Referentenentwurf

des Bundesministeriums der Justiz und für Verbraucherschutz

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 Polizeibehörden 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 Polizeibehörden zu verbessern und der Strafverfolgungspraxis die Funkzellenabfrage im Umfang wie vor der Entscheidung des Bundesgerichtshofs zu ermöglichen.

B. Lösung

Es wird erstens eine Pflicht zur Speicherung von IP-Adressen eingeführt, um den Strafverfolgungsbehörden und Polizeibehörden 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 für Verkehrsdaten das Instrument der Sicherungsanordnung geschaffen. Damit können die Strafverfolgungsbehörden die Sicherung von Verkehrsdaten veranlassen, sofern und solange die rechtlichen oder tatsächlichen Voraussetzungen einer Datenerhebung noch nicht vorliegen. Für den Bereich der Gefahrenabwehr sieht der Entwurf eine entsprechende Befugnis für das Bundeskriminalamt vor. 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

[*Die Haushaltsausgaben für Bund, Länder und Gemeinden werden nach der Ressortabstimmung und der Länder- und Verbändeanhörung ergänzt.*]

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht oder entfällt kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

[*Der Erfüllungsaufwand für die Wirtschaft wird nach der Verbändeanhörung ergänzt.*]

Davon Bürokratiekosten aus Informationspflichten

Keine.

E.3 Erfüllungsaufwand der Verwaltung

Für die Bundesnetzagentur entsteht zusätzlicher Personalaufwand in Höhe von 25 Vollzeitäquivalenten (zwei im höheren Dienst, 15 im gehobenen Dienst, acht im mittleren Dienst).

Im Übrigen entsteht dem Bund, den Ländern oder den Gemeinden voraussichtlich kein zusätzlicher Erfüllungsaufwand.

F. Weitere Kosten

Für den Bund und die Länder ist der Entwurf im justiziellen Kernbereich voraussichtlich kostenneutral.

Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz

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

Vom ...

Der Bundestag hat mit Zustimmung des Bundesrates 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 2 des Gesetzes vom 17. Juli 2025 (BGBl. 2025 I Nr. 163) 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 des Beschuldigten dürfen bei demjenigen erhoben werden, der öffentlich zugängliche Telekommunikationsdienste anbietet oder daran mitwirkt, wenn

1. 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,

---

[1] Zu notifizieren 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).

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

3. 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. ein Verdacht nach Absatz 1 Satz 1 Nummer 1 besteht hinsichtlich einer mittels Telekommunikation begangener Straftat und

2. abweichend von Absatz 1 Satz 1 Nummer 2 wäre die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert.

(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 besonderen Voraussetzungen nach 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 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, und

2. 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 erbringt 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 mit der Maßgabe entsprechend, dass eine Erhebung zulässig ist, wenn der Verdacht hinsichtlich einer mittels 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 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 in der Entscheidungsformel nach § 100e Absatz 3 Satz 2 an die Stelle der Rufnummer (§ 100e Absatz 3 Satz 2 Nummer 5) soweit möglich eine eindeutige Kennung des Nutzerkontos des Betroffenen, ansonsten eine möglichst genaue Bezeichnung des digitalen Dienstes tritt, auf den sich das Auskunftsverlangen bezieht,

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 und 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 in der Entscheidungsformel nach § 100e Absatz 3 Satz 2 Nummer 3 Dauer und Endzeitpunkt der Maßnahme nicht anzugeben sind. Satz 1 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 5 oder 7, § 100j Absatz 3 oder § 100k Absatz 1 bis 4 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 4, § 100j Absatz 2 und 3 und nach § 100k Absatz 1 bis 3 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:

aa) In Nummer 1 wird die Angabe „§ 100g Absatz 1, 2 und 3“ durch die Angabe „§ 100g Absatz 1, 2, 3, 4 und 7“ ersetzt.

bb) Nummer 2 wird wie folgt geändert:

aaa) Nach Buchstabe c werden die folgenden Buchstaben d und e eingefügt:

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

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

bbb) 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:

„(5) 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 12. Juli 2024 (BGBl. 2024 I Nr. 234) geändert worden ist, wird wie folgt geändert:

§ 12 wird durch den folgenden § 12 ersetzt:

„§ 12

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 … [einsetzen: Ausfertigungsdatum und Fundstelle, Bundestagsdrucksache 21/3192], 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 Gerichte und Staatsanwaltschaften für den Erlass von Europäischen Sicherungsanordnungen zum Zweck der Strafverfolgung nach Artikel 4 Absatz 3 Buchstabe a der Verordnung (EU) 2023/1543 in der Fassung von 12. Juli 2023 und für die Übermittlung der dazugehörigen Bescheinigung richtet sich nach dem Achten Abschnitt des Ersten Buchs der Strafprozessordnung.

(2) Zuständig für den Erlass Europäischer Sicherungsanordnungen zum Zwecke der Strafvollstreckung 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 sind die Staatsanwaltschaften."

Artikel 4

Änderung des Justizvergütungs- und -entschädigungsgesetzes

Das Justizvergütungs- und -entschädigungsgesetz vom 5. Mai 2004 (BGBl. I S. 718, 776), das zuletzt durch Artikel 10 des Gesetzes vom 7. April 2025 (BGBl. 2025 I Nr. 109) 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:

   „(2) 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	45,00 €
	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 4 des Gesetzes vom 17. Juli 2025 (BGBl. 2025 I Nr. 163) 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 25 des Gesetzes vom 2. Dezember 2025 (BGBl. 2025 I Nr. 301) 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 Verarbeitungsbefugnis von Verkehrsdaten aufgrund von Sicherungsanordnungen

   § 176 Speicherpflicht und Verwendungsbefugnis von Verkehrsdaten zur Identifizierung von Anschlussinhabern

   §§ 177 bis 181 (weggefallen)“.

2. Die §§ 175 bis 181 werden durch die folgenden §§ 175 und 176 ersetzt:

„§ 175

Verarbeitungsbefugnis von Verkehrsdaten aufgrund von Sicherungsanordnungen

(1) Anbieter öffentlich zugänglicher Telekommunikationsdienste dürfen Verkehrsdaten verarbeiten, soweit dies zur Erfüllung einer Sicherungsanordnung nach

1. § 100g Absatz 7 der Strafprozessordnung oder

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

sowie eines jeweils darauf bezogenen Auskunftsverlangens erforderlich ist. Verkehrsdaten, die allein aufgrund einer Sicherungsanordnung gemäß Satz 1 gesichert wurden, dürfen nur im Rahmen des jeweiligen Zwecks verwendet werden.

(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 Strafverfolgungsbehörde, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung verlangt, unverzüglich erfolgen kann, und

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

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

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

Sie haben über das Vorliegen einer Sicherungsanordnung, einer hierzu ergangenen Herausgabeanordnung und über die auf dieser Grundlage erfolgte Datenübermittlung gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren.

(3) In der Rechtsverordnung nach § 170 Absatz 5 können Regelungen zur näheren Ausgestaltung der Pflichten nach Absatz 2 sowie zur Übermittlung der aufgrund von Sicherheitsanordnungen 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 Unterlagen mitzuteilen, in denen dargestellt wird, wie die Vorgaben nach Absatz 2 sowie der Rechtsverordnung und der Technischen Richtlinie nach Satz 1 und 2 in ihren Anlagen umgesetzt werden. Änderungen sind der Bundesnetzagentur unverzüglich mitzuteilen. Die Bundesnetzagentur überprüft regelmäßig die Umsetzung der Vorgaben.

§ 176

Speicherpflicht und Verwendungsbefugnis von Verkehrsdaten zur Identifizierung von Anschlussinhabern

(1) Anbieter von Internetzugangsdiensten sind verpflichtet, mit der Zuweisung einer öffentlichen Internetprotokoll-Adresse an einen Anschlussinhaber folgende Daten für drei Monate zu speichern:

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

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

3. das Datum und die sekundengenaue Uhrzeit von Beginn und Ende der Zuweisung der öffentlichen Internetprotokoll-Adressen an einen Anschlussinhaber unter Angabe der jeweils zugrunde liegenden Zeitzone sowie

4. 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.

Inhalte der Kommunikation, wie Daten über den Aufruf oder die Nutzung von anderen Telekommunikationsdiensten oder digitalen Diensten, dürfen nicht aufgrund dieser Vorschrift gespeichert werden.

(2) 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 an die berechtigten Stellen unverzüglich erfolgen kann, und

4. nach drei Monaten ab dem Zeitpunkt des Endes der Zuweisung der öffentlichen Internetprotokoll-Adresse unverzüglich nach dem Stand der Technik irreversibel gelöscht werden.

(3) Die aufgrund des Absatzes 1 gespeicherten Daten dürfen für eine Auskunft nach § 174 Absatz 1 Satz 3 oder für die Erfüllung einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnung zur Erlangung von Teilnehmerdaten gemäß der Verordnung (EU) 2023/1543 verwendet werden, wobei ein leistungsfähiges technisches Verfahren einzusetzen ist, das die getrennte Speicherung nach Absatz 2 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.

(4) In der Rechtsverordnung nach § 170 Absatz 5 können Regelungen zur näheren Ausgestaltung der Pflichten nach Absatz 2, 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 Unterlagen mitzuteilen, in denen dargestellt wird, wie die Vorgaben nach Absatz 2 sowie der Rechtsverordnung und der Technischen Richtlinie nach Satz 1 und 2 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:

aa) In Nummer 38 wird die Angabe „oder § 181 Satz 2“ gestrichen.

bb) 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, § 175 Absatz 3 Satz 3 oder 4 oder § 176 Absatz 4 Satz 3 oder 4 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,“.

cc) Nummer 56 wird durch die folgenden Nummern 56 und 57 ersetzt:

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

57. entgegen § 174 Absatz 6 Satz 2 oder § 175 Absatz 2 Satz 2 Stillschweigen nicht wahrt,“.

dd) Die bisherigen Nummern 57 bis 60 werden durch die folgenden Nummern 58 bis 60 ersetzt:

„58. entgegen § 175 Absatz 2 Satz 1 Nummer 1, 2 oder 3 oder § 176 Absatz 2 Nummer 1, 2 oder 3 nicht sicherstellt, dass Daten geschützt und in der dort genannten Weise gespeichert werden,

59. entgegen § 175 Absatz 2 Satz 1 Nummer 4 oder § 176 Absatz 2 Nummer 4 nicht sicherstellt, dass Daten gelöscht werden,

60. entgegen § 176 Absatz 1 Satz 1 Daten nicht oder nicht für die vorgeschriebene Dauer speichert,“.

b) Absatz 7 wird wie folgt geändert:

aa) In Nummer 2 wird die Angabe „57 bis 59“ durch die Angabe „58 bis 60“ ersetzt.

bb) In Nummer 3 wird die Angabe „50, 53 und 60“ durch die Angabe „50, 53“ ersetzt.

cc) In Nummer 5 wird die Angabe „56“ durch die Angabe „57“ ersetzt.

4. Nach § 230 Absatz 15 wird der folgende Absatz 16 eingefügt:

„(16) Die Vorgaben des § 176 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 3 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) 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:

„b) 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 in Verbindung mit § 22 Absatz 1 Satz 1 Nummer 6 und Absatz 2 des MAD-Gesetzes, § 8a Absatz 1 Satz 1 Nummer 4 des Bundesverfassungsschutzgesetzes, auch in Verbindung mit § 3 des BND-Gesetzes, § 52 des Bundeskriminalamtgesetzes, § 77 des Zollfahndungsdienstgesetzes oder nach Landesrecht;“.

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

„b) 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 auf Grund der jeweiligen Anordnung berechtigt ist,

Auskunftsverlangen über Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes zu stellen;“.

2. § 30 Satz 2 wird gestrichen.

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

4. § 35 wird wie folgt geändert:

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

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

      „4. 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 … [einsetzen: Ausfertigungsdatum und Fundstelle, Bundestagsdrucksache 21/3192] geändert worden ist, wird wie folgt geändert:

1. § 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 eingerichteten Adressaten dürfen personenbezogene Daten verarbeiten, soweit dies zur Erfüllung einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnungen 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) Verpflichtete haben allein nach Absatz 1 gesicherte Daten unverzüglich nach Übermittlung an die anordnende Stelle, spätestens sobald die Datensicherung gemäß der Verordnung (EU) 2023/1543 in der Fassung vom 12. Juli 2023 nicht mehr erforderlich ist, nach dem Stand der Technik irreversibel zu löschen.“

2. § 24a wird durch den folgenden § 24a ersetzt:

„§ 24a

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

(1) Anbieter von digitalen Diensten und die von ihnen gemäß § 3 Absatz 1 bis 3 des Elektronische-Beweismittel-Umsetzungs- und Durchführungsgesetzes eingerichteten Adressaten dürfen personenbezogene Daten verarbeiten, soweit dies zur Erfüllung einer Europäischen Herausgabeanordnung oder einer Europäischen Sicherungsanordnungen gemäß der Verordnung (EU) 2023/1543 in der Fassung vom 12. Juli 2023 erforderlich ist.

(2) Verpflichtete haben allein nach Absatz 1 gesicherte Daten unverzüglich nach Übermittlung an die anordnende Stelle, spätestens sobald die Datensicherung gemäß der Verordnung (EU) 2023/1543 in der Fassung vom 12. Juli 2023 nicht mehr erforderlich ist, nach dem Stand der Technik irreversibel zu löschen.“

Artikel 9

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 10

Änderung des Bundeskriminalamtgesetzes

Das Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), das zuletzt durch Artikel 1 des Gesetzes vom 17. Juli 2025 (BGBl. 2025 I Nr. 172) geändert worden ist, wird wie folgt geändert:

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

   „§ 10b Sicherung von Verkehrsdaten“.

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

„§ 10b

Sicherung von Verkehrsdaten

(1) Zur Erfüllung der Aufgabe als Zentralstelle nach § 2 Absatz 1 kann das Bundeskriminalamt zum Zwecke einer etwaigen Erhebung gegenüber demjenigen, der öffentlich zugängliche Telekommunikationsdienste anbietet oder daran mitwirkt, anordnen, Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes von betroffenen Personen unverzüglich zu sichern (Sicherungsanordnung), wenn die zuständige Strafverfolgungsbehörde oder die zuständige Polizeibehörde noch nicht erkennbar ist und

1. zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Straftat begangen worden ist, welche eine Erhebung der Verkehrsdaten nach § 100g Absatz 1 bis 4 der Strafprozessordnung rechtfertigen würde, oder

2. tatsächliche Anhaltspunkte dafür vorliegen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat im Sinne von § 100g Absatz 1 Satz 1 Nummer 1 der Strafprozessordnung begehen wird, und

   a) nach Feststellung der Zuständigkeit einer Landespolizeibehörde eine Erhebung durch sie nach den jeweils für sie geltenden Vorschriften ermöglicht werden kann oder

   b) nach Feststellung der Zuständigkeit des Bundeskriminalamts gemäß § 5 Absatz 1 eine Erhebung nach § 52 Absatz 1 ermöglicht werden kann oder

3. tatsächliche Anhaltspunkte dafür vorliegen, dass eine Person mit einer Person nach Nummer 2 in nicht nur flüchtigem oder in zufälligem Kontakt und in einer Weise in Verbindung steht, welche die Annahme rechtfertigt, dass nach Gewinnung weiterer Erkenntnisse

   a) nach Feststellung der Zuständigkeit einer Landespolizeibehörde eine Erhebung durch sie nach den jeweils für sie geltenden Vorschriften ermöglicht werden kann oder

   b) nach Feststellung der Zuständigkeit des Bundeskriminalamts gemäß § 5 Absatz 1 eine Erhebung nach § 52 Absatz 1 ermöglicht werden kann.

Die Daten müssen für die jeweiligen Zwecke der Erhebung von Bedeutung sein können.

(2) Die Anordnung darf nur durch die zuständige Abteilungsleitung des Bundeskriminalamts oder deren Vertretung angeordnet werden. Die zuständige Abteilungsleitung kann die Anordnungsbefugnis auf Bedienstete des Bundeskriminalamts mit Befähigung zum Richteramt übertragen.

(3) Die Anordnung 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,

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 sowie

5. die wesentlichen Gründe für die Anordnung der Maßnahme.

Abweichend von Satz 2 Nummer 2 genügt bei der Sicherung von Daten einer Funkzelle eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre.

(4) Die Anordnung ist auf höchstens drei Monate zu befristen. Das Bundeskriminalamt informiert nach Feststellung der Zuständigkeit eines Landes die zuständige Landespolizeibehörde über die Anordnung.

(5) Der auf Grund einer Sicherungsanordnung nach Absatz 1 Verpflichtete hat die von der Anordnung erfassten Daten unverzüglich und vollständig zu sichern. Ob und in welchem Umfang für die unverzügliche Sicherung nach Absatz 1 Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. Der Umfang der Entschädigung bemisst sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes.“

3. § 52 wird wie folgt geändert:

a) In Absatz 1 in der Angabe vor Nummer 1 wird die Angabe „(§§ 9 und 12 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes) erheben“ durch die Angabe „gemäß § 3 Nummer 70 des Telekommunikationsgesetzes bei demjenigen erheben, der öffentlich zugängliche Telekommunikationsdienste anbietet oder daran mitwirkt,“ ersetzt.

b) Nach Absatz 2 wird der folgende Absatz 3 eingefügt:

„(3) Zum Zwecke einer etwaigen Erhebung nach Absatz 1 darf angeordnet werden, dass Verpflichtete nach Absatz 1 Verkehrsdaten von betroffenen Personen unverzüglich zu sichern haben, wenn

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

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

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

c) Der bisherige Absatz 3 wird zu Absatz 4 und in Satz 1 wird die Angabe „§ 51 Absatz 3 bis 6 gilt“ durch die Angabe „Für Maßnahmen nach den Absätzen 1 und 2 gilt § 51 Absatz 3 bis 6“ ersetzt.

d) Nach Absatz 4 werden die folgenden Absätze 5 bis 8 eingefügt:

„(5) Die Maßnahme nach Absatz 3 darf nur durch die zuständige Abteilungsleitung des Bundeskriminalamts oder deren Vertretung angeordnet werden. Die zuständige Abteilungsleitung kann die Anordnungsbefugnis auf Bedienstete des Bundeskriminalamts mit Befähigung zum Richteramt übertragen.

(6) Die Anordnung nach Absatz 3 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,

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 sowie

5. die wesentlichen Gründe für die Anordnung der Maßnahme.

Abweichend von Satz 2 Nummer 2 genügt bei der Sicherung von Daten einer Funkzelle eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre.

(7) Die Anordnung ist auf höchstens drei Monate zu befristen und darf nur auf Antrag der zuständigen Abteilungsleitung des Bundeskriminalamts oder deren Vertretung durch das Gericht um höchstens drei Monate verlängert werden.

(8) Der auf Grund einer Sicherungsanordnung nach Absatz 3 Verpflichtete hat die von der Anordnung erfassten Daten unverzüglich und vollständig zu sichern. Ob und in welchem Umfang für die Maßnahme nach Absatz 3 Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden.“

Artikel 11

Änderung des Geldwäschegesetzes

Das Geldwäschegesetz vom 23. Juni 2017 (BGBl. I S. 1822), das zuletzt durch Artikel 8 des Gesetzes vom 27. Dezember 2024 (BGBl. 2024 I Nr. 438) 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 die Artikel 1 Nummer 2 und 3 sowie Artikel 6 Nummer 2 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).

Strafverfolgungsbehörden und Polizeibehörden 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 Strafverfolgungs- oder Polizeibehörde 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 Strafverfolgungs- und Polizeibehörden 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 Strafverfolgungs- und Polizeibehörden die Sicherung von Verkehrsdaten veranlassen, sofern und solange die rechtlichen oder tatsächlichen Voraussetzungen einer Datenerhebung zu Zwecken der Strafverfolgung oder der Gefahrenabwehr 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 Strafverfolgungs- und Polizeibehörden 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 Strafverfolgungs- und Gefahrenabwehrbehörden 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 Strafverfolgungs- und Polizeibehörden 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 verhindern und für ihre Ermittlungen künftig auf einen größeren Bestand an Verkehrsdaten 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 Gesetzentwurf enthält ferner eine systematische Neuordnung der §§ 100g, 100j und 100k StPO sowie der in § 101a StPO enthaltenen hierauf bezogenen Verfahrensvorschriften.

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

Die Folgeänderungen im Telekommunikationsgesetz und in der Telekommunikations-Überwachungsverordnung 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) und Nummer 11 (Recht der Wirtschaft) sowie aus Artikel 73 Absatz 1 Nummer 7 (Telekommunikation), Artikel 73 Absatz 1 Nummer 9a (Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalpolizeiamt) und Nummer 10 Buchstabe a (Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei).

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 Strafverfahrensrecht 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 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

[*Die Haushaltsausgaben für Bund, Länder und Gemeinden werden nach der Ressortabstimmung und der Länder- und Verbändeanhörung ergänzt.*]

4. Erfüllungsaufwand

a) Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht oder entfällt kein Erfüllungsaufwand.

b) Erfüllungsaufwand für die Wirtschaft

[*Der Erfüllungsaufwand für die Wirtschaft wird nach der Verbändeanhörung ergänzt.*]

c) Erfüllungsaufwand der Verwaltung

aa) Bund

Zum Erfüllungsaufwand bei der Bundesnetzagentur: Durch die vorgesehenen §§ 175 und 176 des Telekommunikationsgesetzes in der Entwurfsfassung (TKG-E) werden die Anbieter öffentlich zugänglicher Telekommunikationsdienste und die Anbieter von Internetzugangsdiensten verpflichtet, insgesamt circa 3.000 Verpflichtete; eine Marginalgrenze ist nicht vorgesehen.

Auf die Bundesnetzagentur kommen durch die §§ 175 und 176 TKG-E folgende Aufgaben zu:

1. Nach den §§ 175 Absatz 3 Satz 2 und 176 Absatz 4 Satz 2 TKG-E sind von der Bundesnetzagentur technische Einzelheiten zur Umsetzung der Pflichten in der Technischen Richtlinie nach § 170 Absatz 6 TKG festzulegen. Die Technische Richtlinie ist an den jeweiligen Stand der Technik anzupassen (§ 170 Absatz 5 TKG in Verbindung mit § 36 Satz 3 Telekommunikations-Überwachungsverordnung).

2. Nach §§ 175 Absatz 3 Satz 4 und 176 Absatz 4 Satz 4 TKG-E ist von der Bundesnetzagentur bei den Verpflichteten die Umsetzung der Vorgaben regelmäßig zu prüfen. Nach der Gesetzesbegründung zu den §§ 175 und 176 TKG-E soll die Überprüfung etwa alle zwei Jahre erfolgen.

Für diese Aufgaben setzt die Bundesnetzagentur einen Personalaufwand von 25 Vollzeitäquivalenten an, und zwar: zwei im höheren Dienst, 15 im gehobenen Dienst und acht im mittleren Dienst.

Der hier angesetzte Personalaufwand für die Bundesnetzagentur ergibt sich aus der Fortschreibung der Aufwandsschätzung zur vorherigen Vorratsdatenspeicherung. Die neuen §§ 175 und 176 TKG-E erzeugen einen zusätzlichen Verwaltungsaufwand. Die Überprüfung soll künftig nicht lediglich regelmäßig, sondern alle zwei Jahre erfolgen. Zudem wird durch § 175 TKG-E der Kreis der Verpflichteten auf alle Diensteanbieter nummernunabhängiger interpersoneller Telekommunikationsdienste erweitert.

Hinsichtlich der weiteren Behörden des Bundes, die die Instrumente der Bestandsdatenabfrage und der Sicherungsanordnung nutzen werden, ist davon auszugehen, dass der Entwurf insgesamt kostenneutral ist. IP-Adressspeicherung und Sicherungsanordnung werden voraussichtlich zusätzlichen Aufwand auslösen, dem aber Einsparungen in mindestens gleicher Höhe gegenüberstehen dürften: Es ist zwar erwartbar, dass die vorsorgliche IP-Adressenspeicherung dazu führt, dass die berechtigten Behörden das Instrument der Bestandsdatenabfrage häufiger einsetzen, was eine entsprechende Entschädigungspflicht auslöst. Außerdem ist zu erwarten, dass Auskunftsersuchen häufiger erfolgreich sind und damit zu weiteren Ermittlungsansätzen führen, die entsprechenden Aufwand nach sich ziehen. Einen ähnlichen Effekt, wenn auch weniger stark ausgeprägt, dürfte die Einführung der Sicherungsanordnung mit sich bringen, da mit einem größeren verfügbaren Datenbestand ebenfalls weitere Ermittlungsansätze einhergehen können. Umgekehrt wird die Einführung der IP-Adressenspeicherung aber auch Einsparungen und Erträge bewirken: Die Bestandsdatenabfrage anhand einer IP-Adresse wird, wenn sie erfolgreich ist, in vielen Fällen einen wertvollen Ermittlungsansatz liefern, nämlich den Inhaber des Anschlusses identifizieren. Dies wird in vielen Fällen andere aufwändige Maßnahmen entbehrlich machen, die ihrerseits entschädigungspflichtig wären. Überdies kommt in Betracht, dass der Betroffene der Maßnahme zur Erstattung verpflichtet ist. Diese Effekte können auch der Sicherungsanordnung zukommen.

Hinsichtlich der Funkzellenabfrage dürfte nennenswerter Mehraufwand nicht entstehen, da die überwiegende Praxis bis Januar 2024 bereits davon ausgegangen ist, dass die Maßnahme bei Straftaten erheblicher Bedeutung, insbesondere solchen nach § 100a Absatz 2 StPO, eingesetzt werden kann.

bb) Länder und Gemeinden

Die Ausführungen unter Doppelbuchstabe aa hinsichtlich der Behörden, die die Instrumente der Bestandsdatenabfrage und der Sicherungsanordnung nutzen werden, sowie hinsichtlich der Funkzellenabfrage gelten entsprechend.

5. Weitere Kosten

Es ist davon auszugehen, dass der Entwurf in Bezug auf die Tätigkeiten im sogenannten justiziellen Kernbereich sowohl für den Bund als auch für die Länder kostenneutral ist. Die Ausführungen unter Ziffer 4 Buchstabe c Doppelbuchstabe aa gelten entsprechend.

Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau für Telekommunikationsdienste, sind im Übrigen nicht zu erwarten.

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-Adressenspeicherung 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 EU-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 ist aufzuheben. Anlass dafür ist das Urteil des Bundesverwaltungsgericht, Urteil 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. 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 bei Berufsgeheimnisträgern vor. Dieser Regelung bedarf es nicht mehr, da sie sich hauptsächlich auf die Erhebung der Daten aus der europarechtswidrigen Vorratsdatenspeicherung bezieht, die aufgehoben werden. Eine neue Speicherpflicht wird zukünftig allein hinsichtlich IP-Adressen eingeführt mit dem Ziel der Identifizierung des Anschlussinhabers. Daraus können keine Erkenntnisse darüber gewonnen werden, mit wem Berufsgeheimnisträger kommuniziert haben. Der Schutz von Berufsgeheimnisträgern ist nach der allgemeinen Schutzvorschrift des § 160a gewährleistet.

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 nicht einher. Ferner sind als Verpflichtete künftig nicht mehr geschäftsmäßige Erbringer, sondern Anbieter von öffentlich zugänglichen Telekommunikationsanbieter benannt sowie die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben. Dies entspricht der Begrifflichkeit des Telekommunikationsgesetzes. Auch diese Anpassung führt nicht zur Änderung der Rechtslage (vergleiche auch Bundestagsdrucksache 19/4671, Seite 61).

Klargestellt ist in der Vorschrift erstmals, dass es sich beim Adressaten der Maßnahme um den Beschuldigten handelt. Dies entspricht bereits der geltenden Rechtslage (vergleiche etwa die insoweit parallele Regelung des § 100j Absatz 1 Satz 1 geltender Fassung). 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 geschäftsmäßig Telekommunikationsdienste erbringen 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.

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.

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 ist lediglich zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre. Dies entspricht der bisherigen Rechtslage (§ 100g Absatz 1 Satz 2 geltende Fassung).

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 für unanwendbar wegen Verstoßes gegen das Unionsrecht erklärt worden (siehe näher im Allgemeinen Teil der Begründung unter I.). Tatsächlich erbringt der Abruf 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 retrograder 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.

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.

Die Erhebung zukünftig anfallender Verkehrsdaten in einer Funkzelle ist auf Grundlage von Absatz 3 weiterhin nicht möglich.

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 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. 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 § 176 Absatz 1 Satz 1 TKG neuer Fassung an; auf die Begründung wird insoweit verwiesen.

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 geltenden Absatz 5.

Zu Absatz 7

Zu Satz 1

Neu geregelt wird in Absatz 7 Satz 1 die Sicherungsanordnung.

Ein solches Instrument 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, auch 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 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 unter Nummer 2, zu § 175 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. Notwendig, aber auch ausreichend für die Eigenschaft als Betroffener 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 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 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

Eine Sicherungsanordnung darf nach Nummer 2 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 („Server-TKÜ“) 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)

Die Änderungen betreffen die Regelung der Bestandsdatenabfrage in § 100j. Sie sind im Wesentlichen redaktioneller Natur. Die Überschrift wird neu gefasst und parallel zu § 100g (Erhebung von Verkehrsdaten) und § 100k (Erhebung von Nutzungsdaten) ausgestaltet.

Zu § 100j (Erhebung von Bestandsdaten)

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. Die neu eingeführte dreimonatige Speicherpflicht in § 176 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 –, 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 –, 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 –, 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 unter Nummer 2, zu § 176 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 –, 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 besteht.

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 smarte Systeme in Fahrzeugen, zu denen insbesondere auch Navigations- und Notrufsysteme zählen, unterfallen dem Begriff der digitalen Dienste. Entsprechend sind die dabei entstehenden Fahrzeugdaten, wie etwa Standortdaten, Nutzungsdaten im Sinne von § 100k Absatz 1 (vergleiche Oberlandesgericht Frankfurt am Main, Beschluss vom 20. Juli 2021 − 3 Ws 369/21).

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 eine geringfügige Erweiterung der Abrufbefugnis, denn bislang ist der Abruf nur zulässig, wenn die Erforschung auf andere Weise aussichtslos wäre. Für strengere Anforderungen als bei einer Verkehrsdatenabfrage gibt es jedoch keinen sachlichen Grund.

Zu Absatz 3

Absatz 3 regelt nun die Standortdatenabfrage bei dem Erbringer eines digitalen Dienstes. Derzeit ist sie in Bezug auf gespeicherte (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. Auf die Begründung dort wird verwiesen.

Zu Absatz 5

Die Vorschrift entspricht dem geltenden § 100k Absatz 4.

Zu Absatz 6

Absatz 6 bleibt inhaltlich unverändert und wird nur geringfügig redaktionell angepasst: In der geltenden Fassung wird nicht nur auf die Erhebung von Nutzungsdaten, sondern auch auf „Inhalte der Nutzung“ abgestellt, doch fallen diese bereits unter den Begriff der Nutzungsdaten, sodass das Tatbestandsmerkmal entbehrlich 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, 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 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.

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, die bislang in Absatz 1a enthalten sind. Inhaltliche Änderungen gehen damit nicht einher.

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.

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 § 100j, soweit sich diese auf besonders sensible Daten wie Passwörter bezieht. Die derzeit nach § 100j Absatz 3 bis 5 geltenden Verfahrensregelungen werden in § 101a Absatz 1 integriert. Satz 2 enthält dabei – wie Satz 1 – einen Verweis auf Regelungen des § 100e. Nicht in Bezug genommen ist allerdings § 100e Absatz 3 Satz 1 Nummer 5, der Vorgaben für die Entscheidungsformel bei Maßnahmen in Bezug auf eine Telekommunikationsverbindung betrifft. Dies hat bei der einmaligen Abfrage von Passwörtern keine Entsprechung.

Zugleich werden die Verfahrensregelungen des bisherigen § 100j vereinfacht. 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.

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 –, 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.

Das bisher geltende Recht (§ 100j Absatz 3 Satz 3) sieht vor, dass die gerichtliche Entscheidung „unverzüglich“ nachzuholen ist. Diese Sonderregelung wird gestrichen. Stattdessen gilt gemäß dem Verweis auf § 100e Absatz 1 Satz 3, dass die Anordnung der Bestätigung durch das Gericht „binnen drei Werktagen“ bedarf.

Ausdrücklich aufgenommen wird die Maßgabe, dass eine Verlängerung der Maßnahme nicht in Betracht kommt. Dies rechtfertigt sich aus 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.

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 sind die Sicherungsanordnung nach § 100g Absatz 7 und die Bestandsdatenabfrage in Bezug auf besonders sensible Daten nach § 100j Absatz 3 aufgenommen, außerdem die Abfrage von Identifizierungsdaten bei OTT-1-Diensten auf Grundlage des neu geschaffenen § 100g Absatz 5. Zur Begründung gilt das zu Absatz 2 Ausgeführte entsprechend. 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 4 sowie bei einer Nutzungsdatenerhebung nach § 100k Absatz 1 bis 3 zu erfolgen hat. Dies entspricht der geltenden Rechtslage (vergleiche Absatz 6 Satz 1 und Absatz 7 Satz 1).

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 –, 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 Absätze 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 auch 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

Zu § 10a (Verfahren bei Europäischen Sicherungsanordnungen)

§ 10a konkretisiert Artikel 4 Absatz 3 und 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 Gerichte und 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 neuer Fassung abzustellen, wonach eine Sicherungsanordnung für Verkehrsdaten erlassen werden kann. § 101a Absatz 1 Satz 1 Nummer 3 neuer Fassung bestimmt zudem, dass für die ersten drei Monaten die Staatsanwaltschaft für eine solche Sicherungsanordnung zuständig ist. Sollte eine Verlängerung der Datensicherung angestrebt werden, ist hingegen ein Gerichtsbeschluss erforderlich.

Zu Absatz 2

Absatz 2 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), benennt Absatz 2 die Staatsanwaltschaft als zuständige Stelle. 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. Strafverfolgungskonstellationen 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 zum Justizvergütungs- und -entschädigungsgesetz – 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 20,00 € vorgeschlagen. 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.

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 den Nummern 2 bis 4 erfolgenden Änderungen, die untenstehend erläutert werden, anzupassen.

Zu Nummer 2

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. § 175 und § 176 werden neu gefasst und enthalten künftig Regelungen zur Verarbeitung von Verkehrsdaten aufgrund von Sicherungsanordnungen (§ 175) und zur Speicherpflicht und Verwendungsbefugnis von Verkehrsdaten zur Identifizierung von Anschlussinhabern (§ 176).

Zu § 175 (Verarbeitungsbefugnis von Verkehrsdaten aufgrund von Sicherungsanordnungen)

§ 175 enthält eine Befugnis der Anbieter zur Verarbeitung von Verkehrsdaten im Rahmen der Umsetzung von Sicherungsanordnungen nach § 100g Absatz 7 StPO oder § 10b Absatz 1 des Bundeskriminalamtgesetzes sowie hierauf bezogener Auskunftsverlangen. Ergänzend dazu ist eine Pflicht zur Umsetzung angemessener Maßnahmen zur Datensicherung und zum Datenschutz 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 sind, zu der dafür erforderlichen Verarbeitung der durch die Nutzung des Dienstes vorhandenen sowie künftig anfallenden Verkehrsdaten (§ 3 Nummer 70). Für eine spätere, erforderliche Auskunft oder Datenherausgabe an berechtigte Stellen regelt Absatz 1 ebenso für all diese Adressaten auch die erforderliche Datenverarbeitungsbefugnis.

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 schlechterdings 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 und nicht aus dem Telekommunikationsgesetz.

Konkrete Angaben zur Datensicherung, insbesondere zu den Adressaten, zu erforderlichen Daten sowie zum Zeitraum der Sicherung, enthält die jeweilige Sicherungsanordnung der Strafverfolgungsbehörde.

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 Strafverfolgungsbehörden unverzüglich nachgekommen werden kann.

Nummer 4 enthält eine Löschverpflichtung für die durch eine Sicherungsanordnung zu sichernden Daten unverzüglich nachdem die angeordnete Datenübermittlung an die Strafverfolgungsbehörde 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 spätestens unverzüglich nach Ablauf der in der Sicherungsanordnung genannten Frist nach dem Stand der Technik irreversibel zu löschen oder die irreversible Löschung sicherzustellen.

Die Anforderungen an den Schutz der zu sichernden Daten bleiben damit bewusst hinter den Vorgaben zum Schutz und zur Sicherheit der §§ 176 bis 181 (zur dauerhaft unanwendbar erklärten Vorratsdatenspeicherung, die mit diesem Gesetz aufgehoben werden) 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 auch für die aufgrund der Sicherungsanordnung gespeicherten Daten gelten werden.

Zu Absatz 3

Die in Absatz 2 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 (Telekommunikationsüberwachungsverordnung – 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 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 Sicherheitsanordnungen und Auskunftsverlangen.

Diese Verfahren ermöglichen den verpflichteten Anbietern eine effiziente Bearbeitung von Sicherheitsanordnungen und von Auskunftsverlangen sowie für die berechtigten Stellen ein standardisiertes, technisches Verfahren für die Übermittlung der Sicherheitsanordnung 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 § 176 (Speicherpflicht und Verwendungsbefugnis von Verkehrsdaten zur Identifizierung von Anschlussinhabern)

Die Vorschrift regelt Vorgaben für Anbieter von Internetzugangsdiensten für eine dreimonatige Speicherung von IP-Adressen und erforderlichen weiteren 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 –, 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). Nicht verpflichtet zur vorsorglichen Speicherung sind daher etwa nummernunabhängige interpersonelle Telekommunikationsdienste (OTT-1-Dienste, etwa Messenger- und E-Mail-Dienste) oder Bereitsteller von lokalen drahtlosen Netzwerken (wie etwa der Hotelbetreiber, der seinen Gästen WLAN zur Verfügung stellt).

Die Speicherung dieser Daten hat – wie auch nach § 175 Absatz 3 – so zu erfolgen, dass die Auskunft an die berechtigte Stelle, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung verlangt, unverzüglich erfolgen kann.

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. Häufig steht den Strafverfolgungsbehörden aber die Portnummer beziehungsweise den Ermittlungsbehörden 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.

Im Internetzugangsdienst sind unter anderen eine eindeutige Kennung des Anschlusses sowie eine zugewiesene Benutzerkennung zu speichern. Dabei bezeichnet die

Anschlusskennung den physikalischen Zugangspunkt des Netzbetreibers beim Anschlussinhaber, wie er ebenfalls vom § 172 Absatz 1 Satz 1 Nummer 2 umfasst ist. 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.

Die Speicherfrist wird auf drei Monate festgelegt. Sie beachtet die Anforderung des Europäischen Gerichtshofs aus seinem Urteil vom 30. April 2024 (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 Praxiserfahrung zeigt, dass mit einer Speicherdauer von drei Monaten voraussichtlich ein relevanter Teil der maßgeblichen Fälle abgedeckt werden kann. Die Speicherdauer 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 Behörden, effektiv Straftaten aufzuklären und Gefahren abzuwehren, in angemessenen Ausgleich mit den Grundrechten vor allem der unbescholtenen Bürger, die von der Speicherung betroffen sind.

Satz 2 bestimmt klarstellend, dass Inhalte der Kommunikation, wie 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 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 sichernden 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, C-470/21, 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 4 durch die Bundesnetzagentur sichergestellt.

Nummer 3 gibt vor, dass die Speicherung so zu erfolgen hat, dass die Auskunft an die berechtigten Stellen unverzüglich erfolgen kann. Welche Stellen berechtigt sind, ergibt sich mittelbar aus Absatz 3, 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. Sofern die Verpflichteten nicht zur Sicherung der Daten aufgefordert wurden, haben sie die Daten nach Absatz 1 spätestens unverzüglich nach Ablauf der dreimonatigen Speicherfrist zu löschen. Die Anforderungen an den Schutz der zu sichernden Daten bleiben – wie auch nach § 175 Absatz 1 aus den dort beschriebenen Gründen – bewusst hinter den Vorgaben zum Schutz und zur Sicherheit der §§ 176 bis 181 (zur dauerhaft unanwendbar erklärten Vorratsdatenspeicherung, die mit diesem Gesetz aufgehoben werden) zurück.

Zu Absatz 3

Absatz 3 regelt, dass die Daten nach Absatz 1 zum einen für eine Auskunft nach § 174 Absatz 1 Satz 3 verwendet werden dürfen, 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 der Auskunft 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 vorbereitende Europäische Sicherungsanordnung erlässt.

Satz 3 bestimmt weiter, dass ein leistungsfähiges technisches Verfahren einzusetzen ist, das die getrennte Speicherung nach Absatz 2 Satz 2 nicht beeinträchtigt. Hierzu wird 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, wie 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.

Ferner stellt Absatz 3 klar, dass diese Daten nicht für andere Zwecke verwendet werden dürfen.

Zu Absatz 4

Die in Absatz 3 getroffenen Regelungen des Gesetzes bedürfen wie zu § 175 Absatz 3 der näheren Ausgestaltung. Die Bundesregierung erhält daher die Ermächtigung zum diesbezüglichen Erlass konkretisierender Regelungen der Pflichten nach Absatz 2, 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)

Bei den Änderungen handelt es sich um redaktionelle Folgeänderungen, die aufgrund der Änderung der §§ 175 und 176 sowie Streichung der bisherigen §§ 177 bis 181 erforderlich sind.

Zur Sicherstellung der praktischen Wirksamkeit des § 176 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 dadurch entsteht, dass das Nichtwahren des Stillschweigens bußgeldbewehrt ist, die eigentliche Übermittlungspflicht jedoch nicht.

Zu Nummer 4 (§ 230)

Die Vorschrift regelt, ab wann die Speicherpflicht von Verkehrsdaten zur Identifizierung von Anschlussinhabern nach § 176 gilt.

Zu Artikel 7 (Änderung der Telekommunikations-Überwachungsverordnung)

Es handelt sich um Folgeänderungen in einzelnen Regelungen der §§ 2, 30, 32 und 35 der Verordnung, die aufgrund der Änderung der §§ 175 und 176 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 Nummer 1

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

Zu Absatz 1

Die Regelung enthält den Wortlaut in der geltenden Fassung, lediglich die Absatzzählung wird hinzugefügt.

Zu Absatz 2

Neu geschaffen wird Absatz 2. Danach sind die aufgrund einer Sicherungsanordnung gespeicherten Daten unverzüglich zu löschen, wenn sie an die anordnende Stelle übermittelt worden sind. Denn nach Herausgabe entfällt der Sicherungszweck (siehe dazu Artikel 6 Absatz 2 der Verordnung [EU] 2023/1543 – die Sicherung muss im Hinblick auf ein späteres Ersuchen um Herausgabe notwendig und verhältnismäßig sein). Da die Verordnung (EU) 2023/1543 in Artikel 11 Absätze 1 bis 3 die einzelnen Szenarien der Sicherung – auch für Sonderkonstellationen – aufführt, statuiert Absatz 2 zusätzlich eine generelle Löschverpflichtung für all die dort genannten Fälle des Wegfalls der Sicherungsverpflichtung (vergleiche zu den Pflichten aus Artikel 11 der Verordnung auch die Begründung zu § 18 Absatz 2 Nummer 8 bis 9, Bundestagsdrucksache 21/3192, Seite 50).

Die Löschverpflichtung in § 13a Absatz 2 setzt die Vorgaben der Datenschutzgrundverordnung (DSGVO) um. Telekommunikationsdienste sind keine für die Strafverfolgung zuständigen Behörden im Sinne von Artikel 1 der Richtlinie (EU) 2016/680 (JI-Richtlinie). Daher finden die Löschverpflichtung aus § 75 Absatz 2 des Bundesdatenschutzgesetzes oder § 489 StPO auf sie keine Anwendung. Eine gesonderte Regelung ist deswegen notwendig.

Zu Nummer 2

Zu § 24a (Erfüllung von Pflichten gemäß den Artikeln 10 und 11 der Verordnung (EU) 2023/1543)

Zu Absatz 1

Die Regelung enthält den Wortlaut in der geltenden Fassung, lediglich die Absatzzählung wird hinzugefügt.

Zu Absatz 2

In Absatz 2 wird wiederum eine Löschverpflichtung zur Umsetzung der Vorgaben der DSGVO wie bei Nummer 1 (siehe oben) eingeführt.

Zu Artikel 9 (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 10 (Änderung des Bundeskriminalamtgesetzes)

Mit § 10b und § 52 Absatz 3 wird für das Bundeskriminalamt das Instrument der Sicherungsanordnung für Verkehrsdaten in Wahrnehmung seiner Aufgabe als Zentralstelle nach § 2 Absatz 1 sowie seiner Aufgabe der Abwehr von Gefahren des internationalen Terrorismus nach § 5 Absatz 1 eingeführt.

Zu Nummer 1 (Inhaltsübersicht)

Es handelt sich um redaktionelle Folgeänderung zur Einführung von § 10b.

Zu Nummer 2 (§ 10b – Sicherung von Verkehrsdaten)

Zu § 10b (Sicherung von Verkehrsdaten)

Das Bundeskriminalamt hat nach § 2 Absatz 1 die Aufgabe, als Zentralstelle für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung, Aufklärung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung zu unterstützen. Aufgrund der Bedeutung von Verkehrsdaten für die Gefahrenabwehr und Strafverfolgung als Grundlage der Erkenntnisgewinnung und Ermittlungsansatz ist es für eine effektive Aufgabenerfüllung unerlässlich, dass die Unterstützung der Polizeien auch die Veranlassung einer vorläufigen Sicherung dieser Daten umfasst, sofern und solange die Zuständigkeit einer Strafverfolgungs- oder Polizeibehörde noch nicht erkennbar ist. Das Bundeskriminalamt kann in diesem Fall vorläufig die Sicherung der Daten veranlassen, um zu ermöglichen, dass diese im weiteren Verlauf der Sachverhaltsbearbeitung durch die sachlich und örtlich zuständige Behörde vollständig erhoben werden können, das heißt sie trotz erkannter möglicher Relevanz nicht zwischenzeitlich durch die Telekommunikationsanbieter oder die betroffenen Personen selbst gelöscht werden.

Wie bei der Sicherungsanordnung zum Zwecke der Strafverfolgung ergibt sich der Bedarf für die Einführung der Sicherungsanordnung für das Bundeskriminalamt in Wahrnehmung

seiner Aufgabe als Zentralstelle also aus dem Umstand, dass Verkehrsdaten flüchtig sind. Wie bereits zu Artikel 1 Nummer 2 dargelegt, speichern zum Beispiel die Netzbetreiber die Daten zu betrieblichen Zwecken häufig maximal sieben Tage lang, sofern überhaupt eine Speicherung erfolgt. Bei anderen Telekommunikationsunternehmen wie zum Beispiel E-Mail-Anbietern besteht die Möglichkeit, dass der Kunde seinen Account jederzeit selbst löscht, eine weitere Aufbewahrung der Daten ist dem Anbieter zu geschäftlichen Zwecken dann nicht erlaubt. Es besteht folglich das Risiko, dass die Daten nicht oder nicht mehr vorliegen, sobald sich die Zuständigkeit einer Strafverfolgungs- oder Polizeibehörde beziehungsweise gegebenenfalls des Bundeskriminalamts selbst festgestellt ist und die Voraussetzung für deren Erhebung vorliegen, mit der Konsequenz, dass weitere Ermittlungen wegen des Fehlens von Daten aussichtslos sind. Diesem Risiko ist mit dem Instrument der Sicherungsanordnung für das Bundeskriminalamt als Zentralstelle entgegenzuwirken.

Die Erhebungsbefugnisse verbleiben bei den jeweils zuständigen Strafverfolgungs- und Polizeibehörden des Bundes und der Länder. Bis die Zuständigkeit geklärt ist und die Voraussetzungen für die etwaige Erhebung der Verkehrsdaten vorliegen, soll ausdrücklich lediglich der Verlust der Daten durch die Sicherung verhindert werden. Eine Datenerhebungsbefugnis für die zu sichernden Daten wird dem Bundeskriminalamt in seiner Aufgabe als Zentralstelle nicht zugeschrieben.

Zu Absatz 1

In Absatz 1 wird die Sicherungsanordnung für das Bundeskriminalamt zur Erfüllung der Aufgabe als Zentralstelle nach § 2 Absatz 1 geregelt.

Sofern und solange die Zuständigkeit einer Strafverfolgungs- oder Polizeibehörde noch nicht erkennbar bzw. festgestellt ist, wird das Bundeskrimimalamt befugt, Verkehrsdaten für eine etwaige Erhebung nach § 100g Absatz 1 bis 4 StPO, eine etwaige Erhebung nach den für die zuständigen Landespolizeibehörden geltenden Vorschriften oder eine etwaige Erhebung bei Feststellung der Zuständigkeit des Bundeskriminalamts gemäß § 5 Absatz 1 Satz 1 beim Telekommunikationsunternehmen durch Anordnung zu sichern.

Das Bundeskriminalamt erhält in seiner Aufgabenwahrnehmung als Zentralstelle regelmäßig Hinweise auf Straftaten, bezüglich derer es die zuständige Strafverfolgungs- oder Polizeibehörde in Deutschland ermitteln muss. Dabei handelt es sich um Sachverhalte, die entweder der Gefahrenabwehr oder der Strafverfolgung zugeführt werden müssen. Sie stammen von ausländischen Sicherheitsbehörden, von nachrichtendienstlichen Behörden, entstehen durch eigene Recherchen im Rahmen der Unterstützung des Bundeskriminalamts als Zentralstelle für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung, Aufklärung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung oder werden dem Bundeskriminalamt von privaten Stellen, zum Beispiel Social Media Plattformen, gemeldet. Bis die Zuständigkeit geklärt ist, wird das Bundeskriminalamt befugt, die Sicherung der Verkehrsdaten, die für die weitere effektive und zielgerichtete gefahrenabwehrende oder strafverfolgende Sachbearbeitung von Bedeutung sein können, anzuordnen.

Hinsichtlich der Anforderungen zum Vorliegen von tatsächlichen Anhaltspunkten, dass eine Straftat begangen worden ist, welche die Erhebung nach § 100g Absatz 1 bis 4 StPO rechtfertigen würde, wird auf die Begründung zur Änderung der Strafprozessordnung unter Nummer 2, zu § 100g Absatz 7 StPO, verwiesen.

Für die Sicherungsanordnung zur Gefahrenabwehr müssen tatsächliche Anhaltspunkte vorliegen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat im Sinne von § 100g Absatz 1 Satz 1 Nummer 1 StPO, das heißt eine Straftat von erheblicher Bedeutung, insbesondere eine in §100a Absatz 2 StPO bezeichnete Straftat, begehen wird. Steht diese Person mit einer anderen Person derart in Kontakt beziehungsweise Verbindung, dass eine Verwicklung der anderen

Person in prognostizierte Straftat angenommen werden kann, kann auch in Bezug auf die andere Person eine Sicherungsanordnung erfolgen. In beiden Fällen soll entweder eine Erhebung durch die zuständigen Polizeibehörden nach den jeweils für sie geltenden Vorschriften oder, sofern eine Gefahrenlage im Sinne von § 5 Absatz 1 vorliegt, eine Erhebung durch das Bundeskriminalamt selbst nach § 52 Absatz 1 ermöglicht werden.

Von der Sicherungsanordnung zur Gefahrenabwehr wird damit zum einen die Person erfasst, bei der gestützt auf Tatsachen die Begehung einer Straftat von erheblicher Bedeutung prognostiziert wird. Zum anderen werden Personen erfasst, bei denen tatsächliche Anhaltspunkte für eine Beziehung zu einer solchen Person beziehungsweise für einen Tatbezug bestehen und damit Anhaltspunkte für eine Einbeziehung in den Handlungskomplex der Straftatenbegehung, insbesondere eine Verwicklung in den Hintergrund oder das Umfeld der prognostizierten Straftat, die abgewehrt beziehungsweise verhütet werden soll. Zum Zeitpunkt der Gefahrenprognose kann die für die Erhebung von Verkehrsdaten erforderliche konkrete Wahrscheinlichkeit des Eintretens der Gefahr in Bezug auf einen Störer gegebenenfalls bereits vorliegen, aufgrund der offenen Frage der Zuständigkeit einer Polizeibehörde ist eine unmittelbare Erhebung aber noch nicht möglich. Im Falle der Kontaktpersonen wiederum lassen Anhaltspunkte einen Zusammenhang zur Gefahr beziehungsweise den Gefährder oder Störer erkennen, die nach weiteren Ermittlungen den Gefahrenverdacht verdichten könnten, der eine Erhebung der Daten möglich machen würde.

Wie bereits zu Artikel 1 Nummer 2 dargelegt, darf die Sicherungsanordnung gegenüber denjenigen angeordnet werden, die auch zur Herausgabe verpflichtet wären, also gegenüber allen Telekommunikationsanbietern, siehe näher bei der Begründung zur Änderung der Strafprozessordnung unter Nummer 2, zu § 100g Absatz 7 StPO.

Die Sicherung darf für den Fall einer etwaigen Erhebung angeordnet werden. Die gesicherten Daten dürfen ausschließlich für die korrespondierende Erhebungsmaßnahme verwendet werden, siehe näher bei der Begründung zur Änderung des Telekommunikationsgesetzes unter Artikel 6 Nummer 2, zu § 175 Absatz 1.

Nach Satz 2 müssen die Verkehrsdaten für die jeweiligen Zwecke der Erhebung von Bedeutung sein können. Es reicht aus, dass im Moment der Sicherungsanordnung die Möglichkeit besteht, dass die Verkehrsdaten für die etwaige Erhebung (Abwehr schwerwiegender Gefahren und die Verhütung gewichtiger Straftaten) verwendet werden können. Die erforderliche Prognosestellung, dass die Daten für die weitere Sachverhaltsaufklärung und vollständige Gefahrenausräumung von Bedeutung sein müssen, stellt sicher, dass keine Daten gesichert werden, die mit dem Sachverhalt nicht unmittelbar in Verbindung gebracht werden können.

Zu Absatz 2

Die Vorschrift regelt die Anordnungskompetenz. Die zuständige Abteilungsleitung oder deren Vertretung kann die Anordnungsbefugnis auf Bedienstete des Bundeskriminalamts mit Befähigung zum Richteramt übertragen.

Zu Absatz 3

Die Vorschrift regelt den Anordnungsinhalt. Anzugeben sind der Name und die Anschrift des Betroffenen, soweit dies möglich ist. Diese Einschränkung zielt auf Fälle, in denen die vollständigen Angaben zur Person des Betroffenen der Behörde nicht bekannt sind.

Da bei der Sicherung von in einer Funkzelle angefallenen Verkehrsdaten Informationen zu Rufnummer oder Kennung eines Mobiltelefons noch nicht vorliegen, genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, sodass sämtliche Verkehrsdaten unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 1 oder Nummer 2

und Satz 2 gesichert werden können, die innerhalb einer Funkzelle anfallen oder angefallen sind.

Neben Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sind die Art der zu erhebenden Daten sowie deren voraussichtlich Bedeutung für die Zwecke der Erhebung zu benennen. Zudem muss die schriftliche Angabe der wesentlichen Gründe für die Anordnung der Maßnahme erfolgen.

Zu Absatz 4

Die Vorschrift regelt den Zeitraum der Anordnung. Die Sicherung darf für einen Zeitraum von höchstens drei Monaten angeordnet werden.

Zu Absatz 5

Die Vorschrift regelt die Mitwirkungspflichten und den Entschädigungsanspruch der Verpflichteten. In Bezug genommen werden die Regelungen des Telekommunikationsgesetzes und der Telekommunikations-Überwachungsverordnung. Der Umfang der Entschädigung bemisst sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes.

Zu Nummer 3 (§ 52)

Zu Absatz 1

Die Vorschrift wird redaktionell angepasst, indem Anbieter öffentlich zugänglicher Telekommunikationsdienste als Verpflichtete benannt werden, ohne dass damit eine Änderung an der Rechtslage einhergeht.

Zu Absatz 3

Auch im Rahmen der Wahrnehmung der Aufgabe des Bundeskriminalamts zur Abwehr von Gefahren des internationalen Terrorismus gemäß § 5 Absatz 1 besteht der Bedarf, flüchtige Daten zu sichern, wenn die vorliegenden Erkenntnisse und Informationen noch keine hinreichend konkretisierte Zuordnung einzelner Gefährder oder Störer zulassen. Erforderlich ist eine weitere Verdichtung von Informationen, in deren Zuge sich Verdachtsmomente erhärten, Gefährder oder Störer identifiziert und Verbindungen zwischen Personen erhellt werden, die im Ergebnis eine Erhebung rechtfertigen könnten.

Zu Beginn der Gefahrermittlung kann es vorkommen, dass die Informationslage noch nicht ausreicht, um sie einem konkreten Gefährder oder Störer zuzuordnen. 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 § 52 Absatz 1 zu den dort genannten Personen zulässig. Bis zu dem Zeitpunkt, in dem eindeutig festgestellt ist, dass zu der betroffenen Person eine Datenerhebung im Sinne der Nummer 1 bis Nummer 5 zulässig ist, soll sichergestellt sein, dass relevante Verkehrsdaten zum Beispiel zum E-Mail-Account der Person nicht gelöscht werden. Dies ist insbesondere dann von Bedeutung, wenn die Gefahr besteht, dass die betreffende Person selbst oder gar eine andere Person den Account vollständig löscht.

Das Gleiche gilt für ermittelte Telekommunikationsmittel der Personen im Umfeld des Störers (Sicherung noch gespeicherter Verkehrsdaten zu Mobilfunknummern) 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.

Darüber hinaus muss dem Umstand Rechnung getragen werden, dass bei Vorliegen der Voraussetzungen zur Erhebung von Verkehrsdaten nach § 52 Absatz 1 zeitgleich eine Sicherung der Verkehrsdaten angeordnet werden muss, um einen Datenverlust zu verhindern, bis die technischen Voraussetzungen zur unverzüglichen Erteilung der erforderlichen Auskünfte vorliegen. Vergleiche hierzu auch die Ausführungen zu Artikel 1 Nummer 2 zu § 100g Absatz 7 StPO.

Die Verkehrsdaten müssen für die jeweiligen Zwecke der Erhebung von Bedeutung sein können. Es reicht aus, dass im Moment der Sicherungsanordnung die Möglichkeit besteht, dass die Verkehrsdaten für die etwaige Erhebung (Abwehr schwerwiegender Gefahren und die Verhütung gewichtiger Straftaten) verwendet werden können. Die erforderliche Prognosestellung, dass die Daten für die weitere Sachverhaltsaufklärung und vollständige Gefahrenausräumung von Bedeutung sein müssen, stellt sicher, dass keine Daten gesichert werden, die mit dem Sachverhalt nicht unmittelbar in Verbindung gebracht werden können.

Zu Absatz 4

Es erfolgt eine redaktionelle Anpassung, indem die Verpflichteten benannt werden, ohne dass sich daraus eine Änderung der geltenden Rechtslage ergibt.

Zu Absatz 5

Die Vorschrift regelt die Anordnungskompetenz. Die zuständige Abteilungsleitung oder deren Vertretung kann die Anordnungsbefugnis auf Bedienstete des Bundeskriminalamts mit Befähigung zum Richteramt übertragen.

Zu Absatz 6

Die Vorschrift regelt den Anordnungsinhalt. Anzugeben sind der Name und die Anschrift des Betroffenen, soweit dies möglich ist. Diese Einschränkung zielt auf Fälle, in denen die vollständigen Angaben zur Person des Betroffenen der Behörde nicht bekannt sind.

Da bei der Sicherung von in einer Funkzelle angefallenen Verkehrsdaten Informationen zu Rufnummer oder Kennung eines Mobiltelefons noch nicht vorliegen, genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, sodass sämtliche Verkehrsdaten gesichert werden, die innerhalb einer Funkzelle anfallen oder angefallen sind.

Neben Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sind die Art der zu erhebenden Daten sowie deren voraussichtlich Bedeutung für die Zwecke der Erhebung zu benennen. Zudem muss die schriftliche Angabe der wesentlichen Gründe für die Anordnung der Maßnahme erfolgen.

Zu Absatz 7

Die Sicherung darf für einen Zeitraum von höchstens drei Monaten angeordnet werden. Eine Verlängerung ist einmalig um höchsten drei Monate möglich, kann aber nur auf Antrag der zuständigen Abteilungsleitung oder deren Vertretung durch das Gericht angeordnet werden.

Zu Absatz 8

Die Vorschrift regelt die Mitwirkungspflichten und den Entschädigungsanspruch der Verpflichteten. Die Telekommunikationsunternehmen werden verpflichtet die Verkehrsdaten unverzüglich und vollständig zu sichern. In Bezug genommen werden zudem die Regelungen des Telekommunikationsgesetzes und der Telekommunikations-Überwachungsverordnung. Für die Entschädigung der Diensteanbieter sind die Regelung in § 23 JVEG entsprechend anwendbar.

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 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 werden. 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 und des Telekommunikationsgesetzes in Artikel 6 Nummer 2 eingeschränkt wird.

Zu Artikel 13 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten.