicherungsanordnung trägt zur Verwirklichung von Ziel 16 „Friedliche und inklusive Gesellschaften für eine nachhaltige Entwicklung fördern, allen Menschen Zugang zur Justiz ermöglichen und leistungsfähige, rechenschaftspflichtige und inklusive Institutionen auf allen Ebenen aufbauen“ der Agenda 2030 für nachhaltige Entwicklung bei. Dieses Nachhaltigkeitsziel verlangt mit seinen Zielvorgaben 16.1, 16.2, 16.4 und 16.5, alle Formen der Gewalt und die gewaltbedingte Sterblichkeit überall deutlich zu verringern, alle Formen von Gewalt gegen Kinder zu beenden, alle Formen organisierter Kriminalität zu bekämpfen und Korruption und Bestechung erheblich zu reduzieren. Die vorsorgliche IP-Adressspeicherung und die Sicherungsanordnung leisten einen Beitrag zur Erreichung dieser Ziele, indem sie die Erfassung und Verwertung digitaler Spuren ermöglicht, die für die Strafverfolgung bisher nicht in diesem Umfang zugänglich waren.

Der Entwurf folgt damit den Prinzipien der Deutschen Nachhaltigkeitsstrategie „(1.) Nachhaltige Entwicklung als Leitprinzip konsequent in allen Bereichen und bei allen Entscheidungen anwenden“, „(2.) Global Verantwortung wahrnehmen“ und „(5.) Sozialen Zusammenhalt in einer offenen Gesellschaft wahren und verbessern“.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Im Haushalt des Bundes sind nachfolgende Mehrbedarfe zu erwarten. Die Berechnung der Bedarfe erfolgt entsprechend den Vorgaben zur Veranschlagung von Ausgaben und (Plan-) Stellen im Bundeshaushalt.

Im Haushalt des Bundesministeriums des Innern, Einzelplan 06, entstehen beim Bundesamt für Verfassungsschutz zusätzliche Personal- und Sachkosten ab dem Haushaltsjahr 2027. Für die notwendigen technischen Anpassungen im Bereich der IT-Infrastruktur (Netzübergänge, Netzwerktechnik, elektronische Schnittstellen) entstehen im Haushaltsjahr 2027 rund 254 000 Euro einmalige Sachkosten. Für den laufenden Betrieb entstehen ab 2027 jährliche Sachkosten in Höhe von 177 000 Euro. Die erforderlichen technischen Anpassungen und der laufende Betrieb sind nach derzeitigen Schätzungen mit einem zusätzlichen Personalmehrbedarf von vier (Plan-)Stellen (1 A14, 1 A12, 1 A11, 1 E9a) verbunden. Die zusätzlichen jährlichen Personalkosten betragen 372 000 Euro.

Im Haushalt des Bundesministeriums der Justiz und für Verbraucherschutz, Einzelplan 07, werden beim Bundesgerichtshof (BGH) und bei dem Generalbundesanwalt beim Bundesgerichtshof (GBA) ab dem Jahr 2027 minimale zusätzliche Sachkosten entstehen. Es ist bei BGH und GBA insgesamt von rund drei Sicherungsanordnungen pro Jahr auszugehen. Bei durchschnittlichen Kosten einer Entschädigung nach Nummer 500 bis 507 und 600 der Anlage 3 zum JVEG in Höhe von 105 Euro ergeben sich prognostizierte zusätzliche Sachkosten von weit unter 1 000 Euro pro Jahr.

Zusätzliche Sachkosten oder Personalkosten im Haushalt des Bundesministeriums der Finanzen sind nicht zu erwarten. Die zusätzlichen Stellenbedarfe bei den Behörden der Zollverwaltung (Zollfahndungsdienst und Zollkriminalamt) betragen in der Summe weniger als 0,5 Stellen und sind damit nicht mehr präzise ermittelbar.

Der zuvor dargestellte Mehrbedarf sowie etwaiger sonstiger Mehrbedarf soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Im Haushalt des Bundesministeriums für Wirtschaft und Energie, Einzelplan 09, entsteht bei der Bundesnetzagentur ab dem Haushaltsjahr 2027 für die Aufsichtsaufgaben und für zusätzliche Bußgeldverfahren geschätzt ein Personalmehrbedarf in Höhe von insgesamt 26,0 Planstellen (1 A16, 1 A15, 1 A14, 1 A13gZ, 3 A13g, 5 A12, 5 A11, 1 A10, 1 A9mZ, 2 A9m, 3 A8, 1 A7, 1 A6m). Für die Fachaufgaben entstehen somit zusätzliche jährliche

Personalkosten in Höhe von insgesamt 2,376 Mio. Euro, Sacheinzelkosten in Höhe von 891 000 Euro sowie Gemeinkosten in Höhe von 960 000 Euro. Für die zusätzlichen Querschnittsaufgaben sind weitere 7,8 Stellen erforderlich (jeweils 0,3 A16, A15, A14 und A13gZ, 0,9 A13g, jeweils 1,5 A12 und A11, jeweils 0,3 A10 und A9mZ, 0,6 A9m, 0,9 A8 und jeweils 0,3 A7 und A6m). Die zusätzlichen Personal- und Sachkosten für die Querschnittsaufgaben sind in den Gemeinkosten enthalten.

Hinzu kommen im Jahr 2027 einmalige Sachkosten in Höhe von 25 000 Euro für die Erweiterung der bestehenden Laboranlage sowie ab dem Haushaltsjahr 2027 jährliche Sachkosten in Höhe von 5 000 Euro.

Im Einzelplan 09 sind zudem zusätzliche Einnahmen durch zusätzliche Bußgeldverfahren zu erwarten. Die Höhe der Einnahmen hängt von der Anzahl der Bußgeldverfahren und der Höhe der verhängten Bußgelder ab. Sie lassen sich daher nicht prognostizieren.

Der stellenmäßige Mehrbedarf soll im Einzelplan 09 ausgeglichen werden. Der finanzielle Mehrbedarf soll in den jeweiligen Einzelplänen ausgeglichen werden.

In den Haushalten der Länder ist insgesamt mit Minderbedarfen von insgesamt 1,429 Mio. Euro zu rechnen. Den prognostizierten Mehrbedarfen für zusätzliche Bestandsdatenauskünfte in Höhe von rund 172 000 Euro (11 773 zusätzliche Anfragen x 15 Euro Entschädigung nach Nummer 201 der Anlage 3 zum JVEG) und den Mehrbedarfen für Sicherungsanordnungen in Höhe von 120 000 Euro (1 134 Anordnungen x durchschnittliche Entschädigung in Höhe von 105 Euro nach Nummer 500 bis 507 und 600 der Anlage 3 zum JVEG) stehen Einsparungen gegenüber infolge der abgesenkten Entschädigungshöhe bei Bestandsdatenauskünften (jährlich 57 367) von 45 Euro auf 15 Euro nach Nummer 201 der Anlage 3 zum JVEG. Diese Einsparungen werden voraussichtlich rund 1,721 Mio. Euro betragen.

Auswirkungen auf die Haushalte der Gemeinden sind nicht zu erwarten.

4. Erfüllungsaufwand

a) Erfüllungsaufwand für Bürgerinnen und Bürger und für die Wirtschaft

Keiner.

b) Erfüllungsaufwand der Verwaltung

Keiner.

5. Weitere Kosten

Die Regelungen zur IP-Adressspeicherung und Einführung einer Sicherungsanordnung für Verkehrsdaten betreffen den justiziellen Kernbereich. Es ist davon auszugehen, dass die Auswirkungen sowohl für den Bund als auch für die Länder überwiegend kostenneutral sind. Für die Wirtschaft entstehen weitere Kosten. Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau für Telekommunikationsdienste, sind im Übrigen nicht zu erwarten. Im Einzelnen:

a) Länder

aa) Funkzellenabfrage

Hinsichtlich der Funkzellenabfrage ist nennenswerter Mehraufwand nicht zu erwarten. Die überwiegende Praxis ist bis Januar 2024 davon ausgegangen ist, dass die Maßnahme bei

Straftaten von erheblicher Bedeutung, insbesondere solchen nach § 100a Absatz 2 StPO, eingesetzt werden kann. Dies stellt der Entwurf nun ausdrücklich klar.

bb) IP-Adressspeicherung

Im Hinblick auf die Bestandsdatenauskunft nach § 100j Absatz 2 StPO ist zwar wegen der Einführung einer dreimonatigen IP-Adressspeicherung damit zu rechnen, dass sich das Aufkommen von Auskunftsersuchen erhöht. Im Hinblick auf den damit einhergehenden unmittelbar hervorgerufenen Aufwand ist aber davon auszugehen, dass der Entwurf kostenneutral ist.

Als unmittelbar hervorgerufener Sachaufwand sind nur die Entschädigungspflichten nach Nummer 201 der Anlage 3 zum JVEG zu betrachten. Die erwartbare Erhöhung des Aufkommens von Auskunftsersuchen löst zwar zusätzliche Entschädigungspflichten aus. Neutralisierend steht dem jedoch die Reduktion der Entschädigungshöhe von 45 Euro auf 15 Euro je Auskunft gegenüber.

Für die Schätzung der zukünftigen Erhöhung des Aufkommens an Auskunftsersuchen steht keine breite Datenbasis zur Verfügung. Die Länder konnten nicht mitteilen, in wie vielen Verfahren in der Vergangenheit zusätzlich eine Bestandsdatenauskunft anhand einer IP-Adresse durchgeführt worden wäre, wenn eine dreimonatige Speicherpflicht bereits bestanden hätte. Sie konnten auch überwiegend keine Angaben dazu machen, wie viele Bestandsdatenauskünfte in wie vielen Verfahren durchgeführt worden wären beziehungsweise sie dem Grunde nach rechtlich möglich gewesen wären. Eine statistische Erfassung dieser Werte ist nicht vorsehen, eine nachträgliche Erhebung hätte unverhältnismäßigen Aufwand bedeutet.

Eine Schätzung kann aber anhand der von Nordrhein-Westfalen geschätzten Zahlen an Bestandsdatenauskünften für die Jahre 2023, 2024 und 2025 vorgenommen werden. Das Land Nordrhein-Westfalen hat anhand der in dem IT-Verfahren Infreq100 gespeicherten Zahlen geschätzt, dass im Jahr 2024 13 277 (2023: 13 144; 2025: 11 431) Bestandsdatenauskünfte für die Zwecke der Strafverfolgung durchgeführt worden sind. Die in Rede stehenden Bestandsdatenabfragen anhand des Kriteriums einer IP-Adresse (BDA-IP) erfolgen bei der dortigen Polizei über die Elektronische Schnittstelle Behörde (ESB), hier dem IT-Verfahren Infreq100, soweit die Verpflichteten aufgrund der TKÜV ebenfalls zur Teilnahme an der ESB verpflichtet oder an diese angebunden sind. BDA-IP-Abfragen, welche nicht über die ESB erfolgen, bewegen sich aufgrund der Erfahrungswerte in Nordrhein-Westfalen quantitativ im marginalen Bereich. In der Übersicht der Infreq100 zu den BDA-IP ist keine Unterteilung zu den einzelnen Ermittlungsverfahren gegeben, sodass keine Aussage erfolgen kann, in wie vielen unterschiedlichen Ermittlungsverfahren diese Abfragen erfolgten. Für eine bundesweite Schätzung der Anzahl der Bestandsdatenauskünfte soll daher angenommen werden, dass pro Verfahren ein Auskunftsersuchen gestellt wurde. Dies entspricht auch dem von den Telekommunikationsanbietern mitgeteilten Erfahrungswert, dass pro Verfahren typischerweise eine Kennung abgefragt wird. Setzt man die 13 277 Abfragen aus dem Jahr 2024 ins Verhältnis zur Gesamtzahl der Verfahrenseingänge bei den Staatsanwaltschaften in Nordrhein-Westfalen dieses Jahres (1 270 996), so ergibt sich ein Prozentsatz von 0,0104461383. Hochgerechnet auf alle Länder ergibt sich ausgehend von den bundesweiten Eingängen aus dem Jahr 2024 von 5 491 712 eine geschätzte Anzahl von Bestandsdatenauskünften anhand der IP-Adresse durch die Strafverfolgungsbehörden der Länder für das Jahr 2024 von 57 367.

Übereinstimmend wurde von den Ländern die Einschätzung abgegeben, dass aufgrund der Einführung einer dreimonatigen IP-Adressspeicherung mit einer erheblichen Erhöhung des Aufkommens von Auskunftsersuchen zu rechnen sei. Einen gewissen Anhaltspunkt für das Maß der Erhöhung kann die Untersuchung des Bundeskriminalamtes aus dem Jahr 2022 zu tatsächlichen und hypothetischen

Erfolgsquoten bei den dortigen Ermittlungen nach Hinweisen des National Center for Missing & Exploited Children (NCMEC) bieten (vergleiche das Positionspapier des Bundeskriminalamts zu erforderlichen Speicherfristen von IP-Adressen vom 21. Juli 2023, abrufbar unter https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html, oder auch die Stellungnahme des Bundeskriminalamts zu Bundestagsdrucksache 20/3687 vom 5. Juli 2023, abrufbar unter https://www.bundestag.de/resource/blob/970516/Stellungnahme-Link_BKA.pdf). Hiernach waren in rund 24 Prozent der 66 000 untersuchten Fälle die übermittelten IP-Adressen zum Zeitpunkt des Einganges des Hinweises älter als acht Tage (rund 15 600 Vorgänge). Geht man davon aus, dass in diesen Fällen bisher von vornherein auf eine Bestandsdatenauskunft verzichtet wurde, wäre der Anteil der Verfahren, in denen zusätzlich eine Bestandsdatenauskunft anhand einer IP-Adresse durchgeführt worden wäre, wenn eine dreimonatige Speicherpflicht gegolten hätte, mit 24 Prozent anzugeben. Allerdings wäre auch zu berücksichtigen, dass die NCMEC-Vorgänge nicht repräsentativ für alle Verfahren sind, in denen eine Bestandsdatenauskunft anhand einer IP-Adresse als Ermittlungsansatz in Betracht kommt. Bei anderen Verfahren können die IP-Adressen im Zeitpunkt der Kenntniserlangung von einem möglichen strafbaren Verhalten durch die Strafverfolgungsbehörden auch deutlich älter sein (vergleiche auch die Begründung zu Artikel 6 Nummer 2 zu § 177 Absatz 1 TKG).

Legt man auf dieser Grundlage bei der Schätzung des sich zusätzlich ergebenden Aufkommens an Bestandsdatenauskünften einen großzügigen Maßstab von einer Zunahme um circa 20 Prozent an, so ergäbe sich ausgehend von den oben genannten Zahlen für das Jahr 2024 ein Mehr an Auskunftsersuchen von 11 473. Multipliziert mit 15 Euro gemäß der geänderten Nummer 201 der Anlage 3 zum JVEG ergibt sich ein Betrag von 172 095 Euro. Wird der von den Telekommunikationsanbietern mitgeteilte Erfahrungswert, dass pro Verfahren typischerweise eine Kennung abgefragt wird, zugrunde gelegt, ergibt sich eine Mehrbelastung von 172 095 Euro, die aus den Länderhaushalten zu finanzieren sein wird. Neutralisierend steht dem jedoch die Reduktion der bisherigen Entschädigungshöhe nach Nummer 201 der Anlage 3 zum JVEG von 45 Euro auf 15 Euro entgegen, was bezogen auf geschätzte bundesweite Zahl von 57 367 Bestandsdatenauskünften anhand der IP-Adresse durch die Strafverfolgungsbehörden der Länder für 2024 zu einem Einsparvolumen von 1,721 Mio. Euro führt. Mit Blick auf die bereits nach der bisherigen Rechtslage möglichen Auskunftsersuchen ist – ausgehend von der geschätzten Zahl an Bestandsdatenauskünften für das Jahr 2024 – zukünftig von einer erheblichen Minderbelastung auszugehen. Zwar ist der Betrag von 45 Euro nach Nummer 201 der Anlage 3 zum JVEG gegenwärtig für bis zu zehn in demselben Verfahren gleichzeitig angefragte Kennungen vorgesehen, die der Auskunftserteilung zugrunde liegen, während der Entwurf einen Betrag von 15 Euro für nur bis zu drei in demselben Verfahren gleichzeitig angefragte Kennungen vorsieht. Dieser Umstand wirkt sich mit Blick auf von den Telekommunikationsanbietern mitgeteilten Erfahrungswert, dass pro Verfahren typischerweise nur eine Kennung abgefragt wird, indes faktisch nicht aus.

Unmittelbar hervorgerufener Personalmehraufwand, der nicht mit dem vorhandenen Personal erledigt werden könnte, entsteht nicht. Insbesondere ist wesentliche Tatbestandsvoraussetzung für die Bestandsdatenauskunft das Vorliegen eines Anfangsverdachts, was bereits für die Einleitung des Verfahrens zu prüfen ist.

Eine weitere Auswirkung des Entwurfs ist, dass Auskunftsersuchen anhand einer IP-Adresse zukünftig häufiger erfolgreich sein und damit zu weiteren Ermittlungsansätzen führen, die als mittelbare Effekte entsprechenden Aufwand nach sich ziehen (weitere Ermittlungen und etwaige gerichtliche Verfahren). Diese Kosten können nicht beziffert werden, denn eine Vorhersage, in wie vielen Verfahren die zusätzlichen Auskunftsersuchen mit welchen zusätzlichen Ermittlungsmaßnahmen zu einer Anklage führen werden, lässt sich nicht treffen. Hinzu kommt, dass jedes Verfahren abhängig von

den Umständen des Einzelfalls einen unterschiedlichen Umfang entwickeln kann. Setzt man allerdings die Zahl von 11 473 zusätzlichen Auskunftsersuchen ins Verhältnis zu den 561 539 bundesweit 2024 neu eingegangen Strafverfahren bei Gerichten, so wäre – unter der Annahme, dass jedes zusätzliche Auskunftsersuchen einen Ermittlungserfolg nach sich ziehen würde – höchstens mit einem Anstieg von 0,02 Prozent zu rechnen, was sich innerhalb der üblichen jährlichen Schwankungen bewegt.

Die weiteren Kosten bei den Landespolizeibehörden in ihrer Gefahrenabwehrfunktion und den Nachrichtendiensten der Länder lassen sich nicht sicher beziffern. Allerdings ist zu berücksichtigen, dass ausgehend von den aus Nordrhein-Westfalen gemeldeten Zahlen die Bestandsdatenabfragen zur Gefahrenabwehr im Verhältnis zu denjenigen für die Strafverfolgung nur einen geringen Anteil ausmachen (für das Jahr 2024 in Nordrhein-Westfalen insgesamt 13 485 Bestandsdatenabfragen und hiervon 208 zur Gefahrenabwehr). Vor diesem Hintergrund und angesichts der Senkung der Kostenpauschale für diese Auskunftsart dürfte aber – wenn überhaupt – nur mit geringfügigen weiteren Kosten zu rechnen sein.

cc) Sicherungsanordnung

Es ist davon auszugehen, dass von dem Ermittlungsinstrument der Sicherungsanordnung im Verhältnis zu den Maßnahmen zur Erhebung der Daten nach § 100g Absatz 1 bis Absatz 4 StPO bei nationalen Sachverhalten in geringerem Umfang Gebrauch gemacht werden wird, weil hier in vielen Fällen bereits die Voraussetzungen für den Erhebung der im Einzelfall relevanten Daten nach den § 100g Absatz 1 bis Absatz 4 StPO vorliegen dürften. Im Jahr 2024 sind von den Strafverfolgungsbehörden der Länder insgesamt 22 684 Maßnahmen nach § 100g StPO durchgeführt worden. Hiervon entfielen insgesamt 15 955 auf Funkzellenabfragen. Geht man davon aus, dass das Volumen der Sicherungsanordnungen geschätzt 5 Prozent von 22 684 betragen würde, so wäre mit Blick auf den unmittelbar hervorgerufenen Sachaufwand der Entschädigungspflichten nach den Nummern 500 bis 507 und 600 der Anlage 3 zum JVEG von einer Mehrbelastung für die Länderhaushalte in Höhe von insgesamt circa 120 000 Euro auszugehen.

Eine weitere Auswirkung des Entwurfs ist, dass die Sicherungsanordnung auch zu weiteren Ermittlungsansätzen führen kann, die als mittelbare Effekte entsprechenden Aufwand nach sich ziehen können, und zwar weitere Ermittlungen und etwaige gerichtliche Verfahren. Diese Kosten können wie bei der vorsorglichen IP-Adressspeicherung ebenfalls nicht beziffert werden. Setzt man allerdings die geschätzte Zahl von circa 567 Sicherungsanordnungen ins Verhältnis zu den 561 539 bundesweit 2024 neu eingegangen Strafverfahren bei Gerichten, so wäre – unter der Annahme, dass jede Sicherungsanordnung einen Ermittlungserfolg nach sich ziehen würde – höchstens mit einem Anstieg von 0,001 Prozent zu rechnen, was sich innerhalb der üblichen jährlichen Schwankungen bewegt.

Das Instrument kann mit der Sicherung der Daten gleichzeitig auch für – ebenfalls nicht bezifferbare – Einsparungen sorgen, wenn andere aufwändigere Maßnahmen (etwa OSINT-Maßnahmen) entbehrlich werden, die andernfalls möglicherweise durchgeführt worden wären.

Das Rechtsinstrument der Europäischen Sicherungsanordnung könnte hingegen eine höhere praktische Relevanz aufweisen. Diese Annahme gründet darauf, dass eine Datensicherung durch die Staatsanwaltschaft – in Notfällen nach Artikel 4 Absatz 5 der Verordnung (EU) 2023/1543 auch durch deren Ermittlungspersonen – vorgenommen werden kann, wohingegen bei Europäischen Herausgabeanordnungen betreffend Verkehrsdaten ein Richtervorbehalt besteht und eine Eilkompetenz der Staatsanwaltschaft aufgrund der Vorgaben der Verordnung (EU) 2023/1543 nicht vorgesehen werden kann (vergleiche Bundestagsdrucksache 21/3192, Seite 44). Der

Zeitvorteil, der damit verbunden ist, kann in grenzüberschreitenden Fällen entscheidend sein und dazu führen, dass sich deutsche Anordnungsbehörden vermehrt des Rechtsinstruments der Sicherungsanordnung bedienen werden, wenn sie Daten in anderen Mitgliedstaaten sichern wollen. Eine prozentuale Schätzung, in wie vielen Fällen dies plausibel anzunehmen ist, ist allerdings nicht möglich. Es handelt sich um ein gänzlich neues Rechtsinstrument, weshalb keine Erfahrungswerte bestehen. Auch eine Herleitung über ausgehende, auf eine Verkehrsdatenerhebung gerichtete Ersuchen ist nicht möglich, da im Bereich der sonstigen Rechtshilfe keine Statistiken existieren und ausgehende Ersuchen, die nicht auch im Inland vollzogen werden, nicht in die nationalen Statistiken nach § 101b StPO einfließen.

Die weiteren Kosten bei den Landespolizeibehörden lassen sich nicht valide beziffern.

b) Bund

aa) Justizbehörden, Zollverwaltung, Polizeibehörden und Nachrichtendienste

(1) Funkzellenabfrage

Hinsichtlich der Funkzellenabfrage ist nennenswerter Mehraufwand nicht zu erwarten.

(2) Vorsorgliche IP-Adressspeicherung und Sicherungsanordnung

Zum Generalbundesanwalt und Bundesgerichtshof (Ermittlungsrichter)

Die Ausführungen zu den Ländern geltend entsprechend. Im Jahr 2024 sind vom Generalbundesanwalt beim Bundesgerichtshof insgesamt 65 Maßnahmen nach § 100g StPO veranlasst worden. Im Hinblick auf die Sicherungsanordnung ist ausgehend hiervon nur mit einer geringfügigen Mehrbelastung zu rechnen.

Zur Zollverwaltung

Bestandsdatenauskunft in Verfahren des Zollfahndungsdienstes: Die Ermittlungen des Zollfahndungsdienstes richten sich regelmäßig gegen schwere und organisierte Kriminalität. Nach Einschätzung des Zollfahndungsdienstes ist durch die Möglichkeit, drei Monate rückwirkend IP-Adressen bei den Internetzugangsdiensteanbietern abzufragen, von einer Zunahme der Anfragen auszugehen. Prognostiziert wird ein Ansatz von 100 zusätzlichen Auskünften je Zollfahndungsamt je Jahr, was bei acht Zollfahndungsämtern eine Fallzahl von 800 ergibt. Im Ergebnis entstehen letztendlich geringfügige zusätzliche Personalkosten, die nicht beziffert werden können.

Sicherungsanordnung in eigenen Verfahren des Zollkriminalamts: Aufgrund der Bedeutung des Sachverhalts oder weil ein Zollfahndungsamt danach ersucht oder der Generalbundesanwalt einen entsprechenden Ermittlungsauftrag erteilt, führt das Zollkriminalamt die strafrechtlichen Ermittlungen selbst durch. Abhängig vom Sachverhalt kann es erforderlich sein, Verkehrsdaten von Beschuldigten und anderen Personen auszuwerten. Hier ist gegebenenfalls bereits frühzeitig die Sicherung von Verkehrsdaten anzuordnen, um sie im späteren Verfahren erheben zu können. Im Ergebnis entstehen hierdurch geringfügige zusätzliche Personalkosten, die nicht beziffert werden können.

Sicherungsanordnung in Verfahren der Zollfahndungsämter: Die Ermittlungen der Zollfahndungsämter richten sich regelmäßig gegen schwere und organisierte Kriminalität. Bandenmäßige Begehungen sind die Regel. Die Ermittlungspersonen der Staatsanwaltschaft im Zollfahndungsdienst benötigen das Instrument der Sicherungsanordnung in einem frühen Stadium des Ermittlungsverfahrens, um Verkehrsdaten von potentiellen Beschuldigten und weiteren Tatbeteiligten zu sichern. Im

Ergebnis entstehen letztendlich geringfügige zusätzliche Personalkosten, die nicht beziffert werden können.

Der Zollverwaltung entstehen in ihrer Gefahrenabwehrfunktion keine haushaltswirksamen Ausgaben.

Zu den Polizeibehörden

Im Rahmen der Aufgabe des Bundeskriminalamtes (Abwehr von Gefahren des internationalen Terrorismus) nach § 5 Bundeskriminalamtgesetzes (BKAG) kann für die Befugnis zur Bestandsdatenabfrage anhand IP-Adressen gemäß § 40 Absatz 4 Satz 1 BKAG davon ausgegangen werden, dass trotz des erwartbaren steigenden Abfrageverhaltens keine höheren Sachkosten für das Bundeskriminalamt entstehen werden. Letztlich hängt die Zahl an Bestandsdatenerhebungen von der Zahl der eingeleiteten Gefahrenabwehrvorgänge pro Jahr ab, die nicht seriös geschätzt werden kann und Schwankungen unterliegt. Das Mehr an erwartbar aussichtsreich zu stellenden Bestandsdatenabfragen kann nach gegenwärtiger Einschätzung mit dem vorhandenen Personal erledigt werden. Darüber hinaus wird die Kostenpauschale für diese Auskunftsart (vergleiche Nummer 201 der Anlage 3 zum JVEG) mit diesem Gesetz gesenkt, sodass zusätzliche Kosten zunächst nicht zu erwarten sind.

Gleiches gilt für die Aufgabe des Bundeskriminalamtes nach § 6 BKAG (Schutz von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamtes) und die Befugnis zur Bestandsdatenabfrage anhand IP-Adressen gemäß § 63a Absatz 4 Nummer 2 BKAG (Zahl an Bestandsdatenerhebungen anhand einer IP-Adresse in 2022: 162).

Im Rahmen der Aufgabe des Bundeskriminalamtes nach § 2 BKAG kann für die Befugnis der Bestandsdatenabfrage anhand IP-Adressen zur Feststellung der örtlichen Zuständigkeit in den Ländern gemäß § 10 Absatz 3 BKAG trotz des erwartbaren steigenden Abfrageverhaltens derzeit davon ausgegangen werden, dass keine höheren Sachkosten für das Bundeskriminalamt entstehen werden. Es wird nach aktueller Einschätzung kein zusätzliches Personal notwendig sein (Zahl an Bestandsdatenerhebungen anhand einer IP-Adresse in 2022: 86 250). Darüber hinaus wird durch die zukünftig sichergestellte Identifizierung des Anschlusses anhand der IP-Adresse bislang noch zu leistender erweiterter Mehraufwand in der Zentralstelle reduziert, die örtliche Zuständigkeit für einen Fall über aufwändigere oder zeitintensivere Maßnahmen doch noch zu ermitteln. Auch vor dem Hintergrund der zukünftig festgelegten Kostenpauschale für diese Auskunftsart sind zunächst keine zusätzlichen Sachkosten zu erwarten.

Im Rahmen der Aufgabe der Bundespolizei kann vor dem Hintergrund der zukünftig festgelegten Kostenpauschale für die Befugnis zur Bestandsdatenabfrage anhand IP-Adressen gemäß § 22a Absatz 3 Satz 1 des Bundespolizeigesetzes davon ausgegangen werden, dass trotz des erwartbaren steigenden Abfrageverhaltens keine höheren Sachkosten für die Bundespolizei entstehen werden. Es wird nach aktueller Einschätzung auch kein zusätzliches Personal notwendig sein. Im Hinblick auf die Sicherungsanordnung nach § 25a Absatz 1 des Bundespolizeigesetzes ist nur mit einer geringfügigen Mehrbelastung zu rechnen.

Im Rahmen der Aufgabe des Bundeskriminalamt nach § 4 BKAG wird es einen Anstieg an Bestandsdatenanfragen zur Täteridentifizierung anhand IP-Adressen gemäß § 100j StPO geben. Trotz des erwartbaren steigenden Abfrageverhaltens wird derzeit davon ausgegangen, dass keine höheren Sachkosten für das Bundeskriminalamt entstehen werden. Es wird nach aktueller Einschätzung kein zusätzliches Personal notwendig sein. Selbiges gilt für die Sicherungsanordnung im Strafverfahren.

Zu den Nachrichtendiensten

Aufgrund der zu erwartenden Erhöhung der Anzahl der Bestandsdatenabfragen, bedingt durch die längere Speicherdauer von IP-Adressen, wird beim Bundesamt für Verfassungsschutz eine Automatisierung des bislang manuell wahrgenommenen Prozesses erforderlich. Für die technische Umsetzung werden eine hD-Funktion und zwei gD-Funktionen benötigt. Hierin berücksichtigt sind notwendige Anpassungen im Bereich der Netzübergänge, Netzwerktechnik und Systemerweiterungen an den TKÜ-Systemen zur Automation der neuen Abfragen aus den TKÜ-Bestandssystemen sowie technische Anpassungen an der ESB. Es muss zugleich sichergestellt sein, dass keine als Verschlusssachen eingestuften Daten abfließen. Ebenso müssen die entsprechenden Auskunftsantworten wieder den jeweiligen Abfragen im TKÜ-System zugeordnet werden. Für den fachlichen Aufwand zur Durchführung der neuen Abfragemöglichkeiten wird eine zusätzliche Funktion im mD benötigt. Dem Bundesamt für Verfassungsschutz entsteht folglich ein Personalmehrbedarf in Höhe von rund vier (Plan-)Stellen (1 hD, 2 gD, 1 mD). Die daraus resultierenden Personalkosten betragen jährlich rund 395 000 Euro. Dem Bundesamt für Verfassungsschutz entstehen zudem Sachkosten in Höhe von rund 254 000 Euro (einmalig) sowie rund 177 000 Euro (jährlich).

Die weiteren Kosten beim Bundesnachrichtendienst lassen sich nicht valide beziffern.

bb) Bundesnetzagentur

Der Bundesnetzagentur werden voraussichtlich weitere Kosten entstehen.

Der Kreis der Verpflichteten wird durch die §§ 176 und 177 TKG definiert. Dies sind nach § 176 TKG die Anbieter öffentlich zugänglicher Telekommunikationsdienste und nach § 177 TKG die Anbieter von Internetzugangsdiensten. Aufgrund dieser Verpflichtungen geht die Bundesnetzagentur aufgrund der Meldungen nach § 5 Absatz 1 TKG von rund 3 000 Verpflichteten nach § 176 TKG und von rund 700 Verpflichteten nach § 177 TKG aus.

Aufgrund der §§ 176 Absatz 4 und 177 Absatz 4 TKG werden in der Technischen Richtlinie nach § 170 Absatz 6 TKG technische Einzelheiten zu den verschiedenen Verpflichtungen festgelegt sowie, dass die Verpflichteten unverzüglich nach Dienstaufnahme der Bundesnetzagentur mitzuteilen haben, wie die Vorgaben umgesetzt werden; Änderungen sind unverzüglich mitzuteilen. Darüber hinaus überprüft die Bundesnetzagentur nach diesen Regelungen die Umsetzung der Vorgaben nach der ersten Umsetzung, bei Änderungen sowie regelmäßig im Turnus von etwa zwei Jahren.

Auf die Bundesnetzagentur kommen durch diese Regelungen danach folgende Aufgaben zu:

Erarbeitung, Fest- und Fortschreibung der Anforderungen zur getrennten und sicheren Speicherung der zu sichernden bzw. speicherpflichtigen Verkehrsdaten sowie zur sicheren Übermittlung der Anordnungen und Verkehrsdaten in der Technischen Richtlinie nach § 170 Absatz 6 TKG. Hierbei müssen sowohl einschlägige nationale Vorgaben wie etwa die des Bundesamts für Sicherheit in der Informationstechnik sowie internationale Standards berücksichtigt werden. Um dem Stand der Technik fortlaufend zu entsprechen, müssen die Festlegungen fortwährend überprüft und fortgeschrieben werden. Die Erarbeitung erfolgt im Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände und der Hersteller. Zur Erfüllung dieser Aufgabe sind 1 hD sowie 3 gD mit informationstechnischer Ausbildung notwendig.

Entgegennahme und Prüfung der Unterlagen zur Umsetzung der Vorgaben sowie Prüfung der tatsächlichen technischen und organisatorischen Umsetzung bei allen rund 3 000 Verpflichteten. Darüber hinaus regelmäßige Kontrollen der Umsetzung der gesetzlichen

Verpflichtungen im Turnus von etwa zwei Jahren. Bei 220 Arbeitstagen pro Jahr ergibt dies eine Überprüfung von sieben Verpflichteten pro Tag. Zur Erfüllung dieser Prüftätigkeit und der damit verbundenen Verwaltungsverfahren bedarf es eines hohen personellen Einsatzes. Zur Erfüllung dieser Aufgabe sind 1 hD, 10 gD und 8 mD notwendig.

Durchsetzung der oben genannten Verpflichtungen nach § 228 TKG sowie nach § 230 Absatz 16 TKG. Hierfür wird ein zusätzlicher Aufwand zur Bearbeitung der notwendigen Ordnungswidrigkeitsverfahren notwendig. Zur Durchsetzung von Pflichten der Unternehmen können auch Durchsetzungsverfahren nach § 183 Absatz 1 TKG in Betracht kommen. Zur Erfüllung dieser Aufgabe sind 1 hD sowie 2 gD notwendig.

Insgesamt besteht zur Erfüllung der Aufgaben bei der Bundesnetzagentur ein Personalaufwand von 26 Personaleinheiten, und zwar 3 hD, 15 gD, 8 mD. Die daraus resultierenden Personalkosten betragen jährlich rund 1,727 Mio. Euro. Der Bundesnetzagentur entstehen zudem Sachkosten in Höhe von rund 25 000 Euro (einmalig) sowie rund 5 000 Euro (jährlich).

c) Wirtschaft

Für die betroffenen Telekommunikationsunternehmen entstehen durch die Erfüllung der mit einer Sicherungsanordnung verbundenen und der in § 177 Absatz 1 TKG vorgesehenen Speicherpflichten und der weiteren Vorgaben nach § 176 Absatz 2 TKG und nach § 177 Absatz 2 TKG weitere Kosten.

Anders als bei früheren Regelungen zu einer umfassenden Vorratsdatenspeicherung wird nur eine anlasslose Speicherpflicht im Hinblick IP-Adressen eingeführt sowie eine anlassbezogene Pflicht zur Sicherung von Verkehrsdaten aufgrund einer Sicherungsanordnung in einem konkreten Strafverfahren.

Da die Speicherpflicht unterschiedslos alle Anbieter von Internetzugangsdiensten betrifft, sind circa 700 Unternehmen betroffen. Bei den voraussichtlichen Kosten ist zwischen dem Investitionsaufwand für eine erforderliche erstmalige Einrichtung der technischen Maßnahmen zur Erfassung sowie der sicheren Speicherung der Daten und den laufenden Kosten für die stetige Aktualisierung dieser Systeme zu unterscheiden. Die Lage kann sich bei den einzelnen Unternehmen sehr unterschiedlich gestalten. Wenn IP-Adressen bei Unternehmen bereits aus betrieblichen Gründen für einen gewissen Zeitraum gespeichert werden, könnte es bei diesen Unternehmen ausreichen, diese Zeiträume lediglich technisch zu verlängern. Bei Unternehmen, die derzeit IP-Adressen betrieblich nicht speichern, sind die Kosten für die erstmalige Einrichtung sowie für die laufenden Kosten entsprechend höher. Bei Unternehmen, die die öffentlichen IP-Adressen mehreren Anschlussinhabern gleichzeitig mittels Verfahren der Network Address Translation (NAT) zuweisen und daher auch Portnummern und gegebenenfalls andere Daten speichern müssen, um einen Anschlussinhaber zu identifizieren, ist zu beachten, dass diese Daten regelmäßig nicht außerhalb der eingesetzten NAT-Systeme zur Verfügung stehen. In diesen Fällen müssen diese NAT-Systeme zunächst ausgetauscht werden, was einen erheblichen Eingriff in die Wirknetze der Unternehmen darstellt und entsprechend zusätzliche Kosten verursacht.

Zudem müssen alle Anbieter von Telekommunikationsdiensten technische und organisatorische Vorkehrungen für die Sicherung und Herausgabe von Verkehrsdaten treffen. Dies betrifft insbesondere die Einrichtung einer Speicherinfrastruktur, die es ermöglicht, Identifizierungsdaten für bis zu drei Monate oder länger zu speichern und wieder zu löschen, einschließlich der Integration in die bestehenden Prozesse. Von den Vorkehrungen sind circa 3 000 Unternehmen betroffen.

Das Verfahren der Sicherung und Herausgabe unterscheidet sich durch die Schutz- und Löschvorgaben von den bereits heute stattfindenden Auskunftsersuchen zur Strafverfolgung, die von den Unternehmen auf der Grundlage des geltenden Rechts beantwortet werden müssen. Insoweit besteht ein nennenswerter zusätzlicher Aufwand für die Sicherung und Herausgabe von Verkehrsdaten, die alle Anbieter von Telekommunikationsdiensten unterschiedslos betrifft.

Einige Verbände und Unternehmen geben an, dass für die Umsetzung der Speicherpflicht je nachdem, ob NAT-Verfahren eingesetzt werden oder nicht, und in Abhängigkeit der noch festzulegenden Details der Schutz- und Löschmaßnahmen einmalige Investitionskosten von 1 bis 2 Millionen Euro für große Anbieter, 150 000 bis 200 000 Euro für mittlere und 80 000 Euro für kleine Anbieter anfallen könnten. Die laufenden Kosten betragen nach diesen Angaben durchschnittlich 10 Prozent der Investitionskosten. Personalkosten könnten nach der Einschätzung einiger großer Unternehmen zwischen 200 000 und 550 000 Euro liegen; für mittlere und kleinere Unternehmen liegen hierzu keine konkreten Angaben vor.

Für die Umsetzung der Sicherung und Herausgabe von Verkehrsdaten geben einige Unternehmen an, dass in Abhängigkeit der noch festzulegenden Schutzmaßnahmen von einmaligen Investitionskosten von 60 000 bis 300 000 Euro für große Anbieter und von 30 000 Euro für kleine Anbieter notwendig seien. Die laufenden Kosten wurden hierzu von bis zu 40 Prozent der Erstinvestition angegeben. Personalkosten könnten zudem zwischen 100 000 und 250 000 Euro für große Anbieter betragen und rund 10 000 Euro für kleinere Anbieter.

Die Verbände und Unternehmen, die sich zu den Kosten geäußert haben, betonen hierzu, dass es sich aufgrund der individuellen Notwendigkeit zur Umgestaltung des Internetzugangsnetzes zur Erfassung der Daten sowie aufgrund der noch festzulegenden Anforderungen zu den Schutzmaßnahmen lediglich um aktuelle, grobe Schätzungen handele.

Für die Bearbeitung der Sicherung und späteren Herausgabe von Verkehrsdaten gehen die großen Anbieter von einem Zeitbedarf von etwa 30 bis 60 Minuten pro Fall aus; für die Herausgabe von Anschlussinhaberdaten aufgrund einer IP-Adresse von einem Zeitbedarf von etwa 10–15 Minuten. Zu berücksichtigen ist, dass dieser Aufwand nach Anlage 3 zum JVEG entschädigt werden kann. Die mit Artikel 4 dieses Entwurfes vorgesehenen Entschädigungstatbestände decken diesen Aufwand.

6. Weitere Gesetzesfolgen

Die geplanten Regelungen haben keine Auswirkungen für Verbraucher. Aus gleichstellungspolitischer Sicht sind die Regelungen neutral. Demografische Auswirkungen sind nicht zu erwarten.

VIII. Befristung; Evaluierung

Eine Befristung der Regelungen kommt nicht in Betracht. Sie betreffen den Kernbereich des Strafverfahrensrechts und des dazugehörigen Telekommunikationsrechts und sind schon wegen der erforderlichen technischen Umsetzung auf Dauer angelegt.

Eine eigenständige Evaluierung ist nicht erforderlich. Die vorsorgliche IP-Adressspeicherung dient ausschließlich der Möglichkeit, anhand einer IP-Adresse einen Anschlussinhaber zu identifizieren, und stellt damit einen nicht als schwer einzustufenden Eingriff in Grundrechte dar (vergleiche Europäischer Gerichtshof, Urteil vom 30. April

2024, Rechtssache C-470/21, Quadrature du Net II – Hadopi, Randnummer 90), sodass eine Evaluierung insoweit nicht erforderlich ist. Für die Einführung der Sicherungsanordnung ist sie entbehrlich, da sie auch der Durchführung der Verordnung (EU) 2023/1543 dient. Außerdem ist ohnehin eine statistische Erfassung vorgesehen, sodass der Nutzen laufend nachvollzogen werden kann.

B. Besonderer Teil

Zu Artikel 1 (Änderung der Strafprozessordnung)

In der Strafprozessordnung werden die Vorschriften zur Bestandsdatenabfrage (§ 100j), zur Verkehrsdatenabfrage (§ 100g) und zur Nutzungsdatenabfrage (§ 100k) sowie die hierauf bezogenen Verfahrensbestimmungen (§ 101a) überarbeitet. Diese Vorschriften betreffen die Befugnisse der Strafverfolgungsbehörden, verschiedene Arten von Daten bei Anbietern von Telekommunikationsdiensten und Erbringern von digitalen Diensten zu erheben. Die Überarbeitung ist geboten, da die Vorschriften infolge mehrfacher Reformgesetzgebung in den letzten Jahren zunehmend unübersichtlich geworden sind. Dies gilt insbesondere mit Blick auf den im Jahr 2021 eingeführten § 100k, der die Erhebung von Nutzungsdaten betrifft: Die Vorschrift trifft Regelungen vergleichbar zu § 100g, ist aber zum Teil abweichend aufgebaut und formuliert. Insoweit werden systematische Anpassungen vorgenommen. Darüber hinaus wird der bisherige § 100g Absatz 2, der die Anlasstaten für einen Abruf von Vorratsdaten regelt, aufgrund der Unvereinbarkeit der Vorschriften zur Vorratsdatenspeicherung mit europäischem Recht gestrichen. Außerdem wird in § 100g Absatz 4 die Funkzellenabfrage neu geregelt und mit § 100g Absatz 7 erstmalig eine Sicherungsanordnung für Verkehrsdaten eingeführt.

Zu Nummer 1 (Inhaltsübersicht)

Es handelt sich um redaktionelle Folgeänderungen zu Nummer 3 (Neufassung von § 100j) und Nummer 4 (Neufassung von § 101a).

Zu Nummer 2 (§ 100g – Erhebung von Verkehrsdaten)

Die Vorschrift wird neu gefasst.

Der bisherige Absatz 2 enthält einen Straftatenkatalog für die Erhebung von auf Vorrat gespeicherten Verkehrsdaten. Er ist aufzuheben. Anlass dafür ist das Urteil des Bundesverwaltungsgerichts vom 14. August 2023 (6 C 6.22), das nach Vorabentscheidung des Europäischen Gerichtshofs (Urteil vom 20. September 2022 – C-793/19 und C-794/19, Spacenet und andere) Folgendes entschieden hat: Die in § 175 Absatz 1 Satz 1 in Verbindung mit § 176 des Telekommunikationsgesetzes (TKG) – § 113a Absatz 1 Satz 1 in Verbindung mit § 113b TKG alte Fassung – geregelte Verpflichtung der Anbieter öffentlich zugänglicher Telekommunikationsdienste zur Speicherung der dort genannten Telekommunikations-Verkehrsdaten ist in vollem Umfang unvereinbar mit Artikel 15 Absatz 1 der Richtlinie 2002/58/EG und daher nicht anwendbar, weil eine anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten vorgeschrieben wird und – soweit das Unionsrecht einer eingeschränkten Vorratsdatenspeicherung nicht von vornherein entgegensteht – die Voraussetzungen hinsichtlich der Bestimmtheit und Normenklarheit der Regelung, der zulässigen Zwecke sowie der weiteren inhaltlichen und verfahrensmäßigen Anforderungen nicht vorliegen. Der geltende Absatz 2 bezieht sich auf die Erhebung der Daten aus dieser europarechtswidrigen Vorratsdatenspeicherung und ist daher zur Bereinigung aufzuheben. Soweit Absatz 2 in der geltenden Fassung noch von Absatz 1 Satz 3

hinsichtlich der der Erhebung gespeicherter Standortdaten in Bezug genommen wird, gelten künftig andere Voraussetzungen, siehe hierzu die Begründung zu Absatz 3.

Absatz 1 enthält künftig den Grundtatbestand der Verkehrsdatenerhebung. Die Abfrage aus Anlass von Straftaten, die mittels Telekommunikation begangen worden sind, ist fortan in Absatz 2 geregelt. Die Regelungen zur Standortdatenabfrage (Absatz 3) und zur Funkzellenabfrage (Absatz 4) bauen als spezielle Formen der Verkehrsdatenabfrage auf die Voraussetzungen von Absatz 1 auf. Neu geschaffen wird in Absatz 5 eine Befugnis zur Erhebung bestimmter Verkehrsdaten bei nummernunabhängigen interpersonellen Kommunikationsdiensten mit dem Ziel der anschließenden Identifizierung des Beschuldigten. Absatz 7 enthält neu die Befugnis zum Erlass einer Sicherungsanordnung.

Nicht fortgeführt wird der bisherige Absatz 4. Die Vorschrift sieht ein ausdrückliches Verbot der Verkehrsdatenerhebung aus der Vorratsdatenspeicherung bei Berufsgeheimnisträgern vor. Dieser Regelung bedarf es nicht mehr, da sie sich auf die Erhebung der Daten aus der europarechtswidrigen Vorratsdatenspeicherung bezieht, die aufgehoben werden. Da diese Regeln nie durchgesetzt worden sind, ändert sich durch die Streichung das Niveau, mit dem Berufsgeheimnisträger geschützt sind, nicht. Der Schutz von Berufsgeheimnisträgern, einschließlich des Schutzes journalistischer Quellen, ist – wie bislang – nach der allgemeinen Schutzvorschrift des § 160a gewährleistet. Die neu eingeführte Speicherpflicht von IP-Adressen und zugehörigen Daten steht mit der Verkehrsdatenerhebung nach § 100g in keinem Zusammenhang, sondern effektiviert lediglich die – bereits heute mögliche – Bestandsdatenabfrage nach § 100j Absatz 2. Aus den Bestandsdaten können keine Erkenntnisse darüber gewonnen werden, mit wem Berufsgeheimnisträger kommuniziert haben. Denn abgefragt werden darf nur, wer der Anschlussinhaber einer den Strafverfolgungsbehörden bekannt gewordenen IP-Adresse ist.

Demgemäß ändert sich auch das Niveau, mit dem Medienschaffende geschützt sind, nicht. Soweit das europäische Medienfreiheitsgesetz (European Media Freedom Act – EMFA) Gewährleistungen zum Schutz von Medienschaffenden enthält, sind diese – wie bislang – bei der Rechtsanwendung vorrangig zu beachten.

Zu § 100g (Erhebung von Verkehrsdaten)

Zu Absatz 1

Zu Satz 1

Die Regelung enthält den Grundfall der Verkehrsdatenerhebung bei demjenigen, der öffentlich zugängliche Telekommunikationsdienste anbietet oder daran mitwirkt, § 100g Absatz 1 Satz 1 Nummer 1 und Satz 2 der geltenden Fassung. Die Vorschrift ist redaktionell neu gefasst, ohne dass damit wesentliche Änderungen an der Rechtslage einhergehen.

Hinsichtlich des Begriffs der Verkehrsdaten verweist das geltende Recht auf die §§ 9 und 12 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG). Dieser Verweis wird aus systematischen Gründen durch Verweis auf die gesetzliche Begriffsbestimmung in § 3 Nummer 70 TKG ersetzt. Eine Änderung der Rechtslage geht damit ausdrücklich nicht einher. Ausdrücklich klargestellt wird, dass die Daten aus der vorsorglichen IP-Speicherung nach § 177 TKG nicht unmittelbar als Verkehrsdaten auf Grundlage von § 100g Absatz 1 erhoben werden können. Strafverfolgungsbehörden können lediglich Auskunft über den Anschlussinhaber zu einer IP-Adresse nach § 100j Absatz 2 verlangen.

Klargestellt ist in der Vorschrift erstmals, dass es sich beim Adressaten der Maßnahme um den Beschuldigten handelt. Dies entspricht bereits der geltenden Rechtslage,

vergleiche § 101a Absatz 1 Satz 1 in Verbindung mit § 100a Absatz 3. Der Begriff des Beschuldigten umfasst dabei – wie bislang – auch namentlich noch unbekannte Tatverdächtige, wenn also ein Verfahren zunächst gegen Unbekannt geführt wird (vergleiche zu § 100a Bundesgerichtshof, Beschluss vom 8. Februar 1994 – 1 BGs 88/94).

Neu in die Vorschrift aufgenommen ist erstmals ausdrücklich, wer mit einer Anordnung verpflichtet werden kann. Die tauglichen Verpflichteten ergaben sich bislang nur indirekt aus der Formulierung aus der Bezugnahme auf die erhebungsfähigen Verkehrsdaten im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz und im Gesetz über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben. Nun sind in Satz 1 ausdrücklich diejenigen als Verpflichtete benannt, die öffentlich zugängliche Telekommunikationsdienste anbieten oder daran mitwirken. Die Formulierung ist angelehnt an § 100j Absatz 1 Satz 1 Nummer 1, der die Bestandsdatenabfrage ermöglicht und die Verpflichteten ausdrücklich benennt. § 100g Absatz 1 Satz 1 erlaubt es weiterhin nicht, Abfragen an Telekommunikationsanbieter zu richten, die keine öffentlich zugänglichen Telekommunikationsdienste anbieten (vergleiche Bundestagsdrucksache 19/4671, Seite 61; Rückert, in: Münchener Kommentar zur StPO, 2. Auflage 2023, § 100g Randnummer 42). Hierzu gehören etwa die Betreiber von drahtlosen Netzwerken (WLANs) in Hotels.

Die ausdrückliche Benennung der tauglichen Verpflichteten in § 100g hat keine Änderung der Rechtslage zu Folge. Strafverfolgungsbehörden sind daher auch nicht darauf beschränkt, Daten nur noch unter Mitwirkung des Verpflichteten zu erheben. So kann beispielsweise bei einer sogenannten IP-Tracking-Maßnahme, die eine Ermittlungsbehörde selbst durchführt, die Erhebung der Verkehrsdaten weiterhin auf § 100g gestützt werden (vergleiche dazu Bundesgerichtshof, Beschluss vom 23. September 2014 – 1 BGs 210/14).

Der neue § 100g Absatz 1 Satz 1 enthält außerdem katalogartig die materiellen Voraussetzungen für die Verkehrsdatenabfrage. Nummer 1 enthält wie bislang die Anforderungen an die Anlasstat. Nummer 2 regelt, dass die Erhebung der Verkehrsdaten, sofern erforderlich, nicht nur wie bisher für die Erforschung des Sachverhalts zulässig ist, sondern auch zur Ermittlung des Aufenthaltsorts des Beschuldigten. Hinsichtlich des Erfordernisses der Verhältnismäßigkeit in Nummer 3 gilt ebenfalls geltende Rechtslage fort.

Zu Satz 2

In Satz 2 ist aufgenommen, dass neben den Verkehrsdaten des Beschuldigten auch Daten von Personen erhoben werden können, bei denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt (sogenannte Nachrichtenmittler). Diese Regelung gilt auch derzeit schon (§ 101a Absatz 1 Satz 1 in Verbindung mit § 100a Absatz 3). Es handelt sich dabei nicht um eine Verfahrensregelung, sondern um die Regelung des Adressatenkreises, sodass die Überführung in die Erhebungsnorm aus systematischen Gründen sachgerecht ist.

Zu Satz 3

Satz 3 bestimmt in der neuen Fassung ausdrücklich, dass auch die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben Verpflichtete sein kann. Auch diese Anpassung führt nicht zur Änderung der Rechtslage (vergleiche auch Bundestagsdrucksache 19/4671, Seite 61).

Zu Absatz 2

Die Vorschrift regelt nun separat die Befugnis, Verkehrsdaten in Fällen zu erheben, in denen ein Verdacht hinsichtlich einer mittels Telekommunikation begangener Straftaten besteht, die nicht bereits von § 100g Absatz 1 Satz 1 erfasst ist. Bei mittels Telekommunikation begangenen Straftaten muss es sich nicht um Straftaten von auch im Einzelfall erheblicher Bedeutung handeln; dies entspricht der geltenden Rechtslage. Die eigenständige Regelung vereinfacht den Grundtatbestand in Absatz 1 und die hierauf bezogenen besonderen Maßnahmen der Standortdaten- und Funkzellenabfrage.

Die Erhebung von Verkehrsdaten ist künftig zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Dies ist eine geringfügige Lockerung der Subsidiaritätsklausel, denn bislang ist der Abruf nur zulässig, wenn die Erforschung auf andere Weise aussichtslos wäre (§ 100g Absatz 1 Satz 2 geltende Fassung). Die Änderung dient der Vereinheitlichung bei den Erhebungsbefugnissen (vergleiche § 100a Absatz 1 Satz 1 Nummer 3, § 100b Absatz 1 Nummer 3, § 100c Absatz 1 Nummer 4, § 100f Absatz 1 und Absatz 2 sowie § 100h Absatz 2 Satz 2 Nummer 2).

Einer ausdrücklichen Regelung, dass eine Maßnahme nach Absatz 2 nicht zur Erhebung von Standortdaten ermächtigt, bedarf es nicht. Denn dies ergibt sich aus der neuen Normsystematik, nach der die Erhebung von Standortdaten (Absatz 3) nur unter den Voraussetzungen von Absatz 1 – also gerade nicht von Absatz 2 – möglich ist.

Zu Absatz 3

Die Regelungen zur Standortdatenabfrage werden in einen eigenen Absatz überführt und neu geordnet. Erstmals wird dabei ausdrücklich auf die gesetzliche Begriffsbestimmung in § 3 Nummer 56 TKG Bezug genommen. Eine Änderung der Rechtslage geht damit insoweit nicht einher.

Künftig gelten dabei die gleichen Voraussetzungen für den Abruf bereits vorhandener Standortdaten und solchen, die künftig oder in Echtzeit erhoben werden. Die begriffliche Unterscheidung kann damit entfallen.

Der Abruf vorhandener Standortdaten ist gemäß § 100g Absatz 1 Satz 3 der bisher geltenden Fassung nur unter den strengen Voraussetzungen des geltenden Absatzes 2 möglich, das heißt bei Verdacht einer besonders schweren Straftat, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre. Der Abruf von Standortdaten, die künftig anfallen, oder in Echtzeit ist derzeit hingegen unter den geringeren Anforderungen des geltenden Absatzes 1 Satz 1 Nummer 1 zulässig, nämlich bei Verdacht einer Straftat von im Einzelfall erheblicher Bedeutung, soweit die Maßnahme für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Diese Differenzierung geht darauf zurück, dass für Standortdaten ursprünglich eine anlasslose Vorratsdatenspeicherung von vier Wochen vorgesehen war. Die Erhebung war als besonders sensibel eingeschätzt worden, da sich daraus Bewegungsprofile auch von Unbeteiligten hätten erstellen lassen können. Die Erhebung von künftig anfallenden Standortdaten und Standortdaten in Echtzeit waren demgegenüber als weniger sensibel eingeordnet worden, da sie nicht auf gespeicherte Daten zurückgreife (vergleiche Bundestagsdrucksache 18/5088, Seite 27).

Tatsächlich ist eine Vorratsdatenspeicherung von Standortdaten nie durchgesetzt und mittlerweile durch das Bundesverwaltungsgericht wegen Verstoßes gegen das Unionsrecht für unanwendbar erklärt worden (siehe näher im Allgemeinen Teil der Begründung unter I.). Tatsächlich erbringt der Abruf vorhandener (retrograder) Standortdaten daher in vielen Fällen nur wenig Daten, da die zur Auskunft Verpflichteten

die Daten allenfalls zu betrieblichen Zwecken speichern. Regelmäßig sind Daten nach spätestens sieben Tagen gelöscht. Die Erstellung von mehreren Wochen zurückreichenden Bewegungsprofilen ist auf dieser Datengrundlage nicht möglich. Es ist daher gerechtfertigt, den Abruf von Standortdaten in Absatz 3 insgesamt unter den Voraussetzungen des neuen Absatz 1 zuzulassen, also bei Verdacht einer Straftat von im Einzelfall erheblicher Bedeutung.

Umgekehrt bedarf es für den Abruf von künftig anfallenden Standortdaten einer moderaten Anhebung der Eingriffsvoraussetzungen. Denn mit diesem Ermittlungsinstrument könnten sich die Strafverfolgungsbehörden ein dauernd aktualisiertes Bewegungsprofil – allerdings erst ab Anordnung beziehungsweise Wirksamwerden der Maßnahme – erstellen lassen. Der Abruf von künftig anfallenden Standortdaten steht fortan – wie bereits der Abruf bereits vorhandener Standortdaten – unter dem Erfordernis der Subsidiarität, darf also nur eingesetzt werden, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Zu Absatz 4

Die Vorschrift enthält die Befugnis zur Funkzellenabfrage, die im bisher geltenden § 100g Absatz 3 geregelt ist.

Nach derzeitiger Rechtslage ist die Funkzellenabfrage unter anderem nur unter den Voraussetzungen des geltenden Absatzes 1 Satz 1 Nummer 1 zulässig. Lange hat die Praxis die Vorschrift dahingehend ausgelegt, dass die Abfrage zulässig sei, sofern der Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung bestehe (exemplarisch Landgericht Stade, Beschluss vom 26. Oktober 2018 – 70 Qs 133/18 – und Landgericht Arnsberg, Beschluss vom 29. April 2019 – 2 Qs-410 UJs 254/19-43/19). Der Bundesgerichtshof hat mit Beschluss vom 10. Januar 2024 – 2 StR 171/23 – entschieden, dass eine Funkzellenabfrage den Verdacht einer besonders schweren Straftat gemäß § 100g Absatz 2 voraussetze. Verschiedene Landgerichte sind der Ansicht des Bundesgerichtshofs nicht gefolgt (unter anderem Landgericht Hamburg, Beschluss vom 6. Juni 2024 – 621 Qs 32/24; Landgericht Düsseldorf, Beschluss vom 19. Juni 2024 – 1 Qs 1/24; Landgericht Regensburg, Beschluss vom 5. September 2024 – 8 Qs 30/24); sie meinen weiter, es genüge der Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung.

Die neue Regelung in Absatz 4 verweist auf die Voraussetzungen des Absatzes 1 und lässt damit den Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung genügen. Dies entspricht dem Verständnis der Praxis, bis die Entscheidung des Bundesgerichtshofs ergangen ist. In Bezug auf die Anlasstat besteht damit kein Unterschied zur Abfrage vorhandener Standortdaten. Dies ist in der Sache auch angebracht: Beide Instrumente betreffen Positionsdaten. Sie sind auch in ihrer Eingriffsintensität ungefähr vergleichbar. Die Funkzellenabfrage hat eine hohe Streubreite, erfasst insbesondere gegebenenfalls auch Unbeteiligte, die zu einem gegebenen Zeitpunkt in einer Funkzelle mit ihrem Mobiltelefon aktiv waren. Die Abfrage ermöglicht allerdings keine größeren Rückschlüsse, außer dass ein Anschlussinhaber zu einem bestimmten Zeitpunkt in einer bestimmten Funkzelle mit dem Mobilfunknetz verbunden war. Die Standortdatenabfrage hingegen kann, sofern Daten bei Abfrage vorhanden sind, Rückschlüsse auf Bewegungen erlauben. Doch steht der damit verbundenen höheren Eingriffstiefe eine sehr viel geringere Streubreite entgegen, da sich Maßnahme unmittelbar auf einen Anschlussinhaber bezieht.

Unverändert bleibt die Rechtslage dahingehend, dass lediglich solche Daten erhoben werden können, die bereits angefallen sind. Die Erhebung zukünftig anfallender Verkehrsdaten in einer Funkzelle ist auf Grundlage von Absatz 3 daher weiterhin nicht möglich. Dies unterscheidet sich – auch dies entspricht der bisherigen Rechtslage – von

der Erhebung von Standortdaten nach Absatz 3, wonach sowohl bereits vorhandene als auch künftige Daten erhoben werden können und auch die Erhebung in Echtzeit erlaubt ist.

Beibehalten wird das bereits bestehende Erfordernis der Subsidiarität (Absatz 4 in Verbindung mit Absatz 3), sodass die Maßnahme weiter nur zulässig ist, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Dies trägt der mitunter erheblichen Streubreite der Maßnahme, die auch Unbeteiligte mit einbezieht, Rechnung.

Zu Absatz 5

Neu geschaffen wird in Absatz 5 eine Befugnis zur Erhebung bestimmter Verkehrsdaten bei nummernunabhängigen interpersonellen Kommunikationsdiensten (OTT-1-Diensten; siehe näher unten bei Absatz 7 Satz 1) mit dem Ziel der anschließenden Identifizierung des Beschuldigten. Die Vorschrift nimmt den geltenden § 100k Absatz 3 (§ 100k Absatz 4 neuer Fassung) zum Vorbild, der eine solche Erhebung bereits gegenüber digitalen Diensten erlaubt. Sie betrifft den praktisch häufigen Fall, dass die Strafverfolgungsbehörde einen verfahrensgegenständlichen Inhalt bereits kennt, zum Beispiel, weil sie mit einer Strafanzeige, der ein Screenshot beigefügt ist, darauf hingewiesen worden ist. Nach dem geltenden § 100k Absatz 3 kann in diesem Fall die Staatsanwaltschaft Nutzungsdaten bei digitalen Diensten ausschließlich zur Identifikation des Nutzers erheben, ohne dass dies der Anordnung durch das Gericht bedürfte. Praktisch geht es dabei darum, die IP-Adresse des Nutzers zu erfahren, die ihm zugewiesen war. Anhand dieser Daten kann die Strafverfolgungsbehörde eine Bestandsdatenabfrage bei einem Internetzugangsdiensteanbieter nach § 100j Absatz 2 vornehmen und so gegebenenfalls den Inhaber des Anschlusses identifizieren, von dem aus der Dienst genutzt worden ist.

Der Tatbestand des Satzes 1 setzt voraus, dass die Strafverfolgungsbehörde bereits Kenntnis von dem Inhalt der Nutzung des Dienstes hat. Dies entspricht dem bereits geltenden Erfordernis in § 100k Absatz 3. Neu gegenüber dem geltenden § 100k Absatz 3 ist, dass diese Befugnis nicht allein der Staatsanwaltschaft zusteht, sondern allen Strafverfolgungsbehörden, also auch den Ermittlungspersonen der Staatsanwaltschaft. Dies ist sachgerecht, da die zu erhebenden Identifizierungsdaten keine besondere Sensibilität aufweisen und lediglich die Bestandsdatenabfrage bei dem Internetzugangsdiensteanbieter ermöglichen, die den Ermittlungspersonen bereits heute gestattet ist.

Anders als im geltenden § 100k Absatz 3 werden die erhebbaren Daten nun ausdrücklich benannt, nämlich die gespeicherte IP-Adresse, der genaue Zeitpunkt ihrer Nutzung und gegebenenfalls weitere, zur Identifizierung anhand der IP-Adresse erforderliche Daten wie etwa die Portnummer. Dies lehnt sich an § 177 Absatz 1 Satz 1 TKG neuer Fassung an; auf die Begründung wird insoweit verwiesen. Die Vorschrift erlaubt hingegen keine Erhebung von Bestandsdaten wie Nutzernamen, Accountbezeichnungen, E-Mail-Adressen oder Telefonnummern; insoweit würde sich eine Erhebung nach § 100j richten.

Die Vorschrift begründet keine Speicherpflicht für Anbieter; das Ersuchen bezieht sich also stets nur auf beim Anbieter vorhandene Daten.

Satz 2 bestimmt, dass Absatz 1 Satz 2 entsprechend gilt, die Maßnahme also auch in Bezug auf Nachrichtenmittler angewendet werden kann. Auf die Begründung zu Absatz 1 Satz 2 wird verwiesen.

Zu Absatz 6

Die Vorschrift entspricht unverändert dem derzeit geltenden Absatz 5, der in Absatz 6 verschoben wurde.

Zu Absatz 7

Zu Satz 1

Neu geregelt wird in Absatz 7 Satz 1 die Sicherungsanordnung für Verkehrsdaten.

Ein Instrument der Sicherungsanordnung sieht auch die Verordnung (EU) 2023/1543 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (E-Evidence-Verordnung) für EU-grenzüberschreitende Fälle vor. Eine Europäische Sicherungsanordnung kann für alle Straftaten erlassen werden, wenn sie in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen hätte erlassen werden können, Artikel 6 Absatz 3 E-Evidence-Verordnung. Erst die Schaffung der Sicherungsanordnung für rein nationale Sachverhalte ermöglicht es also den nationalen Strafverfolgungsbehörden, für Maßnahmen im europäischen Ausland die Europäische Sicherungsanordnung anzuwenden. Besondere Bestimmungen betreffend die Anwendung der E-Evidence-Verordnung sind im Elektronische-Beweismittel-Umsetzungs-und-Durchführungsgesetz (Artikel 3) geregelt.

Der Bedarf für die Einführung einer Sicherungsanordnung ergibt sich aus dem Umstand, dass insbesondere Verkehrsdaten flüchtig sind. Telekommunikationsunternehmen speichern die Daten zu betrieblichen Zwecken häufig maximal sieben Tage lang. Aus diesem Grund bedarf es eines Instruments, das auch dann, wenn die Voraussetzungen für die Erhebung der Verkehrsdaten noch nicht vorliegen, den Verlust dieser Daten verhindern kann.

Die Sicherung darf für den Fall einer etwaigen späteren Erhebung angeordnet werden. Die Sicherungsanordnung ist in diesem Sinne ein akzessorisches Sicherungsinstrument:

Die Sicherungsanordnung darf demgemäß gegenüber all jenen angeordnet werden, die auch zur Herausgabe verpflichtet wären, also gegenüber allen Telekommunikationsanbietern. Dazu gehören zum einen Anbieter von nummerngebundenen interpersonellen Telekommunikationsdiensten, insbesondere Internetzugangsdienste, sowie Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden (vergleiche § 3 Nummer 61 TKG). Zum anderen gehören auch Anbieter nummernunabhängiger interpersoneller Telekommunikationsdienste (sogenannte Over-The-Top-1-Dienste oder OTT-1-Dienste, etwa Erbringer von E-Mail- und Messengerdiensten) zu den Verpflichteten (vergleiche § 3 Nummer 40 TKG). Die OTT-1-Dienste treten häufig an die Stelle „klassischer“ Telekommunikationsdienste. So wird beispielsweise die SMS durch Nachrichten über Messengerdienste ersetzt oder der Telefonanruf durch einen Sprachanruf über eine App. Die Einbeziehung der OTT-1-Dienste in den Kreis der Verpflichteten ist daher sachgerecht.

Zum Kreis der Verpflichteten OTT-1-Dienste gehören auch E-Mail-Anbieter. Eine Sicherungsanordnung ihnen gegenüber kann etwa folgende Daten umfassen:

– Daten zum Login beim E-Mail-Postfach (IP-Adresse mit Port und Zeitstempel, sekundengenau mit Zeitzone) sowie gegebenenfalls Standortdaten,

– Routing-Informationen, also die Daten aus dem Header der E-Mail,

– Anzeigename und Kennung, das heißt die E-Mail-Adresse, der anderen Kommunikationsteilnehmer sowie Zeitstempel zu Empfang und Versand der jeweiligen E-Mail.

Die akzessorische Sicherungsanordnung kann sich lediglich auf Verkehrsdaten beziehen, aber – wie die Hauptmaßnahme, die Erhebung nach den Absätzen 1 bis 4, selbst auch – nicht auf Inhaltsdaten. Bei Anhaltspunkten für eine mittels Telekommunikation begangene Straftat, die nicht die Voraussetzungen des Absatzes 1 erfüllt, ist die akzessorische Sicherungsanordnung nur in Bezug auf Verkehrsdaten, nicht aber in Bezug auf Standortdaten möglich, da auch die Erhebung selbst sich nur auf Verkehrsdaten, nicht aber auf Standortdaten beziehen kann (vergleiche Absatz 2 und die Begründung hierzu).

Die Sicherungsanordnung wird sich regelmäßig auf bereits vorhandene Daten beziehen. Soweit die Erhebungsmaßnahme auch die Erhebung künftiger Daten oder von Daten in Echtzeit erlaubt, etwa die Erhebung von Standortdaten nach Absatz 2, gilt dies aber entsprechend auch für die Sicherungsanordnung.

Die Akzessorietät der Sicherungsanordnung schlägt sich auch in der Zweckbindung der gesicherten Daten nieder. Die gesicherten Daten dürfen ausschließlich für die korrespondierende Erhebungsmaßnahme verwendet werden, siehe näher bei der Begründung zur Änderung des Telekommunikationsgesetzes in Artikel 2 Nummer 2, zu § 176 Absatz 1.

Adressat der Sicherungsanordnung sind betroffene Personen. Hierin unterscheidet sich die Sicherungsanordnung von den Erhebungsmaßnahmen nach Absatz 1 bis 4, die sich nur gegen den Beschuldigten oder einen Nachrichtenmittler richten können. Dies trägt dem Umstand Rechnung, dass im frühen Stadium der Ermittlung die Rollen der Personen (Beschuldigter beziehungsweise Nachrichtenmittler oder Tatunbeteiligter) häufig noch nicht feststehen.

Zu Nummer 1

Der Erlass einer Sicherungsanordnung setzt gemäß Nummer 1 voraus, dass zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine in den Absätzen 1 bis 4 bezeichnete Straftat begangen worden ist. Es muss also ein von konkreten Tatsachen gestützter Anfangsverdacht gegeben sein, der über vage Anhaltspunkte und Vermutungen hinausgeht (Köhler und Schmitt, in: Schmitt/Köhler, StPO, 68. Auflage 2025 § 98a Randnummer 7, § 152 Randnummer 4). Dieser Verdachtsgrad entspricht jenem der Rasterfahndung (§ 98a).

Damit ist das Erfordernis gegenüber Absatz 1 Nummer 1 abgesenkt, wonach bestimmte Tatsachen den Verdacht begründen müssen, dass jemand als Täter oder Teilnehmer eine dort genannte Straftat begangen hat. Dieser qualifizierte, sich gegen eine bestimmte Person richtender Tatverdacht ergibt sich häufig erst im Laufe von weiteren Ermittlungen.

Die unverzügliche Sicherung von Verkehrsdaten kann daher bereits unmittelbar dann angeordnet werden, wenn der Anfangsverdacht noch ungerichtet ist, also typischerweise unmittelbar nach Entdeckung der Begehung einer Straftat. Weitere Einzelheiten müssen für die Zulässigkeit der Sicherungsanordnung noch nicht feststehen. Dies steht in Einklang mit der Rechtsprechung des Europäischen Gerichtshofs (Urteil vom 5. April 2022, Rechtssache C-140/20 – Commissioner of An Garda Síochána, Randnummer 91).

Die Sicherungsanordnung kann nur erlassen werden bei Anhaltspunkten für eine Straftat von erheblicher Bedeutung (Absatz 1 Nummer 1, gegebenenfalls in Verbindung mit Absatz 3 oder Absatz 4) oder für eine mittels Telekommunikation begangene Straftat (Absatz 2 Nummer 1). Ein Bedarf für eine Sicherungsanordnung besteht auch für die letztgenannte Konstellation. Denn bei mittels Telekommunikation begangenen Straftaten

ist die Erhebung der Verkehrsdaten häufig der einzige Ermittlungsansatz. Es bestünde die „Gefahr der systemischen Straflosigkeit“ (vergleiche Europäischer Gerichtshof, Urteil vom 30. April 2024, Rechtssache C-470/21, Quadrature du Net II – Hadopi, Randnummer 119), wenn hier keine adäquaten Ermittlungsinstrumente bestünden.

Zu Nummer 2

Notwendig, aber auch ausreichend für die Eigenschaft als betroffene Person ist ein persönlicher oder räumlicher Bezug zur Tat, insbesondere zum Opfer oder zum Tatort (vergleiche auch Europäischer Gerichtshof, Urteil vom 6. Oktober 2020, Rechtssache C-511/18, C-512/18 und C-520/18 – La Quadrature du Net und andere, Randnummer 165). Damit kann die Sicherungsanordnung zwar eine gewisse Streubreite aufweisen. Doch da die Erhebung der Daten gemäß Satz 2 nur in Betracht kommt, wenn sich die Anhaltspunkte zu einem qualifizierten Tatverdacht gegen einen bestimmten Beschuldigten verdichtet haben, ist der Eingriff bei einer Sicherung von überschaubarem Gewicht.

Zu Nummer 3

Eine Sicherungsanordnung darf nach Nummer 3 erlassen werden, soweit die Daten für die in den Absätzen 1 bis 4 genannten Zwecke von Bedeutung sein können. Anders als bei der Erhebung ist es also nicht nötig, dass die Sicherung für die im Erhebungstatbestand jeweils genannten Zwecke erforderlich ist (Absatz 1 Nummer 2) beziehungsweise dass die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre (Absatz 2 Nummer 2 und Absatz 3).

Das Merkmal „von Bedeutung sein können“ lehnt sich an die bestehenden Regelungen über die Sicherstellung und Beschlagnahme von Gegenständen zu Beweiszwecken in § 94 Absatz 1 sowie über die Durchsicht von elektronischen Speichermedien in § 110 Absatz 3 an (sogenannte potentielle Beweisbedeutung). Auf die dort gefundene gefestigte Auslegung soll künftig auch im Rahmen von Nummer 2 zurückgegriffen werden. Danach reicht es aus, dass im Moment der Sicherungsanordnung die Möglichkeit besteht, dass die Verkehrsdaten für die in den Absätzen 1 bis 4 genannten Zwecken (Erforschung des Sachverhalts beziehungsweise Ermittlung des Aufenthaltsortes eines Beschuldigten) verwendet werden können. Als ausreichend wird insoweit die Erwartung im Sinne einer Ex-ante-Prognose angesehen, dass die Verkehrsdaten Schlussfolgerungen auf relevante Tatsachen zulassen; für welche Beweisführung sie im Einzelnen in Betracht kommen und ob sie später tatsächlich relevant werden, braucht hingegen noch nicht festzustehen. Ausgeschlossen wird die Sicherungsanordnung hingegen sein, wenn im Zeitpunkt der Anordnung die fehlende Beweisbedeutung schon sicher feststeht (vergleiche zu alledem: Köhler, Schmitt/Köhler, StPO, 68. Auflage 2025, § 94 Randnummer 6 f.; Hauschild, in Münchener Kommentar zur StPO, 2. Auflage 2023, § 94 Randnummer 21 und 22, jeweils mit weiteren Nachweisen). Dies ist etwa der Fall, wenn das Vorliegen eines Verfahrenshindernisses bereits sicher feststeht. Von dem Ausschluss erfasst sein können bei der Sicherungsanordnung aber auch Fälle, in denen sicher absehbar ist, dass die Voraussetzungen einer späteren Erhebung der Verkehrsdaten nach den Absätzen 1 bis 4 nicht vorliegen werden.

Zu Satz 2

Satz 2 stellt klar, dass Absatz 7 selbst keine Erhebungsbefugnis beinhaltet. Die Strafverfolgungsbehörde hat sich daher mit einem eigenständigen Erhebungsersuchen an den Verpflichteten zu wenden, um die gesicherten Daten ganz oder teilweise abzurufen. Die Erhebung darf nur in dem Umfang geschehen, in dem die Voraussetzungen vorliegen, also insbesondere nur, soweit die Erhebung der Daten erforderlich ist.

Es ist zu erwarten, dass die Sicherungsanordnung der (etwaigen) Erhebung regelmäßig zeitlich vorausgeht. Denkbar ist aber auch, dass die Sicherungsanordnung zugleich mit

der Erhebung angeordnet wird. Dies ist in Fällen relevant, in denen zwar bereits die rechtlichen Voraussetzungen für die Erhebung vorliegen, aber die Daten technisch noch nicht abgerufen werden können. Praktisch bedeutsam ist das in Konstellationen, in denen der Verpflichtete keine Vorkehrungen für die Mitwirkung zu treffen hat. Denn nur in bestimmten Fällen besteht eine solche Pflicht (vergleiche § 101a Absatz 5 neuer Fassung in Verbindung mit § 100a Absatz 4 Satz 2). Davon nicht erfasst sind insbesondere die Erbringer von nummernunabhängigen interpersonellen Telekommunikationsdiensten (sogenannten OTT-1-Diensten). Bei diesen Verpflichteten wird der Modus der Datenerhebung im Einzelfall festgelegt, was Zeit in Anspruch nehmen kann. Dies ist zum Beispiel der Fall, wenn die Erhebung von Verkehrsdaten auf einem Server oder bei einem E-Mail-Provider angeordnet wird. In solchen Fällen kann dann gegenüber dem Verpflichteten die Sicherung angeordnet werden, bis die Erhebung tatsächlich möglich ist.

Zu Nummer 3 (§ 100j – Erhebung von Bestandsdaten und § 100k – Erhebung von Nutzungsdaten)

Die Änderungen betreffen die Regelung der Bestandsdatenabfrage in § 100j sowie die Regelung der Nutzungsdatenabfrage in § 100k.

Zu § 100j (Erhebung von Bestandsdaten)

Die Änderungen sind im Wesentlichen redaktioneller Natur. Die Überschrift wird neu gefasst und parallel zu § 100g (Erhebung von Verkehrsdaten) und § 100k (Erhebung von Nutzungsdaten) ausgestaltet.

Zu Absatz 1

Die Vorschrift regelt wie bislang § 100j Absatz 1 Satz 1 den Grundtatbestand der Bestandsdatenauskunft, also die Erhebung von Bestandsdaten bei Telekommunikationsdiensten (Nummer 1) und bei den Erbringern digitaler Dienste (Nummer 2). Lediglich redaktionell wird klargestellt, dass es sich um eine Erhebung „bei“ diesen Verpflichteten handelt; der bisherige Gesetzestext spricht von einer Erhebung „von“ demjenigen, der die entsprechenden Dienste erbringt.

Nicht fortgeführt werden die Verweise auf § 174 Absatz 1 Satz 1 TKG (manuelles Auskunftsverfahren bei Erbringern von Telekommunikationsdiensten) und auf § 22 Absatz 1 Satz 1 TDDDG (Auskunftsverfahren bei Erbringern digitaler Dienste). Die Verweise sind ohne normativen Gehalt. Eine Änderung der Rechtslage ergibt sich daraus nicht.

Die Erhebungsbefugnis in Bezug auf besondere Daten nach § 100j Absatz 1 Satz 2 und 3 ist ohne inhaltliche Änderungen in Absatz 3 verschoben.

Zu Absatz 2

Wie bislang wird in diesem Absatz die Befugnis geregelt, anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse die Auskunft über Bestandsdaten zu verlangen. Solche Auskünfte werden aktuell nur anhand der Daten, insbesondere IP-Adressen, erteilt, die die Telekommunikationsunternehmen ohnehin zu betrieblichen Zwecken speichern. Auskünfte sind derzeit in der Regel nur dann erfolgreich, wenn die IP-Adresse vor höchstens sieben Tagen zugewiesen worden ist, weil länger regelmäßig nicht gespeichert wird. Die neu eingeführte dreimonatige Speicherpflicht in § 177 TKG wird künftig dazu führen, dass ein innerhalb dieses Zeitraums gestelltes Auskunftsersuchen bei Telekommunikationsanbietern regelmäßig erfolgreich sein wird.

Das Auskunftsersuchen nach § 100j Absatz 2 ist mit Verfassungsrecht vereinbar. Insbesondere bedarf es keiner begrenzenden Straftatenkataloge mit Anlassstraftaten

(Bundesverfassungsgericht, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, Randnummer 261; Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, Randnummer 177). Die Behörden selbst erhalten keine Kenntnis der anlasslos und vorsorglich zu speichernden Daten. Sie rufen diese nicht selbst ab, sondern erhalten lediglich Auskünfte über den Inhaber eines bestimmten Anschlusses, der von den Diensteanbietern unter Rückgriff auf diese Daten ermittelt wurde. Dabei bleibt die Aussagekraft dieser Daten eng begrenzt: Die Verwendung der vorsorglich gespeicherten Daten führt allein zu der Auskunft, welcher Anschlussinhaber unter einer bereits bekannten, etwa anderweitig ermittelten IP-Adresse im Internet angemeldet war. Eine solche Auskunft hat, wenngleich ihr Eingriffsgewicht darüber hinaus geht, ihrer formalen Struktur nach eine gewisse Ähnlichkeit mit der Abfrage des Inhabers einer Telefonnummer. Ihr Erkenntniswert bleibt jedenfalls punktuell. Systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen lassen sich allein auf der Grundlage von Auskünften aus IP-Adressen an der Quelle einer Verbindung nicht verwirklichen (vergleiche Bundesverfassungsgericht, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, Randnummer 256; Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, Randnummer 169). Eine Auskunft darf allerdings nicht ins Blaue hinein eingeholt werden: Wie bei jeder Ermittlungsmaßnahme bedarf es eines hinreichenden Anfangsverdachts auf einzelfallbezogener Tatsachenbasis, da im Ermittlungsverfahren keine anlasslose Ausforschung zur Verdachtsgewinnung zulässig ist (vergleiche Kölbel/Ibold, in: Münchener Kommentar zur Strafprozessordnung 2. Auflage 2024, § 160 Randnummer 71; Bundesverfassungsgericht, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, Randnummer 261; Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, Randnummer 145).

Sofern auch die Portnummer bekannt ist, sollte diese neben Zeitstempel und IP-Adresse in das Ersuchen mit aufgenommen werden. Nur wenn die Portnummer in das Ersuchen aufgenommen ist, besteht die sichere Aussicht, dass der Verpflichtete eine Auskunft erteilen kann. In einigen Fällen wird die Portnummer den Strafverfolgungsbehörden allerdings nicht bekannt sein. Auch in diesen Fällen können die Strafverfolgungsbehörden um Auskunft ersuchen, und es besteht eine Chance, dass der Verpflichtete diese auch hier erteilen kann (vergleiche die Begründung zur Änderung des Telekommunikationsgesetzes in Artikel 6 Nummer 2 zu § 177 Absatz 1).

Die mit der Erhebungsnorm korrespondierenden Verarbeitungsbefugnisse der Diensteanbieter ergeben sich für öffentlich zugängliche Telekommunikationsdienste aus § 174 Absatz 1 Satz 3 TKG und für digitale Dienste aus § 22 Absatz 1 Satz 3 TDDDG.

Bislang verweist die Vorschrift auch auf § 177 Absatz 1 Nummer 3 TKG. Dieser Verweis war zu streichen, da die europarechtswidrige Vorschrift aufgehoben ist. Gestrichen wird auch der geltende § 100j Absatz 2 Satz 2, wonach das Vorliegen der Voraussetzungen für ein Auskunftsverlangen nach Satz 1 aktenkundig zu machen ist. Die Vorschrift ist überflüssig, da die Grundsätze der ordnungsgemäßen Aktenführung ohnehin erfordern, dass Akten vollständig und inhaltlich richtig sind, um einer rechtsstaatlichen Kontrolle zugänglich zu sein. Die rechtlichen und tatsächlichen Grundlagen für eine Bestandsdatenauskunft sind daher auch aktenkundig zu machen (vergleiche auch Bundesverfassungsgericht, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, Randnummer 261; Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, Randnummer 248 ff.).

Zu Absatz 3

Bislang trifft § 100j Absatz 3 Verfahrensregelungen für die Bestandsdatenabfrage. Diese werden zur systematischen Bereinigung in § 101a verschoben; zur näheren Begründung siehe dort.

In der neuen Fassung enthält § 100j Absatz 3 die Regelungen, die sich bislang in § 100j Absatz 1 Satz 2 und 3 finden. Die Verschiebung erfolgt aus systematischen Gründen. Eine Änderung der Rechtslage geht damit nicht einher.

Zu § 100k (Erhebung von Nutzungsdaten bei digitalen Diensten)

§ 100k wird grundlegend redaktionell überarbeitet und in Struktur und Regelungsgehalt dem § 100g weiter angenähert. Dies ist sachgerecht, da § 100k die Befugnis zum Datenabruf bei Erbringern digitaler Dienste ermöglicht und damit in einer Konstellation gilt, die parallel zum Datenabruf bei Anbietern öffentlich zugänglicher Telekommunikationsanbieter (§ 100g) liegt.

§ 100k ist auch nach geltendem Recht ähnlich zu § 100g ausgestaltet: § 100g regelt die Erhebung von Verkehrsdaten bei Telekommunikationsunternehmen, § 100k die Erhebung von Nutzungsdaten bei digitalen Diensten. Die Überarbeitung der Vorschrift beseitigt Abweichungen zwischen beiden Normen, für die kein sachlicher Grund erkennbar ist.

Bereits nach geltender Rechtslage kann auf Grundlage von § 100k eine sogenannte Login-Falle geschaltet werden. Gemeint mit diesem Schlagwort ist die Konstellation, dass die Strafverfolgungsbehörden einen Beschuldigten noch nicht identifizieren konnten, aber Grund zu der Annahme haben, dass er regelmäßig einen bestimmten digitalen Dienst nutzt. In diesem Fall können die Strafverfolgungsbehörden, gestützt auf § 100k Absatz 1 oder 2, die bei einem frischen Login gespeicherte IP-Adresse und gegebenenfalls die verwendete Portnummer beim Erbringer des digitalen Dienstes erheben. Mit Zeitstempel, IP-Adresse und gegebenenfalls Portnummer kann der Anschlussinhaber durch eine Bestandsdatenabfrage nach § 100j Absatz 2 identifiziert werden.

Zu Absatz 1

Absatz 1 wird redaktionell angepasst. Entfallen kann der Verweis auf § 1 Absatz 4 Nummer 1 des Digitalen-Dienste-Gesetzes, in dem gesetzlich der Begriff des digitalen Dienstes definiert ist. Eine Änderung der Rechtslage geht damit nicht einher.

Die Vorschrift verweist künftig für den Abruf von Nutzungsdaten bei digitalen Diensten hinsichtlich der Voraussetzungen auf § 100g Absatz 1 Satz 1. Die Voraussetzungen für den Abruf sind nach bisher geltender Rechtslage identisch, es handelt sich also lediglich um eine redaktionelle Vereinfachung.

Unverändert bleibt auch der Begriff der digitalen Dienste, der sich nach § 1 Absatz 4 Nummer 1 des Digitale-Dienste-Gesetzes in Verbindung mit Artikel 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 richtet. Digitale Dienste sind danach Dienstleistungen der Informationsgesellschaft, das heißt jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Auch vernetzte smarte Systeme in Fahrzeugen, zu denen insbesondere auch Navigations- und Notrufsysteme zählen, unterfallen dem Begriff der digitalen Dienste, wenn sie eine auf individuellen Abruf erbrachte Dienstleistung darstellen. Entsprechend können die dabei entstehenden Fahrzeugdaten, wie etwa Standortdaten, Nutzungsdaten im Sinne von § 100k Absatz 1 sein (vergleiche Oberlandesgericht Frankfurt am Main, Beschluss vom 20. Juli 2021 − 3 Ws 369/21 zum damals geltenden Begriff der Telemediendienste nach § 1 Absatz 1 Satz 1 des zum 14. Mai 2024 außer Kraft getretenen Telemediengesetzes). Inhaltsdaten, die bei der Nutzung digitaler Dienste in vernetzten Fahrzeugen erzeugt werden, können hingegen nicht auf Grundlage von § 100k Absatz 1 erhoben werden.

Wie bei § 100g Absatz 1 können nach geltender Rechtslage auch bei Abfragen nach § 100k Absatz 1 neben den Nutzungsdaten des Beschuldigten (siehe zum Begriff des Beschuldigten die Ausführungen zu § 100g Absatz 1 Satz 1) auch Daten von sogenannten Nachrichtenmittlern erhoben werden. Dies ergibt sich derzeit – wie bei der

Verkehrsdatenerhebung – aus § 101a Absatz 1 Satz 1 in Verbindung mit § 100a Absatz 3. Zukünftig wird dies durch einen Verweis in § 100k Absatz 1 Satz 2 auf § 100g Absatz 1 Satz 2 geregelt.

Zu Absatz 2

Neu geregelt wird die Abrufbefugnis für Nutzungsdaten in Fällen, in denen die Straftat mittels eines digitalen Dienstes begangen worden ist. Bislang sieht § 100k Absatz 2 Satz 1 als weitere Voraussetzung einen Katalog von Straftaten vor. Bei der Parallelvorschrift des § 100g Absatz 2 neue Fassung (entspricht dem bisherigen § 100g Absatz 1 Satz 1 Nummer 2), der die Erhebung von Verkehrsdaten bei Verdacht einer mittels Telekommunikation begangenen Straftat betrifft, existiert ebenfalls kein Katalog. Die Vorschriften werden damit systematisch angeglichen. Dies drückt der fortan geltende Verweis auf § 100g Absatz 2 aus.

Entsprechend dem Verweis ist künftig die Erhebung von Nutzungsdaten in Fällen, in denen eine Straftat mittels eines digitalen Dienstes begangen worden ist, nur dann zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Dies ist – wie bei der entsprechenden Verkehrsdatenerhebung nach § 100g Absatz 2 – eine geringfügige Erweiterung der Abrufbefugnis, denn bislang ist der Abruf nur zulässig, wenn die Erforschung auf andere Weise aussichtslos wäre.

Zu Absatz 3

Absatz 3 regelt nun die Standortdatenabfrage bei dem Erbringer eines digitalen Dienstes. Derzeit ist sie in Bezug auf vorhandene (retrograde) Standortdaten unter den Voraussetzungen des § 100g Absatz 2 zulässig, im Übrigen bei Straftaten von im Einzelfall erheblicher Bedeutung, insbesondere solchen nach § 100a Absatz 2 (§ 100k Absatz 1 Satz 2 und 3); dies entspricht den geltenden Voraussetzungen für die Erhebung von Standortdaten bei einem Telekommunikationsdienst. Künftig wird dieser Gleichlauf auch normsystematisch deutlich, indem Absatz 3 unmittelbar auf die Voraussetzungen des neuen § 100g Absatz 3 verweist. Zu den neu geltenden Voraussetzungen siehe die Begründung zu § 100g Absatz 3.

Der Inhalt des bisherige § 100k Absatz 3 wird aus systematischen Gründen in Absatz 4 verschoben.

Zu Absatz 4

Die Vorschrift knüpft an den geltenden § 100k Absatz 3 an, wird aber an den neu geschaffenen § 100g Absatz 5 angepasst. Die dortigen Tatbestandsvoraussetzungen gelten entsprechend; dies gilt auch für den Datenkranz (IP-Adresse, Speicherzeitpunkt, etwaig erforderliche weitere, zur Identifizierung erforderliche Verkehrsdaten wie die Portnummer; siehe näher bei § 100g Absatz 5), der erhoben werden darf. Auf die Begründung dort wird verwiesen.

Zu Absatz 5

Die Vorschrift entspricht dem geltenden § 100k Absatz 4.

Zu Absatz 6

Absatz 6 führt den geltenden Absatz 5 fort. Die Vorschrift bleibt inhaltlich unverändert und wird nur geringfügig redaktionell angepasst: In der derzeit geltenden Fassung wird nicht nur auf die Erhebung von Nutzungsdaten, sondern auch auf „Inhalte der Nutzung“ abgestellt. Dies wurde im neuen Absatz 6 nicht übernommen, weil die Erhebung von

Inhaltsdaten weder nach alter noch nach neuer Rechtslage auf Grundlage von § 100k möglich ist. Bislang ist der digitale Dienst durch Verweis auf § 1 Absatz 4 Nummer 1 des Digitale-Dienste-Gesetzes definiert, doch kann dieser Verweis entfallen (siehe auch bei Absatz 1).

Zu Nummer 4 (§ 101a – Verfahrensregelungen bei Erhebung von Verkehrs-, Nutzungs- und Bestandsdaten)

In § 101a sind alle Verfahrensregelungen zu den §§ 100g, 100j und 100k zusammengefasst. Dies wird in der neu gefassten Überschrift der Norm ausgedrückt.

Die Norm wird rechtsförmlich insgesamt neu gefasst. Dabei werden die bislang in § 100j vorgesehenen Verfahrensregelungen für die Bestandsdatenauskunft in § 101a integriert.

Nicht fortgeführt wird der bisher geltende Absatz 4, der besondere Verwendungsregeln für verwertbare personenbezogene Daten enthält, die durch Maßnahmen nach dem geltenden § 100g Absatz 2, auch in Verbindung mit § 100g Absatz 1 Satz 3 oder Absatz 3 Satz 2, erhoben worden sind. Die Einführung der Vorschrift diente der Umsetzung der Vorgabe des Bundesverfassungsgerichts, nach der eine Weitergabe der im Rahmen einer Vorratsdatenspeicherung von Verkehrs- und Standortdaten gespeicherten und im Rahmen der Verkehrsdatenerhebung nach den genannten Vorschriften übermittelten personenbezogenen Daten an andere Stellen gesetzlich nur vorgesehen werden darf, soweit sie zur Wahrnehmung von Aufgaben erfolgte, derentwegen ein Zugriff auf diese Daten auch unmittelbar zulässig wäre (Bundesverfassungsgericht, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, Randnummer 236); die Regelung sollte damit eine Umgehung der engen Verwendungsregeln in § 113c Absatz 1 TKG alter Fassung verhindern (vergleiche Bundestagsdrucksache 18/5088, Seite 35). Da die Regelungen zur Vorratsdatenspeicherung von Verkehrs- und Standortdaten, auf die sich § 100g Absatz 2 geltender Fassung bezieht, wegen Unvereinbarkeit mit dem europäischen Recht unanwendbar sind und aufgehoben werden (siehe die Änderung des Telekommunikationsgesetzes), bedarf es keiner entsprechenden besonderen Verwendungsbeschränkung mehr. Für erhobene Daten gelten die Verwendungsbeschränkungen aus den allgemeinen Vorschriften, also aus § 161 Absatz 3 und § 479 Absatz 2.

Ebenfalls entbehrlich geworden ist der bisherige Absatz 5, der die Konstellation betrifft, dass personenbezogene Daten aus der europarechtswidrigen Vorratsdatenspeicherung durch eine polizeirechtliche Maßnahme erlangt worden sind.

Zu § 101a (Verfahrensregelungen bei Erhebung von Verkehrs-, Nutzungs- und Bestandsdaten)

Zu Absatz 1

Die Vorschrift enthält wie bislang einen Verweis auf Vorschriften des § 100a und § 100e zu Verfahrensregelungen hinsichtlich Datenerhebungen bei Telekommunikations- und digitalen Diensten. Diese Verweisung wird nun klarer strukturiert.

Zu Satz 1

Der geltende § 101a Absatz 1 verweist auf § 100a Absatz 3 und 4 sowie auf § 100e insgesamt. Dabei kann der Verweis auf § 100a Absatz 3, der die Adressaten der Maßnahme konkretisiert, entfallen, da diese Regelung unmittelbar in den Tatbestand der Verkehrsdatenerhebung aufgenommen ist, § 100g Absatz 1 Satz 2; hierauf verweist die Nutzungsdatenerhebung nach § 100k Absatz 1 Satz 2. Der Verweis auf § 100a Absatz 4, der Mitwirkungspflichten der Diensteanbieter betrifft, findet sich fortan in Absatz 5.

Fortan nicht mehr in Bezug genommen wird § 100e Absatz 2 sowie Absatz 3 Satz 2 Nummer 6 und 7. Diese Vorschriften betreffen besondere Verfahrensvorgaben für Maßnahmen der Online-Durchsuchung (§ 100b) und der akustischen Wohnraumüberwachung (§ 100c), die bei den hier gegenständlichen Erhebungen von Daten bei Diensteanbietern keine Entsprechung haben. Nicht mehr in Bezug genommen werden aus gleichem Grund § 100e Absatz 5 Satz 3 bis 5. In diesen Normen finden sich besondere Verfahrensbestimmungen für die Online-Durchsuchung nach § 100b und die Akustische Wohnraumüberwachung nach § 100c, wonach das anordnende Gericht auch über den Verlauf der Maßnahme zu unterrichten ist und gegebenenfalls das Gericht auch den Abbruch der Maßnahme anzuordnen hat. Der Verweis ist mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl. I 2017, S. 3202) neu eingeführt worden. Tatsächlich waren aber lediglich redaktionelle Folgeänderungen beabsichtigt (Bundestagsdrucksache 18/12785, Seite 58). Es ist auch sachlich nicht erforderlich, das Gericht nach Anordnung einer Verkehrsdaten- oder Nutzungsdatenerhebung laufend einzubeziehen, da die hier gegenständlichen Datenerhebungen in ihrer Eingriffsintensität nicht vergleichbar sind mit den Maßnahmen nach den §§ 100b und 100c.

Der Verweis auf § 100e Absatz 4 zu besonderen Vorgaben für die Begründung einer Anordnung oder Verlängerung kann entfallen, weil hierfür eine eigene Regelung in § 101a Absatz 2 besteht.

In den Nummern 1 bis 3 sind die Maßnahmen genannt, für die der Verweis auf die einzelnen Bestimmungen des § 100e gilt. Neben Maßnahmen nach § 100g Absatz 1 bis 4, den der geltende § 101a Absatz 1 betrifft, sind auch Maßnahmen nach § 100k Absatz 1 und 2 sowie nach § 100g Absatz 7 enthalten.

Auch hinsichtlich der neu in § 101a Absatz 1 aufgenommenen Maßnahmen, die auf gerichtlicher Entscheidung beruhen, ist künftig die Beschwerde gemäß § 304 Absatz 1 statthaft, ohne dass es dafür einer weiteren Rechtsänderung bedarf. Dies gilt auch dann, wenn ein Oberlandesgericht im ersten Rechtszug zuständig ist. Denn § 304 Absatz 4 Satz 2 Nummer 1 regelt in seiner geltenden Fassung allgemein, dass ausnahmsweise die Beschwerde gegen Beschlüsse und Verfügungen der Oberlandesgerichte, die im ersten Rechtszug zuständig sind, zulässig ist, welche die in § 101a Absatz 1 bezeichneten Maßnahmen – also auch die dort neu aufgenommenen – betreffen. Wegen der vergleichbaren Natur der genannten Maßnahmen ist die Erweiterung des Beschwerderechts sachgerecht. Hinsichtlich der Maßnahmen, die nicht auf gerichtlicher Entscheidung beruhen – zum Beispiel bei der Anordnung einer Sicherungsanordnung nach § 100g Absatz 7 durch die Staatsanwaltschaft – gelten die allgemeinen Rechtsschutzregeln; vergleiche hierzu auch die Begründung zu Absatz 4.

Zu Nummer 1

Die Vorschrift enthält Verfahrensregelungen zur Erhebung von Verkehrsdaten. In Bezug genommen werden lediglich § 100g Absatz 1 bis 4, in denen die Erhebung verschiedener Arten von Verkehrsdaten geregelt ist. Verfahrensregelungen zur Sicherungsanordnungen sind gesondert in Nummer 3 geregelt.

Die unter Buchstabe a getroffene Regelung entspricht Absatz 1 Satz 1 Nummer 1 in der geltenden Fassung. Die Regelung in Buchstabe b entspricht dem geltenden Absatz 1 Satz 3. Es handelt sich insoweit um rein redaktionelle Anpassungen.

Nicht fortgeführt wird der geltende Absatz 1 Satz 2. Danach findet in den Fällen des § 100g Absatz 2, auch in Verbindung mit § 100g Absatz 3 Satz 2, die Regelung zur Eilbefugnis der Staatsanwaltschaft nach § 100e Absatz 1 Satz 2 keine Anwendung. Dieses Ausschlusses bedarf es nicht mehr, da sich die Vorschriften auf den Abruf von

Daten aus der europarechtswidrigen Vorratsdatenspeicherung beziehen, die aus dem Gesetz getilgt werden.

Zu Nummer 2

In dieser Bestimmung sind besondere Verfahrensregelungen für die Nutzungsdatenerhebung nach § 100k Absatz 1 bis 3 enthalten.

Zu Buchstabe a

Die hier getroffene Maßnahme ist bislang in Absatz 1a enthalten sind. Die Vorschrift wird redaktionell angepasst; inhaltliche Änderungen gehen damit nicht einher.

Zu Buchstabe b

Ausdrücklich aufgenommen ist die Anforderung, dass in der Entscheidungsformel auch die zu übermittelnden Daten und der Zeitraum, für den sie übermittelt werden sollen, eindeutig anzugeben sind. Dies entspricht der parallelen Regelung zur Erhebung von Verkehrsdaten in Nummer 1 Buchstabe a.

Im bisherigen Absatz 1a ist auch ein Verweis auf § 100a Absatz 3 enthalten, der die Adressaten der Abfrage betrifft; dies ist nunmehr inhaltsgleich in § 100k Absatz 3 Satz 2 in Verbindung mit § 100g Absatz 1 Satz 2 geregelt und kann aus den Verfahrensregelungen gestrichen werden. Der bislang ebenfalls geregelte Verweis auf § 100a Absatz 4 wird aus redaktionellen Gründen in Absatz 5 verschoben.

Zu Nummer 3

Die Regelung enthält neue Verfahrensbestimmungen für die Sicherungsanordnung nach § 100g Absatz 7. Wie für die Verkehrsdatenabfrage selbst gelten auch für die vorgelagerte Sicherungsanordnung die Verfahrensbestimmungen aus § 100e, allerdings mit folgenden Maßgaben:

Zu Buchstabe a

Abweichend von § 100e Absatz 1 Satz 1 bis 3 kann die Staatsanwaltschaft die Sicherung selbst, also ohne Einbeziehung des Gerichts, anordnen. Bei Gefahr im Verzug steht diese Befugnis auch ihren Ermittlungspersonen zu. Dies ist sachgerecht: Die Sicherungsanordnung soll verhindern, dass flüchtige Daten verloren gehen, weil die tatsächlichen oder rechtlichen Voraussetzungen für die Herausgabe noch nicht erfüllt sind. Jeder Zeitverzug muss damit vermieden werden. Gleichzeitig bedarf es in diesem Stadium keiner gerichtlichen Kontrolle, da die Strafverfolgungsbehörden die Daten (noch) nicht herausverlangen können. Der Eingriff gegenüber dem Betroffenen ist daher relativ gering. Aus diesem Grund bedarf die Sicherungsanordnung abweichend von § 100e Absatz 1 Satz 3 auch keiner nachträglichen gerichtlichen Bestätigung.

Die Sicherung darf für einen Zeitraum von höchstens drei Monaten angeordnet werden. Häufig wird dies den Strafverfolgungsbehörden ausreichen, um die Abfragevoraussetzungen herzustellen. Eine Verlängerung ist einmalig um höchsten drei Monate möglich, kann aber nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden.

Zu Buchstabe b

Buchstabe b sieht vor, dass in der Entscheidungsformel auch die zu sichernden Daten und der Zeitraum, für den sie gesichert werden sollen, eindeutig anzugeben sind. Es handelt sich dabei um eine besondere Regelung für die Entscheidungsformel für die

Sicherung von Verkehrsdaten, die die Regelung für die Erhebung nach von Verkehrsdaten nach Nummer 1 Buchstabe a nachzeichnet.

Zu Buchstabe c

Buchstabe c sieht vor, dass bei Sicherung von Daten einer Funkzelle in der Entscheidungsformel auch eine räumlich und zeitlich eng begrenzte und hinreichend bestimmte Beschreibung der Telekommunikation ausreichend ist; dies entspricht der Regelung bei der Erhebung von Funkzellendaten nach Nummer 1 Buchstabe b.

Zu Satz 2

Die Vorschrift betrifft die Verfahrensregelungen zur Bestandsdatenabfrage nach dem neu gefassten § 100j Absatz 3, die sich auf besonders sensible Daten wie Passwörter bezieht. Die derzeit nach § 100j Absatz 3 bis 5 geltenden Verfahrensregelungen werden in § 101a Absatz 1 integriert und zugleich vereinfacht. Satz 2 enthält dabei – wie Satz 1 – einen Verweis auf Regelungen des § 100e. Der Verweis unterscheidet sich aber von jenem in Satz 1, da die dortigen Maßnahmen, zum Beispiel eine Erhebung von Verkehrsdaten, solche von längerer Dauer sein können. Bei einer Bestandsdatenabfrage, die auf die Herausgabe von Passwörtern gerichtet ist, kommt eine Verlängerung der Maßnahme hingegen nicht in Betracht. Dies liegt in der Natur der Sache: Passwörter können lediglich einmalig herausgegeben werden. Sofern Anhaltspunkte dafür bestehen, dass Passwörter geändert worden oder hinzugekommen sind, kommt eine neue Herausgabeanordnung in Betracht. Diese Einmalnatur spiegelt sich in den eingeschränkten Verweisen und Maßgaben wider.

Hinsichtlich der Anordnungskompetenz gilt das Folgende: Zum geltenden § 100j Absatz 1 Satz 3 (Auskunftsverlangen in Bezug auf als Bestandsdaten erhobene Passwörter oder andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird), ist derzeit geregelt, dass die Eilbefugnis der Staatsanwaltschaft keine Anwendung findet, § 100j Absatz 3 Satz 1. Umgekehrt ist zu § 100j Absatz 1 Satz 2 (Auskunftsverlangen in Bezug auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird) geregelt, dass auch Ermittlungspersonen bei Gefahr im Verzug tätig werden können (§ 100j Absatz 3 Satz 2). Zur Vereinfachung und Vereinheitlichung werden diese Sonderregelungen nicht fortgeführt. Es gilt stattdessen der Verweis auf § 100e Absatz 1 Satz 1, wonach im Grundsatz nur das Gericht auf Antrag der Staatsanwaltschaft eine Anordnung trifft; gemäß § 100e Absatz 1 Satz 2 kann die Staatsanwaltschaft bei Gefahr im Verzug tätig werden.

Die Maßgabe aus Nummer 1 bestimmt, dass die gerichtliche Entscheidung unverzüglich nachzuholen ist; dies ersetzt § 100e Absatz 1 Satz 2, wonach die Anordnung der Staatsanwaltschaft außer Kraft tritt, soweit sie nicht binnen drei Werktagen von dem Gericht bestätigt wird. Damit wird die schon bislang geltende Bestimmung aus § 100j Absatz 3 Satz 3 fortgeführt, wonach die gerichtliche Entscheidung unverzüglich nachzuholen ist. Regelungen zur Dauer und zur Verlängerung der Anordnung aus § 100e Absatz 1 Satz 4 und 5 werden nicht in Bezug genommen, da es sich um eine einmalige Abfrage handelt.

In den Verweis auf § 100e ist nicht in Bezug genommen Absatz 3 Satz 1 Nummer 5, der Vorgaben für die Entscheidungsformel bei Maßnahmen in Bezug auf eine Telekommunikationsverbindung betrifft. Dies hat, wie eingangs ausgeführt, bei der einmaligen Abfrage von Passwörtern keine Entsprechung. Aus dem gleichen Grund bestimmt die Maßgabe unter Nummer 2, dass in der Entscheidungsformel Dauer und Endzeit der Maßnahme nicht anzugeben sind.

Für Maßnahmen nach § 100j Absatz 2 neuer Fassung, also für den Abruf von Bestandsdaten anhand einer IP-Adresse, gilt weiterhin kein Verweis auf § 100e Absatz 1 und damit kein Richtervorbehalt. Er ist angesichts der überschaubaren Eingriffstiefe weder verfassungsrechtlich (vergleiche Bundesverfassungsgericht, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, Randnummer 261; Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, Randnummer 254) noch europarechtlich (vergleiche Europäischer Gerichtshof, Urteil vom 30. April 2024, Rechtssache C-470/21, Quadrature du Net II – Hadopi, Randnummer 132 f.) geboten.

Zu Satz 3

Diese Regelung übernimmt den bislang geltenden § 100j Absatz 3 Satz 4, wonach besondere Verfahrensregelungen dann keine Anwendung finden, wenn die betroffene Person vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. Nicht übernommen wurde der lediglich deklaratorische § 100j Absatz 3 Satz 5, wonach das Vorliegen der entsprechenden Voraussetzungen aktenkundig zu machen ist. Hierzu ist die aktenführende Strafverfolgungsbehörde nach dem Grundsatz der ordnungsgemäßen Aktenführung ohnehin verpflichtet (vergleiche auch die Begründung zu § 100j Absatz 2).

Zu Absatz 2

Die Vorschrift regelt besondere Vorgaben für die Begründung von Maßnahmen und entspricht damit dem bisher geltenden Absatz 2. Danach sind in der Begründung einzelfallbezogen die wesentlichen Erwägungen zur Erforderlichkeit und Angemessenheit der Maßnahme dazulegen. In den Anwendungsbereich neu aufgenommen ist zum einen die Sicherungsanordnung nach § 100g Absatz 7. Zum anderen ist die Bestandsdatenabfrage in Bezug auf besonders sensible Daten, insbesondere Passwörter, nach § 100j Absatz 3 ergänzt. Es ist anzunehmen, dass die Strafverfahrenspraxis mit Blick auf die Sensibilität der Daten dem auch bislang schon nachgekommen ist; insoweit handelt es sich lediglich um eine Klarstellung.

Der bislang in § 101a Absatz 1 Satz 1 enthaltene Verweis auf § 100e Absatz 4, der ebenfalls Vorgaben für die Begründung von Maßnahmen enthält, kann entfallen.

Zu Absatz 3

In dieser Vorschrift ist die Kennzeichnungs-, Auswertungs- und Löschpflicht der erhobenen Daten geregelt. Dies entspricht dem bisherigen Absatz 3. Auch hier ist die Bestandsdatenabfrage in Bezug auf besonders sensible Daten nach § 100j Absatz 3 aufgenommen. Zur Begründung gilt das zu Absatz 2 Ausgeführte entsprechend. Nicht aufgenommen sind die Daten, die auf Grundlage einer Identifizierungsdaten bei OTT-1-Diensten nach dem neu geschaffenen § 100g Absatz 5 erhoben werden. Dies entspricht der geltenden Rechtslage zu den Daten aufgrund einer Identifizierungsdatenabfrage nach § 100k Absatz 3. Nicht aufgenommen ist ferner die Sicherungsanordnung nach § 100g Absatz 7, da Daten, deren Sicherung angeordnet ist, (noch) nicht erhoben sind und folglich nicht gekennzeichnet werden können.

Entfallen kann Absatz 3 Satz 2 der geltenden Fassung, der die Kennzeichnung für Daten betrifft, die aus der europarechtswidrigen Vorratsdatenspeicherung stammen, da die Vorschriften über diese Vorratsdatenspeicherung aus dem Gesetz getilgt werden.

Zu Absatz 4

Die Vorschrift regelt die Benachrichtigungspflicht.

Satz 1 bestimmt, dass eine Benachrichtigung bei einer Verkehrsdatenerhebung nach § 100g Absatz 1 bis 5 sowie bei einer Nutzungsdatenerhebung nach § 100k Absatz 1 bis 4 zu erfolgen hat. Dies entspricht der geltenden Rechtslage (vergleiche Absatz 6 Satz 1 und Absatz 7 Satz 1), wobei die Benachrichtigungspflicht für Erhebungen auf Grundlage von § 100g Absatz 5 jener von § 100k Absatz 4 nachgebildet ist.

Aufgenommen ist auch die Bestandsdatenerhebung anhand einer IP-Adresse (§ 100j Absatz 2) und in Bezug auf besondere Daten wie Passwörter (§ 100j Absatz 3). Bislang gilt hierfür mit § 100j Absatz 4 eine eigene Benachrichtigungsregel, die zur Vereinfachung aufgehoben wird. Gleiches gilt für die besondere Benachrichtigungsregel in § 101a Absatz 7 Satz 1 geltender Fassung für die Identifikationsdatenabfrage nach § 100k Absatz 3 geltender Fassung (Absatz 4 neuer Fassung).

In Satz 2 wird hinsichtlich der näheren Regelungen zur Benachrichtigungspflicht auf § 101 Absatz 4 Satz 2 bis 5 und Absatz 5 bis 7 verwiesen, der die Benachrichtigung bei verdeckten Maßnahmen betrifft. Der Verweis entspricht dem bislang für die Erhebung von Verkehrsdaten und von Nutzungsdaten in Bezug auf besondere Daten wie Passwörter geltenden Absatz 6 Satz 2. Die derzeit geltenden Maßgaben – dass ein Absehen von einer Benachrichtigung nach § 101 Absatz 4 Satz 3 (Absatz 6 Satz 2 Nummer 1) und auch die erstmalige Zurückstellung einer Benachrichtigung nach § 101 Absatz 5 Satz 1 einer gerichtlichen Anordnung bedarf (Absatz 6 Satz 2 Nummer 2) – können entfallen. Diese Maßgaben hatte der Gesetzgeber mit Blick auf Transparenzvorgaben des Bundesverfassungsgerichts in seinem Urteil vom 2. März 2010 – 1 BvR 256/08, BVerfGE 125, 260–385 – getroffen (vergleiche Bundestagsdrucksache 18/5088, Seite 36). Diese Vorgaben bezogen sich aber auf eine Vorratsdatenspeicherung von Verkehrs- und Standortdaten; solche Speicherpflichten werden aus dem Gesetz getilgt. Es wäre auch nicht sachgerecht, wenn für die Benachrichtigung für die Erhebung von Verkehrsdaten und Nutzungsdaten weiter strengere Anforderungen gelten würden als bei heimlichen Maßnahmen wie etwa der Telekommunikationsüberwachung nach § 100a.

Wie eben dargestellt, gilt Satz 2 aus Gründen der Vereinfachung künftig auch für die Identifikationsdatenabfrage nach § 100k Absatz 4 neuer Fassung. Daraus ergeben sich folgende Änderungen: Bislang besteht die Möglichkeit, nach Absatz 7 Satz 2 die Benachrichtigung zurückzustellen, um die Vereitelung des Auskunftszwecks zu verhindern. Künftig ist nach § 101a Absatz 4 Satz 2 in Verbindung mit § 101 Absatz 5 Satz 1 geregelt, dass eine Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten, möglich ist. An die Stelle der Unterbleibensregelung aus Absatz 7 Satz 3 tritt jene aus § 101 Absatz 4 Satz 3, wobei künftig die Benachrichtigung nicht mehr allein deshalb unterbleiben kann, wenn schutzwürdige Belange Dritter entgegenstehen. Der geltende § 101a Absatz 7 Satz 4, der regelt, dass die Voraussetzungen nach Absatz 4 aktenkundig zu machen sind, kann entfallen, da dies ohnehin dem Gebot der Aktenmäßigkeit entspricht.

Für die Nutzungsdatenerhebung nach § 100k Absatz 4 ergeben sich infolge der dargestellten Vereinfachung (Aufhebung der Sonderregel in § 101a Absatz 7 und Verweis auf § 101 Absatz 4) folgende Änderungen: Neu ist der Verweis in § 101a Absatz 4 Satz 2 auf § 101 Absatz 4 Satz 2, der zum Hinweis auf nachträglichen Rechtsschutz verpflichtet. Neu ist auch der Verweis auf § 101 Absatz 4 Satz 5, wonach Nachforschungen zur Feststellung der Identität der zu benachrichtigenden Person nur vorzunehmen sind, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist. Neu ist auch, dass gemäß § 101 Absatz 6 eine Zurückstellung der Benachrichtigung über zwölf Monate hinaus der gerichtlichen Zustimmung bedarf. Ferner richtet sich künftig der Rechtsschutz nach § 101 Absatz 7 Satz 2 bis 4 statt, wie bislang, nach § 98 Absatz 2 Satz 2 in analoger Anwendung und § 304.

Für die Bestandsdatenerhebung anhand einer IP-Adresse und in Bezug auf besondere Daten wie Passwörter nach § 100j Absatz 2 und 3 neuer Fassung hat die Vereinfachung (Verweis auf § 101 Absatz 4 Satz 2 bis 5) die gleichen Folgen, wie sie zu § 100k Absatz 4 im vorigen Absatz beschrieben sind. Denn die bislang bestehende besondere Benachrichtigungspflicht nach § 100j Absatz 4 geltender Fassung (vergleiche zum verfassungsrechtlichen Hintergrund Bundesverfassungsgericht, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, Randnummer 263; Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, Randnummer 246) stimmt fast wortgleich mit § 101a Absatz 7 geltender Fassung überein.

Für die Sicherungsanordnung nach § 100g Absatz 7 wird keine Benachrichtigungspflicht eingeführt. Eine solche Pflicht würde erheblichen zusätzlichen Aufwand für die ohnehin stark belasteten Strafverfolgungsbehörden bedeuten. Hierfür besteht kein Bedarf. Denn wenn die gesicherten Daten erhoben werden, greift ohnehin die Benachrichtigungspflicht für Erhebungen nach § 100g Absatz 1 bis 4; ein Mehrwert für den Betroffenen an zwei Benachrichtigungen ist nicht ersichtlich. In dem Fall, dass die Daten nicht erhoben und gelöscht werden, ist das hypothetische Benachrichtigungsinteresse gering. Zu Zwecken der Transparenz wird aber eine Statistikpflicht eingeführt (siehe die Änderung von § 101b). Da keine Benachrichtigungspflicht nach Satz 1 angeordnet ist, gilt auch der Verweis nach Satz 2 auf § 101 Absatz 7 Satz 2 bis 4 nicht, der besondere Rechtsschutzregelungen vorsieht. Es verbleibt für die Sicherungsanordnung daher bei den anerkannten allgemeinen Rechtsschutzregelungen nach § 98 Absatz 2 Satz 2 in analoger Anwendung und § 304.

Zu Absatz 5

Diese Vorschrift verweist hinsichtlich der Mitwirkungspflicht der zur Auskunft Verpflichteten auf § 100a Absatz 4. § 100a Absatz 4 regelt, dass jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen die Ermittlungsmaßnahmen zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen hat. Für die zur Verkehrsdatenauskunft verpflichteten Telekommunikationsunternehmen gilt dieser Verweis bereits nach geltendem Recht gemäß Absatz 1 Satz 1 Halbsatz 1, für die zur Nutzungsdatenauskunft verpflichteten Erbringer von digitalen Diensten nach Absatz 1a. Neu in den Verweis aufgenommen ist die Bestandsdatenauskunft § 100j, zu der ebenfalls Telekommunikationsunternehmen und Erbringer von digitalen Diensten verpflichtet sind. Eine mit § 100a Absatz 4 vergleichbare Regelung findet sich im geltenden § 100j Absatz 5.

Zu Nummer 5 (§ 101b – Statistische Erfassung; Berichtspflichten)

§ 101b regelt die Anforderungen an die statistische Erfassung von Maßnahmen nach den §§ 100a ff. – also auch nach § 100g und § 100k – und die darauf aufbauenden Berichtspflichten der Länder und des Generalbundesanwalts. Diese Normen werden wie folgt angepasst:

Zu Buchstabe a

Es handelt sich um eine redaktionelle Änderung. Die Angabe der Absatzbezeichnungen von § 100k ist an dieser Stelle entbehrlich. Die genaue Bezeichnung der in den Übersichten anzugebenden Maßnahmen erfolgt in Absatz 6.

Zu Buchstabe b

Zu Doppelbuchstabe aa

In Absatz 5 Nummer 1 werden fortan § 100g Absatz 1 bis 4 und 7 einzeln aufgezählt. Damit geht einher, dass die Abfrage von Verkehrsdaten bei Straftaten von erheblicher Bedeutung (§ 100g Absatz 1), bei mittels Telekommunikation begangenen Straftaten (§ 100g Absatz 2), von Standortdaten (§ 100g Absatz 3) und von Funkzellenabfragen (§ 100g Absatz 4) getrennt erfasst werden. Dies gleicht die Gliederung der Angaben an jene zu § 100k an, denn dort sind Maßnahmen nach Absatz 1 (Straftaten von erheblicher Bedeutung) und Absatz 2 (mittels eines Telemedien- beziehungsweise digitalen Dienstes begangene Straftaten) bereits nach geltendem Recht getrennt darzustellen.

Außerdem wird auch die Anordnung einer Sicherungsanordnung statistikpflichtig (§100g Absatz 7). Damit wird auch ohne Benachrichtigung von Betroffenen von Sicherungsanordnungen Transparenz über diese Maßnahmen geschaffen (vergleiche oben die Begründung zu §101a Absatz 4 Satz 1).

Zu Doppelbuchstabe bb

Es handelt sich um eine Folgeänderung.

Zu Buchstabe c

Es handelt sich um eine Folgeänderung zur Neufassung von § 100k. Wie bislang sind berichtspflichtig die Erhebung von Nutzungsdaten bei erheblichen Straftaten (§ 100k Absatz 1), von mittels digitaler Dienste begangenen Straftaten (§ 100k Absatz 2) und von Standortdaten (§ 100k Absatz 3). Neu ist lediglich, dass die letzte Gruppe getrennt darzustellen ist. Dies entspricht den Kategorien der Erfassung zu § 100g.

Zu Nummer 6 (§ 160a – Maßnahmen bei zeugnisverweigerungsberechtigten Berufsgeheimnisträgern)

§ 160a trifft allgemeine Regelungen in Bezug auf Maßnahmen bei zeugnisverweigerungsberechtigten Berufsgeheimnisträgern. In Absatz 5 wird derzeit darauf hingewiesen, dass § 100g Absatz 4 unberührt bleibt. Da diese Vorschrift entfällt (siehe dazu die Begründung zu § 100g, vor Absatz 1), ist als redaktionelle Folgeänderung dieser Hinweis zu streichen.

Zu Artikel 2 (Änderung des Einführungsgesetzes zur Strafprozessordnung)

Die Vorschrift des § 12 wird neu gefasst. Bislang enthält die Vorschrift eine Übergangsregelung zum Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, die obsolet geworden ist.

Künftig legt § 12 das Jahr fest, für das die statistischen Übersichten erstmals in dem auf das Inkrafttreten der neuen Fassung von § 101b Absatz 5 und 6 folgende Berichtsjahr zu erstellen sind. Im gleichen Jahr ist auch erstmals über die Sicherungsanordnung nach § 100g Absatz 7 zu berichten.

Zu Artikel 3 (Änderung des Elektronische-Beweismittel-Umsetzungs-und-Durchführungsgesetzes)

Die Änderungen führen die nötigen Bestimmungen ein, um die Europäischen Sicherungsanordnung nach der Verordnung (EU) 2023/1543 durchführbar zu machen.

Zu Nummer 1 (Inhaltsübersicht)

Es handelt sich um eine redaktionelle Folgeänderung zu Nummer 2.

Zu Nummer 2 (§ 10a – Verfahren bei Europäischen Sicherungsanordnungen)

§ 10a konkretisiert Artikel 4 Absatz 3 und 5 sowie Artikel 6 der Verordnung (EU) 2023/1543. Dort ist geregelt, unter welchen Voraussetzungen Mitgliedstaaten Europäische Sicherungsanordnungen erlassen können. Aus Artikel 4 Absatz 3 geht zunächst hervor, dass bei Europäischen Sicherungsanordnungen – anders als bei Europäischen Herausgabeanordnungen – keine Abstufung nach Datenkategorien greift. Die Vorgaben zu den Zuständigkeiten aus Artikel 4 Absatz 3 gelten demnach für sämtliche Datenkategorien.

Aus Artikel 6 Absatz 2 der Verordnung (EU) 2023/1543 ergibt sich, dass Europäische Sicherungsanordnungen ein späteres Ersuchen um Herausgabe vorbereiten und zu diesem Zweck notwendig und verhältnismäßig sein müssen. Für die Herausgabe der Daten kann, neben einer Europäischen Herausgabeanordnung, auch eine Europäische Ermittlungsanordnung oder ein sonstiges Rechtshilfeersuchen gewählt werden.

Daneben nimmt Artikel 6 Absatz 3 eine Differenzierung im Hinblick auf Europäische Sicherungsanordnungen zur Strafverfolgung auf der einen und zur Strafvollstreckung auf der anderen Seite vor: Für Strafverfolgungskonstellationen gilt – wie bei Europäischen Herausgabeanordnungen – die Entsprechungsklausel. Das bedeutet, dass Europäische Sicherungsanordnungen ausschließlich in den Fällen erlassen werden können, in denen eine Sicherung auch nach den nationalen Regelungen möglich ist. Für Fälle der Strafvollstreckung sieht die Verordnung hingegen keine solche Beschränkung vor und legt lediglich über die Strafhöhe beziehungsweise die Art der Maßregel fest, in welchen Fällen Europäische Sicherungsanordnungen erlassen werden können. Dies wurde auf europäischer Ebene im Rahmen der Trilogverhandlungen so entschieden. In Konstellationen, in denen bereits ein rechtskräftiges Urteil besteht, dürfte der Betroffene als weniger schutzwürdig einzuschätzen sein. Gegebenenfalls bestehende Restriktionen des nationalen Rechts gelten daher in der Vollstreckungsphase nicht mehr. Die Verordnung beschränkt die so vorgenommene Differenzierung auf die Europäische Sicherungsanordnung; im Rahmen der Europäischen Herausgabeanordnung gilt die Entsprechungsklausel sowohl für die Strafverfolgungs- als auch für die Vollstreckungsphase. Hieran ist der nationale Gesetzgeber gebunden.

§ 10a des Gesetzes regelt vor diesem Hintergrund die Zuständigkeit der jeweiligen Anordnungsbehörden wie folgt:

Zu Absatz 1

Absatz 1 bestimmt, dass sich die Zuständigkeit der Staatsanwaltschaften für den Erlass von Europäischen Sicherungsanordnungen zu Strafverfolgungszwecken nach Artikel 4 Absatz 3 Buchstabe a der Verordnung (EU) 2023/1543 nach dem Achten Abschnitt des ersten Buchs der Strafprozessordnung richtet. Dort befinden sich die Rechtsgrundlagen für die Datensicherung.

Aufgrund der nach Artikel 6 Absatz 3 der Verordnung geltenden Entsprechungsklausel für Strafverfolgungsfälle (siehe oben) ist dabei auf die Regelung des § 100g Absatz 7 StPO neuer Fassung abzustellen, wonach eine Sicherungsanordnung für Verkehrsdaten erlassen werden kann. § 101a Absatz 1 Satz 1 Nummer 3 Buchstabe a StPO bestimmt zudem, dass abweichend von § 100e Absatz 1 Satz 1 bis 3 StPO für die ersten drei Monate die Staatsanwaltschaft für eine solche Sicherungsanordnung zuständig ist. Die Anordnungsbefugnis liegt also zunächst allein bei der Staatsanwaltschaft. Die Dauer der Sicherung richtet sich sodann nach Artikel 11 Absatz 1 bis 3 der Verordnung (EU)

2023/1543. Abweichend vom nationalen Recht beträgt sie zunächst 60 Tage, verlängerbar nach den in der zitierten Vorschrift genannten Maßgaben. Da die in Artikel 6 Absatz 2 der Verordnung enthaltene Entsprechungsklausel (siehe dazu oben) nur für die Anordnung der Sicherung gilt, nicht jedoch für deren Aufrechterhaltung, findet § 100e Absatz 1 Satz 4 keine Anwendung. Es bedarf also keines Gerichtsbeschlusses, um eine Verlängerung der Datensicherung aufgrund einer Europäischen Sicherungsanordnung beim Adressaten zu beantragen.

Zu Absatz 2

Absatz 2 basiert auf Artikel 4 Absatz 3 Buchstabe b und Artikel 4 Absatz 5 der Verordnung (EU) 2023/1543. Artikel 4 Absatz 3 Buchstabe b ergänzt die Regelung des Buchstaben a, welche die primär für den Erlass von Sicherungsanordnungen zuständigen Stellen aufführt (siehe dazu oben). Buchstabe b räumt den Mitgliedstaaten die Möglichkeit ein, weitere Behörden zu benennen, die in dem betreffenden Fall nach nationalem Recht für die Anordnung der Erhebung von Beweismitteln zuständig sind. Im Rahmen der nationalen Vorgaben dürfen auch diese Behörden Europäische Sicherungsanordnungen erlassen, sie müssen sie jedoch von einem Richter, einem Gericht, einem Ermittlungsrichter oder einem Staatsanwalt validieren lassen.

Die StPO kennt keine generelle Erlasszuständigkeit der in Absatz 2 Nummer 1 bis 3 aufgeführten Stellen, sodass eine allgemeine Ermächtigung nach Artikel 4 Absatz 3 Buchstabe b der Verordnung nicht möglich ist. Jedoch sind die genannten Behörden gemäß § 101a Absatz 1 Satz 1 Nummer 3 Buchstabe a StPO neue Fassung bei Gefahr im Verzug (neben der Staatsanwaltschaft, siehe dazu oben zu Absatz 1) befugt, eine (nationale) Sicherungsanordnung zu erlassen. Für diese Eilkonstellation ist damit eine Benennung nach Artikel 4 Absatz 5 in Verbindung mit Artikel 4 Absatz 3 Buchstabe b der Verordnung möglich. Allerdings sind weitere, einschränkende Vorgaben der Verordnung zu beachten, die in Artikel 4 Absatz 5 das Vorgehen im „begründeten Notfall“ regelt. Im Einzelnen bedeutet dies: In einem rein nationalen Fall muss ein Gericht erst – und nur dann – eingeschaltet werden, wenn die Maßnahme über drei Monate hinaus verlängert werden soll (§ 101a Absatz 1 Satz 1 Nummer 3 Buchstabe a StPO neue Fassung). Die Verordnung hingegen sieht in Artikel 4 Absatz 5 auch in einem „begründeten Notfall“ eine Validierung vor, die innerhalb von 48 Stunden angefordert werden muss. Artikel 3 Nummer 18 der Verordnung, auf den Artikel 4 Absatz 5 verweist, definiert den „begründeten Notfall“ als „eine Situation, in der eine unmittelbare Gefahr für das Leben, die körperliche Unversehrtheit oder die Sicherheit einer Person oder für eine kritische Infrastruktur im Sinne des Artikels 2 Buchstabe a der Richtlinie 2008/114/EG besteht, wenn die Störung oder Zerstörung einer kritischen Infrastruktur zu einer unmittelbaren Gefahr für das Leben, die körperliche Unversehrtheit oder die Sicherheit einer Person führen würde, auch durch die schwere Beeinträchtigung der Bereitstellung der Grundversorgung für die Bevölkerung oder der Wahrnehmung der Kernfunktionen des Staates“. Der Eilfall wird damit in der Verordnung enger gefasst als im nationalen Recht, das „Gefahr im Verzug“ (Eintritt eines Schadens oder Beweismittelverlust) für eine Anordnung durch beispielsweise Ermittlungspersonen der Staatsanwaltschaft ohne Einbindung einer Justizbehörde ausreichen lässt. Da die Anwendung nationalen Rechts bei den grenzüberschreitenden Fällen gegenüber der Verordnung nachranging ist, müssen deren Voraussetzungen und Abläufe eingehalten werden. Obgleich im nationalen Recht nicht vorgesehen, müssen die in Absatz 2 Nummer 1 bis 3 genannten Stellen in den hier adressierten Notfällen mit grenzüberschreitender Sicherungsanordnung damit innerhalb von 48 Stunden eine Validierung beantragen.

In Nummer 1 sind die Ermittlungspersonen der Staatsanwaltschaft aufgeführt, die in nationalen Fällen gemäß § 101a Absatz 1 Satz 1 Nummer 3 Buchstabe a StPO neue Fassung bei Gefahr im Verzug ebenfalls Sicherungsanordnungen erlassen können. Darunter fallen neben Polizeibeamten insbesondere die Beamten der Finanzbehörden und der Zollverwaltung in den Fällen, in denen sie qua gesetzlicher Zuschreibung als

Ermittlungspersonen der Staatsanwaltschaft tätig werden (zum Beispiel § 404 der Abgabenordnung, § 14 des Gesetzes zur Bekämpfung der Schwarzarbeit, § 21 des Außenwirtschaftsgesetzes).

Die Nummern 2 und 3 ermächtigen die Finanzbehörden und die Behörden der Zollverwaltung darüber hinaus auch in den Konstellationen, in denen sie nicht als Ermittlungspersonen der Staatsanwaltschaft tätig werden, sondern per gesetzlicher Regelung in deren Stellung eintreten. Dabei handelt es sich um die selbstständige Ermittlungsbefugnis der Finanzbehörden nach § 399 Absatz 1 und § 386 Absatz 2 der Abgabenordnung (beispielsweise bei ausschließlichen Steuerstraftaten) und nach den in den §§ 14a und 14b des Gesetzes zur Bekämpfung der Schwarzarbeit aufgeführten Fällen. Die Benennung dieser Behörden als bloß sekundär zuständige Anordnungsbehörden, deren Anordnungen in Notfallkonstellationen ebenfalls einer nachträglichen Validierung durch die Staatsanwaltschaft bedürfen, resultiert aus dem Wortlaut der Verordnung (die in Artikel 4 Absatz 1 Buchstabe a von „Staatsanwaltschaft“ spricht) und aus der zur vergleichbaren Auslegungsfrage ergangenen Rechtsprechung des Europäischen Gerichtshofs zur Europäischen Ermittlungsanordnung (Urteil von 2. März 2023, Rechtssache C-16/22, Staatsanwaltschaft Graz [Finanzamt für Steuerstrafsachen Düsseldorf]).

Zu Absatz 3

Absatz 3 regelt den Ablauf der Ex-Post-Validierung. Die Verordnung normiert das nachträgliche Validierungsverfahren nicht, weswegen es im nationalen Recht ausgestaltet werden muss. Sofern eine Anordnungsbehörde nach Absatz 2 in Notfällen tätig geworden ist, übermittelt sie die Anordnung nach Absatz 3 Satz 1 an die Staatsanwaltschaft binnen der in Artikel 4 Absatz 5 der Verordnung vorgesehenen Frist (48 Stunden). Dies geschieht in elektronischer Form unter Nutzung des nach Artikel 19 Absatz 1 der Verordnung vorgeschriebenen Übermittlungsweges über das dezentrale IT-System, an das alle beteiligten Stellen des Anordnungs- und Validierungsprozesses anzuschließen sind. Die Staatsanwaltschaft überprüft die Rechtmäßigkeit der ergangenen Anordnung anhand der in der Verordnung (EU) 2023/1543 enthaltenen Voraussetzungen (Artikel 4 Absatz 3 und 5 sowie Artikel 5). Im Falle der Ex-Post-Validierung macht sie diese aktenkundig. Der Adressat wird nicht gesondert informiert (vergleiche Anhang II, Abschnitt F). Um der Anordnungsbehörde zu ermöglichen, im Falle der Ablehnung einer Ex-Post-Validierung die Anordnung sofort zurückzuziehen (Artikel 4 Absatz 5 VO), ist eine entsprechende Information über die ablehnende Entscheidung erforderlich. Eine solche Regelung soll in die Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (RiVASt) integriert werden.

Zu Absatz 4

Absatz 4 regelt die örtliche Zuständigkeit für die Validierung (die sachliche Zuständigkeit ergibt sich aus Absatz 3). Wie bei § 9 Absatz 4 ist gemäß Satz 1 hierfür grundsätzlich, ihrer Stellung als Herrin des Ermittlungsverfahrens entsprechend, die ermittlungsführende Staatsanwaltschaft zuständig; dies kann auch der Generalbundesanwalt sein. So wird inhaltliche Kontinuität gewährleistet.

Soweit die sekundär zuständige Anordnungsbehörde nach nationalem Recht die Ermittlungen selbst führt, ist die Staatsanwaltschaft zuständig, in deren Landgerichtsbezirk die anordnende Behörde ihren Sitz hat.

Die Länder können von der örtlichen Zuständigkeit abweichende Regelungen treffen, beispielsweise aus Gründen der Spezialisierung.

Zu Absatz 5

Absatz 5 trifft eine Zuständigkeitsbestimmung für den Erlass Europäischer Sicherungsanordnungen zu Strafvollstreckungszwecken. Da dabei die Entsprechungsklausel aufgrund des Wortlauts in Artikel 6 Absatz 3 der Verordnung (EU) 2023/1543 keine Anwendung findet (siehe oben), sind die Vorgaben des nationalen Rechts nicht automatisch zu beachten. Zur Vereinfachung der Rechtsanwendung erscheint es jedoch sinnvoll, auf einen Gleichlauf mit nationalen Zuständigkeiten zu achten. Deswegen benennt Absatz 5 die Staatsanwaltschaft als zuständige Stelle. Betrifft die Strafvollstreckung einen zu Jugendstrafe verurteilen Jugendlichen oder Heranwachsenden, ist für die Sicherungsanordnung der Jugendrichter als Vollstreckungsleiter zuständig. Letzteres gilt auch für die Vollstreckung der Unterbringung in einem psychiatrischen Krankenhaus und in einer Entziehungsanstalt. Dies bewegt sich im Rahmen der Vorgaben von Artikel 4 Absatz 3 Buchstabe a der Verordnung. Hiernach ist sowohl eine richterliche als auch eine staatsanwaltschaftliche Befugnis gegeben.

Daneben eine sekundär zuständige Stelle zu benennen, ist nicht möglich. Denn der Wortlaut von Artikel 4 Absatz 3 Buchstabe b der Verordnung bezieht sich ausdrücklich nur auf Ermittlungsbehörden und die Erhebung von Beweismitteln. Strafvollstreckungskonstellationen sind damit nicht erfasst.

Zu Artikel 4 (Änderung des Justizvergütungs- und -entschädigungsgesetzes)

Die Entschädigungsregelung für Auskünfte über Bestandsdaten, zu deren Erteilung auf Verkehrsdaten zurückgegriffen werden muss (Nummer 201 der Anlage 3 JVEG), soll angepasst werden. Da der zeitliche Aufwand für diese Auskunftserteilung mit demjenigen der Auskunftserteilung nach Nummer 202 der Anlage 3 zum JVEG vergleichbar ist, soll der Entschädigungsbetrag entsprechend angeglichen werden. Im Gegenzug soll mit der Pauschale nur noch die Abfrage von bis zu drei statt bisher zehn Kennungen abgegolten sein. In der Praxis dürfte sich diese Reduzierung kaum auswirken, da die Strafverfolgungsbehörden regelmäßig nur eine einzige Kennung je Auskunftsbegehren abfragen.

Die Nummern 309 bis 311 der Anlage 3 zum JVEG enthalten Entschädigungstatbestände für Leitungskosten für die Übermittlung von Verkehrsdaten. Mit der vorgeschlagenen Vorbemerkung 3 soll ein Gleichlauf mit der Regelung für die Leitungskosten im Zusammenhang mit der Überwachung der Telekommunikation in Abschnitt 1 der Anlage 3 zum JVEG hergestellt werden. Leitungskosten sollen auch hier nur entschädigt werden, wenn die betreffende Leitung mindestens einmal zur Übermittlung von Verkehrsdaten genutzt worden ist. Außerdem soll klargestellt werden, dass die Entschädigung für den gesamten Übermittlungszeitraum erfolgt.

Darüber hinaus sollen in das JVEG Entschädigungsregelungen für diejenigen Leistungen aufgenommen werden, die von Telekommunikationsunternehmen im Zusammenhang mit Sicherungsanordnungen zu erbringen sind.

Die Ermäßigungsregelung nach Absatz 2 der Allgemeinen Vorbemerkung soll auch für den Fall der Sicherungsanordnung gelten. Zudem sind die Überschriften der Abschnitte 3 und 4 anzupassen.

Der vorgeschlagene neue Abschnitt 5 enthält Entschädigungsregelungen insbesondere für die Sicherung von Verkehrsdaten durch Telekommunikationsunternehmen. Die Tatbestände sowie die Entschädigungsbeträge orientieren sich an den jeweils korrespondierenden Vorschriften der Abschnitte 3 und 4 zur Entschädigung von Auskünften ohne vorhergehende Sicherungsanordnung.

Für die Auskunft über Daten, die aufgrund einer vorausgegangenen Sicherungsanordnung vom Telekommunikationsunternehmen gespeichert sind, wird im neuen Abschnitt 6 eine Entschädigung in Höhe von 20 Euro vorgesehen. Dabei wird davon ausgegangen, dass aufgrund der Vorbefassung im Rahmen der Umsetzung der Sicherungsanordnung der Aufwand für die spätere Beauskunftung dieser Daten regelmäßig vergleichsweise gering ist. Der erhöhte Aufwand, der den Telekommunikationsunternehmen entstehen kann, wenn in einzelnen Fällen die Auskunft lediglich für eine Teilmenge der gesicherten Daten verlangt wird, ist hierbei berücksichtigt.

Zu Artikel 5 (Änderung des Gesetzes über Ordnungswidrigkeiten)

Es handelt sich um eine redaktionelle Folgeänderung zur Änderung von § 100j StPO.

Zu Artikel 6 (Änderung des Telekommunikationsgesetzes)

Zu Nummer 1 (Inhaltsübersicht)

Das amtliche Inhaltsverzeichnis ist entsprechend der unter Nummer 2 erfolgenden Änderungen, die untenstehend erläutert werden, anzupassen.

Zu Nummer 2 (§§ 175 bis 177)

Die bisherigen §§ 175 bis 181 werden ersatzlos gestrichen. Es handelt sich dabei um die bestehenden weitergehenden Regelungen zu einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung von Verkehrs- und Standortdaten. Sie sind spätestens seit der durch Urteil des Bundesverwaltungsgerichts vom 14. August 2023 (6 C 6.22 und 6 C 7.22) festgestellten Unvereinbarkeit mit dem Unionsrecht unanwendbar und daher zu streichen. Die §§ 175 bis 177 werden neu gefasst und enthalten künftig Regelungen zur Auskunftserteilung über Verkehrsdaten an Strafverfolgungs- und Sicherheitsbehörden (§ 175), zur Verarbeitung von Verkehrsdaten aufgrund von Sicherungsanordnungen (§ 176) und zur Speicherpflicht und Verwendungsbefugnis von Verkehrsdaten zur Identifizierung von Anschlussinhabern (§ 177).

Zu § 175 (Befugnis zur Verarbeitung von Verkehrsdaten zur Auskunftserteilung an Strafverfolgungs- und Sicherheitsbehörden)

§ 175 dient der Klarstellung und der Rechtssicherheit der betroffenen Telekommunikationsdienste im Hinblick auf die Befugnis zur Verarbeitung von Verkehrsdaten zum Zweck der Auskunftserteilung an bestimmte berechtigte Stellen. Eine entsprechende Regelung, die die betroffenen Telekommunikationsunternehmen zur Verarbeitung von Verkehrsdaten zum Zweck der Auskunftserteilung über Verkehrsdaten ausdrücklich ermächtigt, ist derzeit im TKG nicht vorhanden, obwohl für die in Absatz 3 genannten Stellen Rechtsgrundlagen für Auskunftsrechte sowie Erhebungsbefugnisse im Hinblick auf Verkehrsdaten bestehen. Nach der Rechtsprechung des Bundesverfassungsgerichts zu verfassungsrechtlichen Maßgaben zum Doppeltürmodell (Bundesverfassungsgericht, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, Randnummer) bedarf es aber neben den Rechtsgrundlagen der Behörden, die diese zum Ersuchen nach Auskunft und zur Datenerhebung berechtigen, zusätzlich der Befugnis der für die Datenverarbeitung verantwortlichen Telekommunikationsunternehmen, die Daten zum Zwecke der Auskunftserteilung zu verarbeiten (sogenannte Doppeltür).

Zu Absatz 1

Absatz 1 stellt klar, dass die betroffenen Unternehmen zur Verarbeitung von Verkehrsdaten zum Zwecke der Auskunftserteilung befugt sind, wenn die in Absatz 3 genannten Stellen diese unter Verweis auf die genannten Rechtsgrundlagen um Auskunft

über Verkehrsdaten ersuchen und hierzu die entsprechende Anordnung übermitteln. Gleiches gilt für Unternehmen beziehungsweise andere Netzbetreiber, denen sich ein Anbieter zur Erbringung seines Telekommunikationsdienstes als sogenannter Vorleister bedient, der die Verkehrsdaten für diesen verarbeitet.

Zu Absatz 2

Nach Absatz 2 haben die betroffenen Unternehmen bei der Entgegennahme von Auskunftsverlangen die genannten formalen Anforderungen zu beachten. Für die Gesetzmäßigkeit des Auskunftsverlangens und der Erhebung dieser Verkehrsdaten durch die ersuchenden Stellen sind allein diese verantwortlich.

Zu Absatz 3

Absatz 3 befugt die betroffenen Unternehmen, Auskünfte über Verkehrsdaten nach Absatz 1 Satz 1 allein den in den Nummern 1 bis 9 genannten Stellen zu erteilen, wobei die Unternehmen die materiell-rechtlichen Übermittlungsvoraussetzungen schon aus tatsächlichen Gründen nicht prüfen können und dementsprechend auch nicht prüfen müssen. Ihre Prüfung ist auf die Einhaltung der formalen Anforderungen nach Absatz 2 beschränkt.

Durch die Übermittlungsregelung des Absatzes 3 nimmt der Bundesgesetzgeber vielmehr seine verfassungsrechtliche Regelungsverantwortung dafür wahr, mit der Öffnung der Datenbestände privater Unternehmen für eine Verwendung zur staatlichen Aufgabenwahrnehmung (Zweckänderung) zugleich die geänderten Verwendungszwecke und wesentlichen Verwendungsvoraussetzungen zu bestimmen (vergleiche Bundesverfassungsgericht, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, Randnummer 130 ff.).

Nummer 2 ermächtigt zur Auskunftserteilung von Verkehrsdaten an Gefahrenabwehrbehörden der Länder, soweit dies im Einzelfall erforderlich ist zur Abwehr einer konkretisierten Gefahr für ein Rechtsgut von zumindest erheblichem Gewicht oder zur Abwehr einer konkreten Gefahr für die öffentliche Sicherheit. Für die Abwehr einer konkretisierten Gefahr müssen zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen (vergleiche dazu Bundesverfassungsgericht, Urteil vom 1. Oktober 2024 – 1 BvR 1160/19 – BVerfGE 141, 220–378, Randnummer 111 ff.).

Durch Nummer 7 erfolgt unter den dort genannten Voraussetzungen eine Ermächtigung zur Auskunftserteilung von Verkehrsdaten an die Verfassungsschutzbehörden der Länder für die Erfüllung des Aufklärungsauftrags des Verfassungsschutzes, der sich entweder entsprechend aus § 3 Absatz 1 des Bundesverfassungsschutzgesetzes oder aus den jeweiligen Landesverfassungsschutzgesetzen ableitet. Dies gilt insbesondere für den Schutz der verfassungsmäßigen Ordnung vor Bestrebungen und Tätigkeiten der organisierten Kriminalität.

Zu Absatz 4

Die die Auskunft erteilenden Unternehmen haben mit Verweis auf die Verschwiegenheitspflicht gemäß § 174 Absatz 6 Satz 2 im Interesse der gesetzmäßigen Aufgabenwahrnehmung durch die ersuchenden Stellen darüber Stillschweigen zu wahren.

In Absatz 4 wird zudem auf die Pflicht zur Anwendung der Regelungen zum elektronischen Verfahren zur Erteilung der Auskünfte sowie zur Datensicherheit und zum Datenschutz in § 174 Absatz 7 verwiesen. Diese Regelungen garantieren somit etablierte und standardisierte Verfahren für den Umgang mit behördlichen Auskunftsverlangen. Diese Verfahren ermöglichen den verpflichteten Unternehmen eine effiziente Bearbeitung

von Auskunftsverlangen sowie für die berechtigten Stellen ein standardisiertes, technisches Verfahren für die Übermittlung von Auskunftsersuchen.

Zu § 176 (Befugnis zur Verarbeitung von Verkehrsdaten zur Erfüllung von Sicherungsanordnungen)

§ 176 enthält eine Befugnis der Anbieter zur Verarbeitung von Verkehrsdaten im Rahmen der Umsetzung von Sicherungsanordnungen nach § 100g Absatz 7 StPO, § 10b Absatz 1 oder § 52 Absatz 3 des Bundeskriminalamtgesetzes und § 25a Absatz 1 des Bundespolizeigesetzes sowie hierauf bezogener Auskunftsverlangen. Ergänzend dazu ist eine Pflicht zur Umsetzung angemessener Maßnahmen zum Datenschutz und zur Datensicherheit geregelt.

Zu Absatz 1

Absatz 1 befugt einerseits Anbieter, die Adressaten einer Sicherungsanordnung nach § 100g Absatz 7 StPO oder nach § 10b Absatz 1 oder nach § 52 Absatz 3 des Bundeskriminalamtgesetzes und nach § 25a Absatz 1 des Bundespolizeigesetzes sind, zu der dafür erforderlichen Verarbeitung der durch die Nutzung des Dienstes vorhandenen sowie künftig anfallenden Verkehrsdaten (§ 3 Nummer 70). Gleiches gilt für Unternehmen beziehungsweise andere Netzbetreiber, denen sich ein Anbieter zur Erbringung seines Telekommunikationsdienstes als sogenannter Vorleister bedient, der die Verkehrsdaten für diesen verarbeitet. Dabei hat der Anbieter des Telekommunikationsdienstes auch die unverzügliche Sicherung der nicht von ihm selbst bei der Erbringung seines Dienstes erzeugten und verarbeiteten Daten sicherzustellen. Auf welche Weise der Erbringer die Sicherung sicherstellt, hat er gegenüber der Bundesnetzagentur auf deren Verlangen nachzuweisen. Durch Satz 2 erfasst die Datenverarbeitungsbefugnis auch die Beantwortung späterer Auskunftsverlangen der gesicherten Verkehrsdaten an die berechtigten Stellen unter den Voraussetzungen des § 175.

Die gesicherten Daten dürfen dabei nur auf ein Erhebungsersuchen hin herausgegeben werden, das unmittelbar mit der Sicherungsanordnung korrespondiert. Die Berechtigung zum Datenabruf folgt dabei der Zuständigkeit für das zugrundeliegende Verfahren. Ist die Sicherungsanordnung beispielsweise durch das Bundeskriminalamt als Zentralstelle erlassen worden und hat das Bundeskriminalamt das Verfahren zwischenzeitlich vor Abruf der Daten an die Staatsanwaltschaft eines Landes abgegeben, so ist ab dem Abgabezeitpunkt nur diese zum Datenabruf berechtigt. Voraussetzung ist dabei stets, dass es sich um dasselbe Verfahren handelt (wobei unschädlich ist, wenn sich im Laufe des Verfahrens etwa der Tatvorwurf ändert). Ausgeschlossen ist daher die Erhebung von gesicherten Daten durch Behörden, deren Erhebungsersuchen in keinem Zusammenhang mit der vorausgehenden Sicherungsanordnung stehen.

Das Telekommunikationsgesetz regelt nur Befugnisse zur Datenverarbeitung zum Zweck der Auskunftserteilung. Die Verpflichtung zur Datenübermittlung an die berechtigten Stellen ergibt sich aus den Rechtsgrundlagen der berechtigten Stellen beziehungsweise aus der jeweiligen Anordnung. Konkrete Angaben zur Datensicherung, insbesondere zu den Adressaten, zu erforderlichen Daten sowie zum Zeitraum der Sicherung, enthält die jeweilige Sicherungsanordnung der anordnenden Stelle.

Überdies stellt Absatz 1 klar, dass diese Daten, soweit sie allein aufgrund einer Sicherungsanordnung gesichert wurden, nicht für andere Zwecke verwendet werden dürfen. Mit dem Tatbestandsmerkmal „allein“ ist dabei klargestellt, dass die Verarbeitung solcher Verkehrsdaten, die auch aus anderen Gründen bei den verpflichteten Telekommunikationsanbietern gespeichert sind, durch eine Sicherungsanordnung nicht eingeschränkt wird. Dies gilt insbesondere für Daten, die die Verpflichteten aus betrieblichen Gründen speichern und zusätzlich aufgrund einer auf die gleichen Daten

bezogenen Sicherungsanordnung gesichert haben. Solange die Daten noch aus betrieblichen Gründen gespeichert sind, dürfen sie also beispielsweise auch für zwischenzeitlich eingehende Auskunftsersuchen anderer Behörden verarbeitet werden.

Zu Absatz 2

Absatz 2 verpflichtet die Adressaten nach Absatz 1 Satz 1 dazu, die Einhaltung der Anforderungen an Datenschutz und Datensicherheit zu gewährleisten.

Nach Nummer 1 haben die Verpflichteten sicherzustellen, dass die aufgrund von Sicherungsanordnungen gesicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden.

Nummer 2 regelt, dass die Verkehrsdaten technisch wirksam getrennt von allen anderen beim Verpflichteten vorhandenen Endnutzerdaten durch eine abgesicherte und zuverlässige Datenverarbeitungseinrichtung zu speichern sind. Das Tatbestandsmerkmal „technisch“ geht auf das Urteil des Europäischen Gerichtshofs vom 30. April 2024 (Rechtssache C-470/21, Quadrature du Net II – Hadopi, Randnummer 87, 164) zurück, das in technischer Hinsicht eine wirksame strikte Trennung zwischen den verschiedenen Kategorien auf Vorrat gespeicherter Daten verlangt. Diese Entscheidung ist unmittelbar zu vorsorglich gespeicherten IP-Adressen ergangen. Es liegt aber nahe, diese Anforderungen auch auf Daten zu beziehen, die aufgrund einer Sicherungsanordnung gespeichert worden sind. Denn hierbei handelt es sich nicht lediglich um Daten, die die Identifizierung eines Anschlussinhabers ermöglichen, sondern um weitere Verkehrs- oder Standortdaten, die regelmäßig sensibleren Inhalts sind.

Nach Nummer 3 hat die Datenspeicherung beim Anbieter dabei so zu erfolgen, dass Übermittlungsersuchen von anordnenden Stellen unverzüglich nachgekommen werden kann.

Nummer 4 enthält eine Löschverpflichtung für die durch eine Sicherungsanordnung zu sichernden Daten unverzüglich nachdem die angeordnete Datenübermittlung an die anordnende Stelle erfolgt ist. Dabei sind die Daten in dem Umfang zu löschen, in dem sie abgerufen wurden. Sofern Adressaten einer Sicherungsanordnung nicht oder nicht in vollem Umfang zur Datenübermittlung aufgefordert wurden, haben sie diese Daten unverzüglich spätestens nach Ablauf der in der Sicherungsanordnung genannten Frist nach dem Stand der Technik und insbesondere den Regelungen der Technischen Richtlinie irreversibel zu löschen oder die irreversible Löschung sicherzustellen.

Dabei bedeutet der Begriff „unverzüglich“ nach § 121 Absatz 1 Satz 1 des Bürgerlichen Gesetzbuches, dass eine Handlung ohne schuldhaftes Zögern erfolgen muss, jedoch nicht zwingend sofort. Entscheidend ist, dass der Handelnde bei sorgfältiger Organisation und Aufmerksamkeit nicht schneller hätte reagieren können, wobei unvermeidbare Hindernisse den Zeitraum verlängern können.

Die unverzügliche irreversible Löschung eines Datensatzes nach Ablauf der jeweiligen Speicherdauer kann in einem mehrstufigen Verfahren erfolgen, welches durch die Technische Richtlinie nach § 170 Absatz 6 beschrieben wird. Berücksichtigt wird dabei der Umstand, dass das sichere Löschen einzelner Dateien in den meisten Fällen nach dem Stand der Technik, zum Beispiel nach dem Baustein CON.6 „Löschen und Vernichten“ des Bundesamtes für Sicherheit in der Informationstechnik, nur eingeschränkt möglich ist.

Dennoch bleiben die nun geregelten Anforderungen an den Schutz der zu sichernden Daten bewusst hinter den Vorgaben zum Schutz und zur Sicherheit der Daten aus der – dauerhaft für unanwendbar erklärten – allgemeinen und unterschiedslosen

Vorratsdatenspeicherung zurück. Die strengen Datenschutz- und Datensicherheitsvorschriften der §§ 176 bis 181 sind in direkter Umsetzung des Urteils des Bundesverfassungsgerichts entstanden, das die erste deutsche Regelung zur Vorratsdatenspeicherung für verfassungswidrig erklärt hatte (Urteil vom 2. März 2010 – 1 BvR 256/08, BVerfGE 125, 260–385). Sie müssen für die Sicherungsanordnung – abgesehen von den zuvor genannten Vorschriften – nicht nachgebildet werden, da insoweit kein dauerhaft vorhandener Datenpool mit entsprechenden Gefahren missbräuchlicher Nutzung vorgesehen ist. Die Datenspeicherung bei der Sicherungsanordnung erfolgt nämlich im Gegensatz zur Vorratsdatenspeicherung anlassbezogen, im Einzelfall, für einen begrenzten Zeitraum und nur hinsichtlich eines beschränkten Datenumfangs. Ferner ist nicht öffentlich bekannt, ob, in welchem Umfang und wen betreffend Daten gespeichert werden. Damit sind die aufgrund einer Sicherungsanordnung gespeicherten Verkehrsdaten ein deutlich weniger reizvolles Ziel für potentielle Angriffe von außen. Für die zu betrieblichen Zwecken gespeicherten Verkehrsdaten sind im bisher geltenden Recht, insbesondere im TKG und im TDDDG, Regelungen zu Datenschutz und Datensicherheit vorgesehen, die – neben den Vorgaben des Absatzes 2 – auch für die aufgrund der Sicherungsanordnung gespeicherten Daten gelten werden.

Zu Absatz 3

Die aufgrund einer Sicherungsanordnung nach Absatz 1 Satz 1 Verpflichteten haben über das Vorliegen einer Sicherungsanordnung, einer hierzu ergangenen Herausgabeanordnung und über die auf dieser Grundlage erfolgte Datenübermittlung im Interesse der gesetzmäßigen Aufgabenwahrnehmung durch die ersuchenden Stellen Stillschweigen zu wahren.

Zu Absatz 4

Die in Absatz 2 und 3 getroffenen Regelungen des Gesetzes bedürfen der näheren Ausgestaltung. Die Bundesregierung erhält daher die Ermächtigung zum diesbezüglichen Erlass konkretisierender Regelungen zur Datensicherheit und zum Datenschutz sowie zum Verfahren zur Erteilung der Auskünfte in der Rechtsverordnung nach § 170 Absatz 5 TKÜV, die die Grundlage für den sachgerechten Vollzug der Regelungen beinhaltet. Die technischen Einzelheiten dafür legt die Bundesnetzagentur in der Technischen Richtlinie nach § 170 Absatz 6 fest.

Die Regelungen zur Gestaltung der Schutzmaßnahmen und der Löschung sowie des Verfahrens zur Erteilung der Auskünfte und zur Einhaltung der Stillschweigensregelung nach den Regelungen der TKÜV und der Technischen Richtlinie nach § 170 Absatz 6 führen die bisher hierfür geltenden Regelungen zur Erteilung von Auskünften über Verkehrsdaten fort und garantieren somit etablierte und standardisierte Verfahren für den Umgang mit Sicherungsanordnungen und Auskunftsverlangen.

Diese Verfahren ermöglichen den verpflichteten Anbietern eine effiziente Bearbeitung von Sicherungsanordnungen und von Auskunftsverlangen sowie für die berechtigten Stellen ein standardisiertes, technisches Verfahren für die Übermittlung der Sicherungsanordnung sowie der Auskunftsverlangen. In der TKÜV sind hierzu unter anderem bereits organisatorische Anforderungen zur technischen Entgegennahme sowie zum Herbeirufen außerhalb der Geschäftszeiten geregelt. In der TKÜV sind zudem Regelungen zu Schutzanforderungen für die Auskunftsverlangen enthalten, die um die Verpflichtungen nach Absatz 2 erweitert werden, um ein einheitliches Sicherheitsniveau sicherzustellen.

Die ergriffenen Maßnahmen sind der Bundesnetzagentur mitzuteilen. Die Bundesnetzagentur überprüft im Turnus von etwa zwei Jahren die Umsetzung der Vorgaben.

Zu § 177 (Pflicht zur Speicherung und Befugnis zur Verwendung von Verkehrsdaten zur Identifizierung von Anschlussinhabern)

Die Vorschrift regelt Vorgaben für Anbieter von Internetzugangsdiensten für eine dreimonatige Speicherung von IP-Adressen und zur Identifizierung erforderlicher weiterer Daten, wie Portnummern, um diese einem Anschlussinhaber eindeutig zuordnen zu können, sowie die Verwendungsbefugnis dieser Daten.

Eine solche Speicherpflicht steht in Einklang mit dem Verfassungsrecht. Diese Speicherpflicht hat ein erheblich weniger belastendes Gewicht als eine vollständige Speicherung von Daten sämtlicher Telekommunikationsverbindungen und kann entsprechend unter deutlich geringeren Voraussetzungen gesetzlich angeordnet werden (vergleiche Bundesverfassungsgericht, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, Randnummer 257; Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, Randnummer 171). Es besteht ein – auch verfassungsrechtlich anerkanntes – gesteigertes Interesse an der Möglichkeit, Kommunikationsverbindungen im Internet zum Rechtsgüterschutz oder zur Wahrung der Rechtsordnung den jeweiligen Akteuren zuzuordnen. Angesichts der evidenten Bedeutung des Internets für die verschiedenartigsten Bereiche und Abläufe des alltäglichen Lebens besteht auch die andauernde Gefahr seiner Nutzung für Straftaten vielfältiger Art. In einem Rechtsstaat darf auch das Internet keinen rechtsfreien Raum bilden. Der Gesetzgeber kann daher zur Gewährleistung einer verlässlichen Zuordnung von IP-Adressen zu Anschlussinhabern über einen gewissen Zeitraum die Vorhaltung der entsprechenden Daten seitens der Diensteanbieter vorsehen (vergleiche Bundesverfassungsgericht, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, Randnummer 260).

Die Speicherpflicht steht auch in Einklang mit dem Unionsrecht, namentlich mit Artikel 15 Absatz 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), wie sie im Lichte der Artikel 7, 8 und 11 sowie von Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union auszulegen ist. Die hier angeordnete Speicherung stellt keinen schwerwiegenden Eingriff in diese Rechte dar, da durch die Speichermodalitäten sichergestellt ist, dass ihre Aussagekraft allein auf die Identitätsauskunft des Anschlussinhabers zu einer bekannten IP-Adresse beschränkt ist; es ist ausgeschlossen, besuchte Internetseiten eines Anschlussinhabers nachzuverfolgen oder seine Kontakte oder Standorte herauszufinden (vergleiche zu den maßstäblichen Vorgaben des Europäischen Gerichtshofs, Urteil vom 30. April 2024, Rechtssache C-470/21, Quadrature du Net II – Hadopi, Randnummern 101 und 115).

Zu Absatz 1

Absatz 1 regelt eine Verpflichtung zur Speicherung von IP-Adressen sowie ergänzender erforderlicher Daten, wie Portnummern und Zeitstempel an der Quelle einer Verbindung beim Anbieter eines Internetzugangsdienstes ausschließlich zum Zweck der Identifizierung des Anschlussinhabers und für einen begrenzten Zeitraum von drei Monaten. Die Regelung ist technologieoffen ausgestaltet, um den verschiedenen Verfahren bei der Vergabe von IP-Adressen Rechnung zu tragen.

Verpflichtet sind ausschließlich Anbieter von Internetzugangsdiensten (vergleiche § 3 Nummer 23). Gleiches gilt für Unternehmen beziehungsweise andere Netzbetreiber, denen sich ein Anbieter zur Erbringung seines Internetzugangsdienstes als sogenannter Vorleister bedient, der die Verkehrsdaten für diesen verarbeitet. Dabei hat der Anbieter des Internetzugangsdienstes auch die unverzügliche Sicherung der nicht von ihm selbst bei der Erbringung seines Dienstes erzeugten und verarbeiteten Daten sicherzustellen.

Auf welche Weise der Erbringer die Sicherung sicherstellt, hat er gegenüber der Bundesnetzagentur auf deren Verlangen nachzuweisen.

Nicht verpflichtet zur vorsorglichen Speicherung sind daher etwa nummernunabhängige interpersonelle Telekommunikationsdienste (OTT-1-Dienste, etwa Messenger- und E-Mail-Dienste). Auch Bereitsteller von lokalen drahtlosen Netzwerken (wie etwa der Hotelbetreiber, der seinen Gästen WLAN zur Verfügung stellt, oder eine Initiative, die die vorübergehende Mitnutzung von privaten lokalen Netzwerken ermöglicht) gehören nicht zum Kreis der Verpflichteten. Denn gemäß Artikel 2 Absatz 2 Nummer 2 der Verordnung (EU) 2015/2120, auf die § 3 Nummer 23 Bezug nimmt, ist Internetzugangsdienst „ein öffentlich zugänglicher elektronischer Kommunikationsdienst, der unabhängig von der verwendeten Netztechnologie und den verwendeten Endgeräten Zugang zum Internet und somit Verbindungen zu praktisch allen Abschlusspunkten des Internets bietet“. Lokale drahtlose Netzwerke bieten aber selbst keinen Zugang „zum Internet und somit Verbindungen zu praktisch allen Abschlusspunkten des Internets“, sondern vermitteln – bildlich gesprochen – nur einen Weg dorthin. Sie sind nämlich ihrerseits auf eine Verbindung zu einem Internetzugangsdienst und dessen Telekommunikationsdienstleistung angewiesen. Erst dieser gewährt den eigentlichen „Zugang zum Internet“ (also zu Internet-Knoten oder den Netzen von anderen Internetdienstanbietern). Entsprechend weisen die lokalen drahtlosen Netzwerke auch keine öffentlichen Internetprotokoll-Adresse zu, sondern allenfalls netzwerk-/routerinterne IP-Adressen. Ferner unterfallen auch Freifunkvereine nicht der Verpflichtung nach Absatz 1, da sie weder dem Inhaber des Freifunkrouters noch dem Freifunknutzer eine Rufnummer oder Anschlusskennung, also keine öffentliche IP-Adresse an Anschlussinhaber vergeben. Aus Nutzersicht verhält sich die Erbringung des Dienstes wie eine Mitnutzung in einem Hotel, bei dem keine Registrierung erfolgt und eine IP-Adresse einem Endgerät zugewiesen wird. Der Dienst beruht dabei immer auf einem Internetzugangsdienst eines anderen Internetzugangsanbieters, der selbst nach Absatz 1 verpflichtet ist.

Nach derzeitigem Stand der Technik ist der Anbieter zur Beauskunftung immer dann in der Lage, wenn im Auskunftsersuchen der Strafverfolgungsbehörde IP-Adresse, Portnummer und Zeitstempel zu einer Verbindung mitgeteilt sind. Nummer 1 verpflichtet zur Speicherung der öffentlichen IP-Adresse, Die Portnummer sowie gegebenenfalls weitere Verkehrsdaten nach Nummer 2 sind dabei regelmäßig nur dann zur Identifikation des Anschlussinhabers erforderlich, wenn mehreren Nutzern die gleiche öffentliche IP-Adresse in einem besonderen technischen Verfahren (Network Address Translation, NAT) zugewiesen wird. Häufig steht den Ermittlungsbehörden aber die Portnummer nicht zur Verfügung, sodass sie sich nur mit IP-Adresse und Zeitstempel an den Anbieter wenden. In diesem Fall ist der Anbieter trotz fehlender Portnummer zur Beauskunftung verpflichtet, sofern dies technisch möglich ist. Eine eindeutige Zuordnung zu einem Anschluss kann in diesem Fall etwa dann möglich sein, wenn der Anbieter dem Anschlussinhaber bei der zugrunde liegenden Verbindung eine IP-Adresse exklusiv zugewiesen hat, ohne dass also eine Unterscheidung anhand einer Portnummer nötig ist. Vergleiche dazu auch die Begründung zur Änderung der Strafprozessordnung unter Nummer 3, zu § 100j Absatz 2.

Nach Nummer 3 sind vom Internetzugangsdienst eine eindeutige Kennung des Anschlusses sowie eine zugewiesene Benutzerkennung zu speichern. Dabei bezeichnet die Anschlusskennung den physischen Zugangspunkt des Netzbetreibers beim Anschlussinhaber, wie er ebenfalls vom § 172 Absatz 1 Satz 1 Nummer 2 umfasst ist. Bei Internetzugangsdiensten sind dies typischerweise die Kennungen der Leitungen, die dem Internetanschluss dauerhaft zugewiesen sind. Unter der zugewiesenen Benutzerkennung ist die vom Erbringer des Internetzugangsdienstes dem Anschlussinhaber für die Authentifizierung gegenüber dem Netz des Anbieters des Internetzugangsdienstes bereitgestellte Kennung zu verstehen. Diese Kennung wird regelmäßig im Internetrouter (zum Beispiel DSL-Modem) des Anschlussinhabers eingetragen und dient zur Anmeldung an dem Anmeldeserver des Internetzugangsanbieters. In jedem Fall ist die Speicherung

technisch so auszugestalten, dass eine Identifizierung und Beauskunftung von Anschlussinhabern innerhalb der Speicherdauer gewährleistet ist (vergleiche hierzu die Vorgaben aus dem Beschluss des Bundesverfassungsgerichts vom 20. Dezember 2018 – 2 BvR 2377/16 – und aus dem Beschluss des Bundesgerichtshofs vom 28. April 2021 – StB 47/20).

Das nach Nummer 4 zu speichernde Datum und die sekundengenaue Uhrzeit soll sich dabei nicht nur auf Beginn und Ende der Zuweisung der öffentlichen IP-Adressen beziehen, sondern auch auf Beginn und Ende der Zuweisung einer Portnummer, wenn diese nach Nummer 2 erforderlich ist. Schließlich können innerhalb des Zeitraums der Zuweisung einer IP-Adresse verschiedene Portnummern nacheinander dieser IP-Adresse zugeordnet werden. Würde nur der Zeitraum der Zuweisung für die IP-Adresse gespeichert werden, kämen auch mehrere Anschlussinhaber in Frage, wenn im Gesamtzeitraum jedem Anschlussinhaber dieselbe Portnummer zugewiesen war. Nur durch die zusätzliche Speicherung des Zeitraums für die Zuweisung der Portnummer kann ein Anschlussinhaber eindeutig ermittelt werden.

Der Verpflichtete speichert fortlaufend alle notwendigen Daten, vom Beginn, über die Dauer der Verbindung, bis einschließlich Verbindungsende. Alle Daten, die während dieser Verbindung die Speicherdauer überschreiten, werden fortlaufend gelöscht, auch der Beginn, wenn er aus der drei monatigen Speicherdauer herausfällt. Als neuer „fiktiver“ Beginn tritt der Anfang der drei monatigen Speicherdauer. Somit werden keine Daten länger als drei Monate gespeichert, aber dennoch ist eine Identifizierung von Anschlussinhabern innerhalb der Speicherdauer gewährleistet.

In Satz 2 wird die Speicherfrist auf drei Monate festgelegt. Sie beachtet die Anforderung des Europäischen Gerichtshofs aus seinem Urteil vom 30. April 2024 (Rechtssache C-470/21, Quadrature du Net II – Hadopi, Randnummer 93), wonach die Dauer der Speicherung auf das absolut Notwendige zu begrenzen ist.

Bei Straftaten, die im oder mithilfe des Internets begangen werden, stellt die IP-Adresse des Täters häufig den einzigen, immer aber den ersten, effizientesten und schnellsten Ermittlungsansatz für die Strafverfolgungsbehörden beziehungsweise Ermittlungsbehörden dar. Auch im Bereich der nachrichtendienstlichen Aufklärungsarbeit stellt die Verfügbarkeit von IP-Adressen ein relevantes und oft essentielles Mittel dar. Ohne die Zuordnung der IP-Adresse zu einem Anschlussinhaber laufen die Ermittlungen und die Erkenntnisgewinnung oft ins Leere, sofern keine anderen Spuren vorhanden sind.

Die notwendige Dauer der Speicherung steht insbesondere in Abhängigkeit des Zeitpunkts, an dem tatrelevante IP-Adressen der Sicherheitsbehörde bekannt werden. Erst in dem Moment können die Ermittlungs- und Gefahrenabwehrbehörden anhand der IP-Adresse eine Anfrage nach Bestandsdaten zum Kundenanschluss beim Internetzugangsanbieter vornehmen. Dies ist von Fall zu Fall verschieden und auch abhängig vom Kriminalitätsphänomen, wie schnell die Ermittlungsbehörde etwa durch Strafanzeige aus der Bevölkerung, durch die Meldung von Digitalen-Dienste-Anbietern, einem Ersuchen oder Hinweis aus dem Ausland oder anhand von Daten aus sichergestellten Datenträgern, von einer Straftat oder einer Gefahrenlage und einer möglicherweise relevanten IP-Adresse erfährt. Teilweise müssen auch weiter zurückliegende Tatbeiträge aufgeklärt werden.

Im Falle der Verbreitung von Kinderpornografie hat sich gezeigt, dass bei einer Durchsuchung aufgefundene und sichergestellte elektronische Asservate IP-Adressen möglicher Mittäter enthalten können, welche bereits mehrere Wochen und Monate alt sein können. Auch bei Fällen der gewerbsmäßigen Erpressung mittels Ransomware kann die Auswertung der betroffenen Systeme und vorhandenen Logdaten komplex und daher zeitintensiv sein. Wird dabei eine tatrelevante deutsche IP-Adresse festgestellt, kann es sein, dass die Zuordnung zum Täteranschluss ausgeschlossen ist, weil die extrahierte

digitale Spur älter ist. Im Falle internationaler Zusammenarbeit im Bereich Straftaten zum Nachteil von Kindern und Jugendlichen kommt es vor, dass bei Eingang von ermittlungsrelevanten Informationen beim Bundeskriminalamt bereits mindestens mehrere Monate vergangen waren. Bei Ermittlungen wegen banden- und gewerbsmäßigen Betäubungsmittelkriminalität werden bei Diensteanbietern Log-In-Daten von Mittätern ermittelt, die nur anhand der genutzten IP-Adresse eindeutig identifiziert werden können. Sind diese älter als wenige Tage, können Fallakten nicht an die örtlich zuständige Strafverfolgungsbehörde herangetragen werden.

Bei der Gefährdungssachbearbeitung im Bereich Terrorismus können relevante IP-Adressen zum Zeitpunkt des Hinweiseingangs auf Anschlagspläne bereits mehrere Monate alt sein. Auch bei geheimdienstlicher Agententätigkeit und Staatsterrorismus kann mittels IP-Adressen erhoben werden, von welchem Anschluss der Täter sich in Netzwerke einloggte oder eine E-Mail versandte, um zielgerichtet zu ermitteln. Hierbei ist wie im Phänomenbereich (Cyber-)Spionage von langfristig angelegten Aktivitäten fremder Nachrichtendienste auszugehen und es sind in der Regel längere, oft auch länger zurückliegende Tatzeiträume zu betrachten. Derartige Fälle werden oftmals erst mit mehrmonatiger Verzögerung den Sicherheitsbehörden bekannt.

Im Phänomenbereich Hasspostings gibt es Fälle, bei denen auch mehrere Monate alte IP-Adressen ermittlungsrelevant sein können. Opfer online begangener Betrugsstraftaten bemerken die Tat zu ihrem Nachteil oftmals erst nach Ablauf von mehreren Wochen. Auch Mitteilungen aus dem Ausland zu Cybergrooming durch einen deutschen Internetnutzer werden mitunter erst nach Ablauf von mehreren Wochen bekannt.

Eine IP-Adresse muss folglich einem Anschluss mindestens für diesen Zeitraum zuzuordnen sein. So bietet sie in vielen Phänomenbereichen einen Mehrwert für die Zwecke der Strafverfolgung und der polizeilichen und nachrichtendienstlichen Tätigkeit. Für diesen Zeitraum muss es mit Blick auf Opfer von online begangenen Straftaten und die Gefahren durch politischen Extremismus und Terrorismus sowie die Bedrohungen durch Spionageaktivitäten gewährleistet sein, dass die Sicherheitsbehörden den vom Täter genutzten Anschluss feststellen können, um die Tat aufzuklären.

Die polizeiliche Praxiserfahrung zeigt, dass mit einer Speicherdauer von drei Monaten voraussichtlich ein relevanter Teil der maßgeblichen polizeilichen Sachverhalte abgedeckt werden kann. Bei der Bemessung der notwendigen Speicherdauer können die bisher durch das BKA erzielten Erfolgsquoten, also der Anteil der Fälle, bei denen das BKA im Rahmen seiner Zentralstellenfunktion durch eine Bestandsdatenabfrage die örtliche Zuständigkeit zuordnen konnte, aus dem individuell standardisierten NCMEC-Prozess nicht verallgemeinernd herangezogen werden. Es handelt sich dabei nämlich um einen stark optimierten und insbesondere automatisierten Prozess, der es ermöglicht, die Zeit bis zur Bestandsdatenabfrage anhand einer IP-Adresse stark zu reduzieren. Bei dem NCMEC-Prozess handelt es sich um die in den USA verpflichtende Meldung durch die Plattformanbieter zu Darstellungen sexualisierter Gewalt, die sie bei freiwilligen Suchmaßnahmen auffinden, an das National Center for Missing & Exploited Children (NCMEC), das seinerseits entsprechende Hinweise zum Zwecke der Strafverfolgung an das BKA als deutsche Zentralstelle der deutschen Polizei übermittelt. Beim NCMEC-Prozess werden die strafrechtlich relevanten Daten durch die Diensteanbieter (über NCMEC) standardisiert nebst Beweismittel zur Verfügung gestellt. Der hierbei etablierte technische Prozess ist auf Ermittlungen in anderen Kriminalitätsbereichen nicht übertragbar, bei denen tatrelevante IP-Adressen z.T. phänomenbedingt erst später im Verfahren polizeilich bekannt werden oder durch (zeit-)aufwändige Maßnahmen zunächst ermittelt werden müssen. Die Speicherdauer von drei Monaten ist daher notwendig, aber auch ausreichend, um in vielen Konstellationen eine Verfügbarkeit der maßgeblichen Daten sicherzustellen. Die dreimonatige Speicherdauer bringt damit den dringenden Bedarf der zuständigen Strafverfolgungsbehörden, effektiv Straftaten aufzuklären und

Gefahren abzuwehren, in angemessenen Ausgleich mit den Grundrechten vor allem der unbescholtenen Bürger, die von der Speicherung betroffen sind.

Satz 3 bestimmt klarstellend, dass Inhalte der Kommunikation sowie Daten über den Aufruf von Internetseiten oder Daten über die Nutzung von anderen Telekommunikationsdiensten oder digitalen Diensten, also die Ziel-IP-Adressen einer Kommunikation, aufgrund dieser Vorschrift nicht gespeichert werden dürfen.

Zu Absatz 2

Absatz 2 bestimmt, dass diejenigen Anbieter von Internetzugangsdiensten, die bei der Erbringung ihres Dienstes Unternehmen beziehungsweise andere Netzbetreiber als sogenannte Vorleister in Anspruch nehmen und daher nicht alle Verkehrsdaten selbst verarbeiten, weiteren Verpflichtungen unterliegen. In diesem Fall haben Anbieter von Internetzugangsdiensten auch die unverzügliche Speicherung der nicht von ihnen selbst bei der Erbringung ihres Dienstes erzeugten und verarbeiteten Daten sicherzustellen. Auf welche Weise die Anbieter die Speicherung sicherstellen, haben sie gegenüber der Bundesnetzagentur auf deren Verlangen nachzuweisen.

Zu Absatz 3

Absatz 3 verpflichtet die Adressaten nach Absatz 1 Satz 1 dazu, die Einhaltung der Anforderungen an Datenschutz und Datensicherheit zu gewährleisten.

Nach Nummer 1 haben die nach Absatz 1 Verpflichteten sicherzustellen, dass die aufgrund des Absatzes 1 zu speichernden Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden.

Im Hinblick auf die Modalitäten der Speicherung hat der Europäische Gerichtshof in seinem Urteil vom 30. April 2024 (Rechtssache C-470/21, Quadrature du Net II – Hadopi) verschiedene Anforderungen formuliert. Danach haben die auf Vorrat gespeicherten Daten nach Absatz 1 in jedem Fall technisch wirksam getrennt von allen anderen beim Verpflichteten vorhandenen Endnutzerdaten durch eine abgesicherte und zuverlässige Datenverarbeitungseinrichtung zu erfolgen, was durch Nummer 2 umgesetzt wird. Die Umsetzung dieser Vorgabe hat danach durch regelmäßige Kontrolle durch eine unabhängige Stelle zu erfolgen und wird in Absatz 5 durch die Bundesnetzagentur sichergestellt.

Nummer 3 gibt vor, dass die Speicherung der aufgrund des Absatzes 1 zu sichernden Daten – wie auch nach § 176 Absatz 2 Nummer 3 – so zu erfolgen hat, dass die Auskunft an die berechtigten Stellen unverzüglich erfolgen kann. Welche Stellen berechtigt sind, ergibt sich mittelbar aus Absatz 4, der regelt, für welche Zwecke die gespeicherten Daten verwendet werden dürfen.

Nummer 4 enthält eine Löschverpflichtung für die nach Absatz 1 zu speichernden Daten nach Ablauf von drei Monaten. Für den Fall, dass eine Strafverfolgungsbehörde aus dem europäischen Ausland auf Grundlage der Verordnung (EU) 2023/1543 eine Europäische Sicherungsanordnung zur Vorbereitung einer späteren Herausgabeanordnung zur Erlangung von Teilnehmerdaten erlässt, hat der Verpflichtete sicherzustellen, dass er der etwaig folgenden Herausgabeanordnung Folge leisten, also die Teilnehmerdatenauskunft erteilen kann, zum Beispiel, indem er die Daten separiert speichert oder die Teilnehmerdatenauskunft vorbereitet.

Die Anforderungen an den Schutz der zu speichernden Daten bleiben – wie nach § 176 Absatz 2 aus den dort beschriebenen Gründen – bewusst hinter den Vorgaben zum Schutz und zur Sicherheit der §§ 176 bis 181 zurück.

Zu Absatz 4

Absatz 4 enthält die sogenannte Verwendungszweckregelung, die abschließend regelt, wofür die nach Absatz 1 vorsorglich gespeicherten Daten verwendet werden dürfen. Danach dürfen die Daten zum einen für eine Auskunft nach § 174 Absatz 1 Satz 3 verwendet werden, wobei in § 174 Absatz 5 geregelt ist, an welche Stellen unter welchen Voraussetzungen Auskunft erteilt werden darf. Dazu gehören insbesondere die Strafverfolgungs- und Gefahrenabwehrbehörden, aber auch die dort benannten Nachrichtendienste. Die Daten nach Absatz 1 dürfen außerdem verwendet werden für die Erfüllung einer Europäischen Herausgabeanordnung zur Erlangung von Teilnehmerdaten gemäß der Verordnung (EU) 2023/1543, wenn also eine Strafverfolgungsbehörde eines anderen Mitgliedsstaates einen deutschen Internetzugangsdienst um Auskunft ersucht oder eine dies vorbereitende Europäische Sicherungsanordnung erlässt. Für andere Zwecke dürfen die Daten nicht verwendet werden. Insbesondere ist es nicht zulässig, die Daten aufgrund einer Europäischen Herausgabeanordnung zur Erlangung von Verkehrsdaten herauszugeben.

Satz 1 bestimmt weiter, dass ein leistungsfähiges technisches Verfahren einzusetzen ist, das die getrennte Speicherung nach Absatz 2 Nummer 2 nicht beeinträchtigt. Für Auskünfte nach § 174 Absatz 1 Satz 3 wird mit Satz 3 auf das Verfahren nach § 174 Absatz 7 zur Beauskunftung von Anschlussinhabern verwiesen. Es verwendet eine gesicherte elektronische Schnittstelle für 100 000 und mehr Vertragspartnern sowie das E-Mail-basierte Übermittlungsverfahren, das auch von allen anderen Verpflichteten zu verwenden ist. Die gesicherte elektronische Schnittstelle nutzt ein seit Jahren etabliertes Verfahren und von allen Seiten angesehenes Mittel zur Beauskunftung. Die Schnittstelle basiert auf einem ETSI-Standard (TS 102 657), der eine einheitliche Beauskunftung auf beiden Seiten der am Verfahren Beteiligten garantiert. Die standardisierten Prozesse für die Auskunftsersuchen sowie für die Antworten garantieren eine schnelle Bearbeitung und eine gleichbleibend hohe Qualität auf beiden Seiten. Sie reduziert die Fehlerhäufigkeit auf ein Minimum, ist durch den einheitlichen Standard zukunftssicher und auf dem freien Markt verfügbar. Durch den einheitlichen Standard und das verwendete maschinenlesbare Format ist bei den verpflichteten Unternehmen eine Teilautomatisierung möglich, die die Zusammenstellung der angefragten Daten erleichtert und eine Beauskunftung beschleunigen kann. Auf Seiten der berechtigten Stellen können umfangreiche Anfragen mittels aufbereiteter Dateien schnell und unkompliziert in die Ersuchen importiert werden und die beauskunfteten Ersuchen mit individuellen Filtern problemlos aufbereitet und ausgewertet werden.

Zu Absatz 5

Die in Absatz 3 getroffenen Regelungen des Gesetzes bedürfen – wie durch § 176 Absatz 4 zu § 176 Absatz 2 – der näheren Ausgestaltung. Die Bundesregierung erhält daher die Ermächtigung zum diesbezüglichen Erlass konkretisierender Regelungen der Pflichten nach Absatz 3, einschließlich Vorgaben zu den eingesetzten Systemen, Verfahren und technischen Einrichtungen zur Speicherung der Daten nach Absatz 1 in der TKÜV, die die Grundlage für den sachgerechten Vollzug der Regelungen beinhaltet.

Die ergriffenen Schutzmaßnahmen sind der Bundesnetzagentur vorzulegen. Die Bundesnetzagentur überprüft im Turnus von etwa zwei Jahren die Umsetzung der Vorgaben.

Zu Nummer 3 (§ 228 – Bußgeldvorschriften)

Bei den Änderungen handelt es sich um redaktionelle Folgeänderungen, die aufgrund der Änderung der §§ 175 bis 177 sowie Streichung der bisherigen §§ 177 bis 181 erforderlich sind.

Zur Sicherstellung der praktischen Wirksamkeit des § 174 Absatz 6 Satz 1 ist diese Regelung, die eine Übermittlungspflicht der betroffenen Telekommunikationsunternehmen vorsieht, mit einem Bußgeld zu bewehren. Zudem wird so einer inkonsistenten Gesetzessystematik entgegengewirkt, die ansonsten bestünde, wenn die Bewahrung des Stillschweigens bußgeldbewehrt ist, die eigentliche Übermittlungspflicht jedoch nicht.

Zu Nummer 4 (§ 230 – Übergangsvorschriften)

Die Vorschrift regelt, ab wann die Speicherpflicht von Verkehrsdaten zur Identifizierung von Anschlussinhabern nach § 177 gilt.

Zu Artikel 7 (Änderung der Telekommunikations-Überwachungsverordnung)

Es handelt sich um Folgeänderungen in einzelnen Regelungen der §§ 2, 32 und 35 der Verordnung, die aufgrund der Änderung der §§ 175 bis 177 TKG sowie Streichung der bisherigen §§ 177 bis 181 TKG erforderlich sind. Die Änderungen sind redaktioneller Natur.

Zu Artikel 8 (Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes)

Zu § 13a **(Erfüllung von Pflichten gemäß den Artikeln 10 und 11 der Verordnung (EU) 2023/1543)**

§ 13a wurde im Zuge der Durchführung der Verordnung (EU) 2023/1543 in das TDDDG eingefügt (BGBl. 2026 I Nr. 64). Durch die Regelung wird sichergestellt, dass von Europäischen Sicherungs- und Herausgabeanordnungen betroffene Anbieter von elektronischen Telekommunikationsdiensten angeforderte Daten verarbeiten dürfen, um diesen Anordnungen nachkommen zu können.

Mit dem neuen § 176 Absatz 2 TKG werden Anforderungen an Datenschutz und Datensicherheit im Zusammenhang mit der dort geregelten nationalen Sicherungsanordnung festgelegt. Diese Anforderungen sollen wegen der Parallelität der Sachlagen entsprechend für Sicherungsanordnungen auf Grundlage der Verordnung (EU) 2023/1543 gelten (soweit nicht in der Verordnung bereits geregelt). Dazu wird in § 13a ein neuer Absatz 2 angefügt. Den betroffenen Anbietern entsteht dadurch kein Mehraufwand, weil sie aufgrund von § 176 Absatz 2 TKG bereits über die technischen und organisatorischen Vorkehrungen verfügen.

Zu Artikel 9 (Änderung des Bundespolizeigesetzes)

Zu Nummer 1 (Inhaltsübersicht)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 2 (§ 25 – Erhebung von Verkehrs- und Nutzungsdaten)

Zu Buchstabe a

In Absatz 1 Satz 1 wird zur Konkretisierung des Begriffs der Verkehrsdaten auf die Legaldefinition in § 3 Nummer 70 des Telekommunikationsgesetzes verwiesen.

Zu Buchstabe b

Neu eingefügt wurde der Einschub „bei der Sicherung von Daten einer Funkzelle“. Damit wird klargestellt, dass der zweite Halbsatz, wonach eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation genügt, sofern andernfalls die

Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre, in Fällen der Sicherung von Daten einer Funkzelle gilt.

Zu Buchstabe c

Es wird auf die Begründung zu Nummer 2 Buchstabe b verwiesen.

Zu Buchstabe d

Absatz 6 wird neu gefasst durch Einfügung des Satzes 2, in dem klargestellt wird, dass die Frage, ob und in welchem Umfang für die Mitwirkungsverpflichtung nach Satz 1 Vorkehrungen zu treffen sind, sich nach dem TKG und der TKÜV bestimmt. Diese Regelung entspricht der Systematik vergleichbarer Mitwirkungsverpflichtungen, im Falle der Telekommunikationsüberwachung etwa in § 40 Absatz 8 Satz 2 des Bundespolizeigesetzes in der Fassung des Entwurfs eines Gesetzes zur Modernisierung des Bundespolizeigesetzes (Bundestagsdrucksache 21/3051) für die Bundespolizei und in § 51 Absatz 6 Satz 2 BKAG für das Bundeskriminalamt.

Zu Nummer 3 (§ 25a – Sicherung von Verkehrsdaten)

§ 25a wird neu eingefügt. Er schafft für die Bundespolizei das Instrument der Sicherungsanordnung in Bezug auf Verkehrsdaten.

Anwendungsfälle im Aufgabenbereich der Bundespolizei sind im Kontext von (teils lebensgefährlichen Behältnis-)Schleusungen, der Einreise von Extremisten oder Terroristen und im Kontext von terroristischen Anschlägen auf Flughäfen, Häfen oder Bahnanlagen verortet.

Hinweise auf bevorstehende Schleusungen, Einreisen von Extremisten/Terroristen und Anschläge auf Flughäfen, Bahnanlagen und Häfen gehen regelmäßig über Nachrichtendienste ein. Häufig können im Rahmen dieser Hinweise einzelne deutsche Telefonnummern genannt werden. Die Hinweise lassen zu diesem Zeitpunkt für die handelnden Polizeibeamten jedoch noch keine hinreichend konkretisierte Zuordnung einzelner Störer zu. Erforderlich ist eine weitere Informationsverdichtung durch die Bundespolizei, in deren Zuge sich Verdachtsmomente erhärten, Störer identifiziert und Verbindungen zwischen Personen erhellt werden. Doch diese weiteren Ermittlungen sind insbesondere im Kontext von organisierter Kriminalität und häufig schwer durchschaubaren Personennetzwerken zeitintensiv, vor allem wenn sich die Hinweise auf einzelne Telefonnummern beschränken. In diesen Fällen ist es für die erfolgreiche Gefahrenabwehr zentral, dass noch vor Vorliegen der Voraussetzung zur Erhebung der Verkehrsdaten die Verkehrsdaten derjenigen Personen gesichert werden, bezüglich derer tatsächliche Anhaltspunkte vorliegen, dass eine Erhebung zu einem späteren Zeitpunkt zulässig sein wird.

Die Bundespolizei hat im Rahmen ihrer Zuständigkeit etwa derzeit über 40 000 Personen mit Extremismus- oder Terrorismusbezug zur Einreiseverweigerung im Schengener Informationssystem ausgeschrieben. Regelmäßig liegen Anhaltspunkte dafür vor, dass diese Einreiseverweigerungen durch unerlaubte Einreisen umgangen werden sollen. In diesem Zusammenhang wird – wie häufig zu Beginn derartiger Gefahrensachverhalte – lediglich eine Handynummer behördlich bekannt, welche im Zusammenhang mit einer beabsichtigten Einreise einer extremistisch motivierten Gruppe mit Bezügen zur Organisierten Kriminalität stehen könnte. Hier ist es von elementarer Bedeutung, dass die Verkehrsdaten zu dieser Handynummer so schnell wie nur möglich durch die Sicherungsanordnung gesichert werden können, um sie zu einem späteren Zeitpunkt rückwirkend erheben können.

Zu Absatz 1

Absatz 1 legt die materiellen Voraussetzungen für die Sicherungsanordnung fest. Eine Sicherungsanordnung darf danach ergehen in Bezug auf eine Person, die in einem persönlichen oder räumlichen Bezug zu der Gefahr oder zu verhütenden Straftat nach § 25 Absatz 1 des Bundespolizeigesetzes in der Fassung des Entwurfs eines Gesetzes zur Modernisierung des Bundespolizeigesetzes (Bundestagsdrucksache 21/3051) steht und bei der tatsächliche Anhaltspunkte dafür vorliegen, dass es sich um eine Person im Sinne des § 25 Absatzes 1 handelt und eine Erhebung nach § 25 Absatz 1 gerechtfertigt sein könnte, oder bei der tatsächliche Anhaltspunkte dafür vorliegen, dass es sich um eine Person handelt, die mit einer Person nach § 25 Absatz 1 Nummer 2 oder 3 in nicht nur flüchtigem oder zufälligem Kontakt und in einer Weise in Verbindung steht, welche die Annahme rechtfertigt, dass nach Gewinnung weiterer Erkenntnisse eine Erhebung nach § 25 Absatz 1 gerechtfertigt sein könnte.

Das Instrument der Sicherungsanordnung adressiert den Bedarf der Bundespolizei, flüchtige Daten zu sichern, wenn die vorliegenden Erkenntnisse und Informationen noch keine hinreichend konkretisierte Zuordnung einzelner Gefährder oder Störer zulassen. Um in derartigen Fällen Verkehrsdaten erheben zu dürfen, ist zunächst eine weitere Verdichtung von Informationen erforderlich, in deren Zuge sich Verdachtsmomente erhärten, Gefährder oder Störer identifiziert und Verbindungen zwischen Personen erhellt werden.

Zu Beginn der Gefahrermittlung ist es ein häufiges Szenario, dass die Informationslage noch nicht ausreicht, um die Gefahr einem konkreten Gefährder oder Störer zuordnen zu können. Zudem ist zumeist nicht eindeutig klar, welcher Natur die Beziehungen zu Kommunikationspartnern eines Störers sind. Erst wenn sich dies im Verlauf der Sachverhaltsaufklärung konkretisiert, ist eine Datenerhebung nach § 25 Absatz 1 zu den dort genannten Personen zulässig. Bis zu diesem Zeitpunkt soll sichergestellt sein, dass relevante Verkehrsdaten nicht gelöscht werden.

Das Gleiche gilt für ermittelte Telekommunikationsmittel von Personen im Umfeld des Störers oder mögliche Aufenthalts- und Handlungsorte des Störers und seiner Kontaktpersonen (Sicherung hoch flüchtiger Funkzellendaten), bis festgestellt ist, ob zu ihnen eine Verkehrsdatenerhebung nach § 52 Absatz 1 angeordnet werden kann. Dann kann die zielgerichtete und vollständige Erhebung der Verkehrsdaten durch das Gericht erfolgen.

Das Instrument der Sicherungsanordnung trägt ferner dem Umstand Rechnung, dass in bestimmten Konstellationen bei Vorliegen der Voraussetzungen zur Erhebung von Verkehrsdaten zeitgleich eine Sicherung der Verkehrsdaten angeordnet werden muss, um einen Datenverlust zu verhindern. Auf die Ausführungen zu § 100g Absatz 7 StPO wird verwiesen.

Die Verkehrsdaten müssen für die in § 25 Absatz 1 jeweils genannten Zwecke von Bedeutung sein können. Anders als bei der Erhebung ist also nicht erforderlich, dass die Abwehr der Gefahr oder Verhütung der genannten Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Vielmehr genügt es, wenn auf Grundlage einer Ex-ante-Prognose zu erwarten ist, dass die gesicherten Verkehrsdaten für Gefahrenabwehrmaßnahmen nach § 25 Absatz 1 benötigt werden.

Zu Absatz 2

Absatz 2 regelt den Kreis der zur Anordnung der Sicherung Berechtigten. Inhalt, Form und Befristung der Anordnung gleichen weitgehend den Anforderungen für die Anordnung zur Erhebung von Verkehrs- und Nutzungsdaten nach § 25 Absatz 5. Abweichend von § 25 Absatz 5 ergeht die Anordnung nicht durch Gericht, sondern durch die behördlichen Anordnungsberechtigten. Der Inhalt der Anordnung ist insofern abweichend von § 25 Absatz 5 geregelt, als im Falle einer Sicherungsanordnung ferner die Art der durch die

Maßnahme zu erhebenden Daten und ihre voraussichtliche Bedeutung für den Zweck der Erhebung anzugeben sind. Ferner wird geregelt, dass über eine Verlängerung der Sicherungsanordnung das Gericht auf Antrag der nach Satz 1 Anordnungsberechtigten entscheidet.

Zu Absatz 3

Absatz 3 regelt, dass der auf Grund einer Sicherungsanordnung nach Absatz 1 Verpflichtete die von der Anordnung erfassten Daten unverzüglich und vollständig zu sichern hat. Im Übrigen wird bezüglich der Frage, ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, über die entsprechende Geltung von § 25 Absatz 6 Satz 2 auf die Regelungen nach dem TKG und der TKÜV verwiesen. Ferner wird über den Verweis auf § 25 Absatz 7 die Entschädigungspflicht gegenüber den zur Erteilung von Auskünften zu Verkehrs- und Nutzungsdaten Verpflichteten auf die zur Sicherung von Verkehrsdaten Verpflichteten erstreckt.

Zu Artikel 10 (Änderung des Vereinsgesetzes)

Zu Nummer 1

Bislang verweist § 4 Absatz 4 Satz 1 auf die §§ 94 bis 97, 98 Absatz 4 sowie die §§ 99 bis 101 StPO. Eingeschlossen in die Verweisung sind damit auch die zwischenzeitlich neu eingefügten §§ 100a ff. StPO. Die dort enthaltenen Regelungen über die Telekommunikationsüberwachung sind für die Beschlagnahme von Gegenständen im Ermittlungsverfahren nach dem Vereinsgesetz nicht anwendbar und daher von der Verweisung auszunehmen.

Zu Nummer 2

Der geltende § 4 Absatz 4 Satz 4 verweist auch auf § 105 Absatz 4 StPO. Der in Bezug genommene Absatz ist zwischenzeitlich aufgehoben worden, die Verweisung ist entsprechend anzupassen.

Neu aufgenommen in die Verweisung sind die §§ 111c, 111n bis 111p StPO. Sie betreffen Vorschriften zur Art und Weise der Beschlagnahme, zur Herausgabe, zu hierauf bezogenen Verfahrensvorschriften und zur Notveräußerung. Diese Vorschriften gelten künftig entsprechend auch für die Beschlagnahme von Gegenständen nach dem Vereinsgesetz.

Zu Artikel 11 (Änderung des Geldwäschegesetzes)

Nach dem geltenden § 29 Absatz 2a Satz 2 Nummer 2 darf die Zentralstelle für Finanztransaktionsuntersuchungen Daten nach § 100k Absatz 1 Satz 2 StPO nicht in automatisierten Verfahren zur Datenanalyse verarbeiten. Der Ausschluss bezieht sich damit nur auf vorhandene (retrograde) Standortdaten, die bei digitalen Diensten erhoben worden sind, nicht aber auf andere Nutzungsdaten.

Nach dem neuen Regelungskonzept werden die Erhebung von Verkehrsdaten bei Telekommunikationsdiensten nach § 100g StPO und von Nutzungsdaten nach § 100k StPO weitgehend gleichbehandelt. Eine Unterscheidung ist auch für das Geldwäschegesetz nicht sachgerecht und wird daher aufgehoben. Künftig sind damit alle Daten aus einer Erhebung nach § 100k StPO von der Verarbeitung in automatisierten Verfahren zur Datenanalyse ausgeschlossen.

Zu Artikel 12 (Einschränkung eines Grundrechts)

Die Vorschrift erfüllt das Zitiergebot, da das Grundrecht aus Artikel 10 Grundgesetz durch die geänderten Regelungen der Strafprozessordnung in Artikel 1 Nummer 2 und 3, des Telekommunikationsgesetzes in Artikel 6 Nummer 2 und des Bundespolizeigesetzes in Artikel 9 Nummer 3 eingeschränkt wird.

Zu Artikel 13 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten.