**BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG**

Drucksache 22/16042

22. Wahlperiode

20.08.24

Mitteilung des Senats an die Bürgerschaft

Drittes Gesetz zur Änderung polizeirechtlicher Vorschriften

1. **Ausgangslage/Anlass und Zielsetzung**

   Mit dem Gesetzentwurf sollen insbesondere Vorgaben des Bundesverfassungsgerichtes aus dem Beschluss vom 27. Mai 2020 (1 BvR 1873/13, 1 BvR 2618/13; Bestandsdatenauskunft II), dem Beschluss vom 9. Dezember 2022 (1 BvR 1345/21) und dem Urteil vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) umgesetzt werden.

   Daneben sollen hiermit auch Änderungsbedarfe der polizeilichen Praxis einer gesetzlichen Regelung zugeführt werden.

   Ferner sieht der Entwurf redaktionelle Änderungen vor, da bei der auf die Novellierung 2019 folgenden Anpassung von Polizeidienstvorschriften redaktionelle Unschärfen im nun geltenden Recht aufgefallen sind, die bereinigt werden sollen. Schließlich bedingen Anpassungen im Bundesrecht Folgeänderungen im Landesrecht.

2. **Lösung**

   Anpassung des Gesetzes über die Datenverarbeitung der Polizei und des Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung.

3. **Kosten**

   Durch die Gesetzesänderung entstehen unmittelbar keine Kosten. Für die Umsetzung der Gesetzesänderung, beispielsweise die Erweiterung der Kennzeichnungsverpflichtungen, können Kosten entstehen. Die Mehrkosten sind aktuell nicht quantifizierbar.

4. **Finanzierung**

   Sofern für die Umsetzung Kosten entstehen, werden diese aus den Ermächtigungen der Produktgruppe 275.13 „Vollzugsunterstützung und Ausbildung“ des Aufgabenbereiches 275 Polizei im Einzelplan 8.1 Behörde für Inneres und Sport gedeckt.

5. **Petitum**

   Der Senat beantragt, die Bürgerschaft wolle

   1. von den vorstehenden Ausführungen dieser Drucksache Kenntnis nehmen und
   2. das anliegende Gesetz beschließen.

Anlage

Drittes Gesetz zur Änderung polizeirechtlicher Vorschriften

Vom . . . . . .

Artikel 1

Zweites Gesetz zur Änderung des Gesetzes über die Datenverarbeitung der Polizei

Das Gesetz über die Datenverarbeitung der Polizei vom 12. Dezember 2019 (HmbGVBl. S. 485) zuletzt geändert am 3. Mai 2023 (HmbGVBl. S. 193), wird wie folgt geändert:

1. Das Inhaltsverzeichnis wird wie folgt geändert:
   a) Der Eintrag zu §16 erhält folgende Fassung: „§16 Erkennungsdienstliche Maßnahmen“.
   b) Hinter dem Eintrag zu §16 werden folgende Einträge eingefügt:
      „§16a Molekulargenetische Untersuchung zur Identitätsfeststellung“
      §16b Verarbeitung von DNA-Identifizierungsmustern zur Erkennung von DNA-Trugspuren“.
   c) Der Eintrag zu §34 erhält folgende Fassung: „Grundsätze der Zweckbindung und Zweckänderung“.
   d) Hinter dem Eintrag zu §47 wird folgender Eintrag eingefügt: „§47a Datenübermittlung an Beratungsstellen bei häuslicher Gewalt und Unterstützungsbedarf bei Distanzierungs- und Ausstiegsberatung“.
   e) Der Eintrag zu §57 erhält folgende Fassung: „§57 Datenschutz-Folgenabschätzung“.
   f) Der Eintrag zu §65 erhält folgende Fassung: „§65 Kennzeichnung von Daten“.
   g) Der Eintrag zu §78 wird gestrichen.
2. §2 wird wie folgt geändert:
   a) In Absatz 2 Nummer 2 Buchstabe b wird die Textstelle „Waffen- oder Betäubungsmittelverkehrs“ durch die Textstelle „Waffen-, Cannabis- oder Betäubungsmittelverkehrs“ ersetzt.
   b) Es werden folgende Absätze 23 und 24 angefügt:
      „(23) „Digitaler Dienst“ ist ein Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtline (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. EU Nr. L 241 S. 1).
      (24) „Vorfeldstraftaten“ im Sinne dieses Gesetzes sind Straftatbestände, die Verhaltensweisen erfassen, die vom Gesetzgeber als generell gefährlich für Individualrechtsgüter oder Kollektivrechtsgüter bewertet werden, aber als einzelne Handlungen in räumlicher oder zeitlicher Hinsicht noch vor einer konkreten oder konkretisierten Gefährdung oder gar Verletzung solcher Rechtsgüter liegen können und damit strafbewehrte Vorbereitungshandlungen darstellen.“
3. §4 Absatz 1 wird wie folgt geändert:
   a) In Nummer 1 wird das Wort „oder“ durch ein Komma ersetzt.
   b) In Nummer 2 wird das Komma am Ende durch das Wort „oder“ ersetzt und folgende Nummer 3 angefügt: „3. in Erfüllung einer Verpflichtung zur Amts- oder Vollzugshilfe“.
4. In §11 Absatz 1 Nummer 6 und Absatz 2 wird jeweils das Wort „Erhebung“ durch das Wort „Verarbeitung“ ersetzt.
5. In §15 erhalten die Sätze 1 und 2 folgende Fassung:
   „Die Polizei kann die über Notrufeinrichtungen und -anwendungen geführte Kommunikation sowie den Funkverkehr ihrer Leitstelle aufzeichnen. Im Übrigen ist eine Aufzeichnung der über Notrufeinrichtungen und -anwendungen geführten Kommunikation zulässig, soweit sie zur Gefahrenabwehr oder zur Verhütung von Straftaten erforderlich ist.“
6. §16 wird wie folgt geändert:
   a) Die Überschrift erhält folgende Fassung:
      „Erkennungsdienstliche Maßnahmen“.
   b) Absatz 4 wird aufgehoben.
7. Hinter §16 werden folgende §§16a und 16b eingefügt:
   „§16a Molekulargenetische Untersuchung zur Identitätsfeststellung
   (1) Ist eine Identitätsfeststellung auf andere Weise nicht möglich, darf die Polizei DNA-Material unbekannter Toter, hilfloser oder vermisster Personen sowie, im Falle eines öffentlichen Interesses an der Aufklärung der Identität, von Verwandten im Sinne des §1589 des Bürgerlichen Gesetzbuches vermisster Personen sicherstellen und molekulargenetische Untersuchungen durchführen. Zum

Zwecke der Sicherstellung von DNA-Material dürfen

1. unbekannten Toten, hilflosen Personen oder Verwandten im Sinne des § 1589 des Bürgerlichen Gesetzbuches von vermissten Personen Körperzellen entnommen werden oder
2. Proben von Gegenständen mit Spurenmaterial der vermissten Person genommen werden und
3. die Proben nach den Nummern 1 oder 2 molekulargenetisch untersucht werden.

Für die Entnahme der Körperzellen gilt § 81a Absatz 1 Satz 2 der Strafprozessordnung entsprechend. Die entnommenen Körperzellen sind unverzüglich zu vernichten, sobald sie für die molekulargenetische Untersuchung nicht mehr erforderlich sind. Bei der Untersuchung nach Satz 1 Nummer 3 dürfen andere Feststellungen als diejenigen, die zur Ermittlung des DNA-Identifizierungsmusters sowie des Geschlechts erforderlich sind, nicht getroffen werden; hierauf gerichtete Untersuchungen sind unzulässig. Das erlangte DNA-Identifizierungsmuster kann zur Identitätsfeststellung verarbeitet, insbesondere zum Zwecke des Abgleichs in einem Dateisystem gespeichert werden. Eine Verarbeitung für andere Zwecke ist nicht zulässig. Wenn der Zweck der Maßnahme erreicht ist, ist das DNA-Identifizierungsmuster zu löschen.

(2) Die Entnahme der Körperzellen und die molekulargenetische Untersuchung von DNA-Material von Verwandten im Sinne des § 1589 des Bürgerlichen Gesetzbuches vermisster Personen bedarf ebenso wie die molekulargenetische Untersuchung von DNA-Material hilfloser oder vermisster Personen ohne schriftliche Einwilligung der betroffenen Person der richterlichen Anordnung. Zuständig ist das Amtsgericht Hamburg. Das Verfahren richtet sich nach Buch 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit vom 17. Dezember 2008 (BGBl. I S. 2586, 2587), zuletzt geändert am 15. Juli 2024 (BGBl. I Nr. 237 S. 1, 8), in der jeweils geltenden Fassung. § 81f Absatz 2 der Strafprozessordnung gilt entsprechend. Liegt eine Naturkatastrophe oder ein besonders schwerer Unglücksfall vor, so sind Maßnahmen nach Absatz 1 auch dann zulässig, wenn eine Identitätsfeststellung unbekannter Toter, hilfloser oder vermisster Personen auf andere Weise wesentlich erschwert wäre; einer richterlichen Anordnung bedarf es in diesen Fällen nicht.

§ 16b

Verarbeitung von DNA-Identifizierungsmustern zur Erkennung von DNA-Trugspuren

(1) Die Polizei kann sowohl von ihren Bediensteten als auch von sonstigen Personen, die Umgang mit Spurenmaterial haben oder die Bereiche in ihren Liegenschaften und Einrichtungen betreten müssen, in denen mit Spurenmaterial umgegangen oder dieses gelagert wird, mit deren schriftlicher Zustimmung

1. mittels eines Mundschleimhautabstrichs oder einer hinsichtlich ihrer Eingriffsintensität vergleichbaren Methode Körperzellen entnehmen,
2. diese zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersuchen und
3. die festgestellten DNA-Identifizierungsmuster mit den an Spurenmaterial festgestellten DNA-Identifizierungsmustern automatisiert abgleichen,

um zur Erkennung von DNA-Trugspuren festzustellen, ob an Spurenmaterial festgestellte DNA-Identifizierungsmuster von diesen Personen stammen.

Die entnommenen Körperzellen dürfen nur für die in Satz 1 genannte molekulargenetische Untersuchung verwendet werden; sie sind unverzüglich zu vernichten, sobald sie hierfür nicht mehr erforderlich sind. Bei der Untersuchung dürfen andere Feststellungen als diejenigen, die zur Ermittlung des DNA-Identifizierungsmusters erforderlich sind, nicht getroffen werden; hierauf gerichtete Untersuchungen sind unzulässig.

(2) Die nach Absatz 1 erhobenen Daten sind zu pseudonymisieren und darüber hinaus in einem Dateisystem der Polizei gesondert zu speichern. Eine Verwendung dieser Daten zu anderen als den in den Absatz 1 genanntem Zweck ist unzulässig. Die DNA-Identifizierungsmuster sind zu löschen, wenn sie für die genannten Zwecke nicht mehr erforderlich sind. Die Löschung hat spätestens drei Jahre nach dem letzten Umgang der betreffenden Person mit Spurenmaterial oder dem letzten Zutritt zu einem in Absatz 1 Satz 1 genannten Bereich zu erfolgen. Betroffene Personen sind vor Erteilung der Zustimmung schriftlich über den Zweck und die Weiterverarbeitung sowie die Löschung der erhobenen Daten zu informieren und darüber aufzuklären, dass sie die Zustimmung verweigern sowie jederzeit mit Wirkung für die Zukunft widerrufen können."

8. § 18 wird wie folgt geändert:

   a) Absatz 5 erhält folgende Fassung:

   „(5) Die Polizei darf bei Anhalte- und Kontrollsituationen im öffentlichen Verkehrsraum durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufaufzeichnungen in Fahrzeugen der Polizei Daten ver-

arbeiten, wenn dies zum Schutz der Vollzugsbediensteten oder eines Dritten erforderlich ist. Absatz 4 Sätze 2 und 4 gilt entsprechend.“

b) Hinter Absatz 5 werden folgende neue Absätze 6 bis 8 eingefügt:

„(6) Die Polizei darf bei der Durchführung von Maßnahmen zur Gefahrenabwehr oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten in öffentlich zugänglichen Bereichen personenbezogene Daten durch den offenen Einsatz mittels körpernah getragener Bild- und Tonaufzeichnungsgeräte verarbeiten, wenn dies nach den Umständen zum Schutz von Vollzugsbediensteten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Die am Körper getragenen Bild- und Tonaufzeichnungsgeräte nach Satz 1 dürfen auch im Bereitschaftsbetrieb Aufzeichnungen anfertigen. Aufzeichnungen nach Satz 2 sind automatisch nach höchstens 60 Sekunden zu löschen, es sei denn, es beginnen in dieser Zeitspanne Aufzeichnungen nach Satz 1. In diesem Fall werden die Aufzeichnungen nach Satz 2 gemeinsam mit den Aufzeichnungen nach Satz 1 gelöscht. Aufzeichnungen sind unzulässig in Bereichen, die der Ausübung von Tätigkeiten von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern nach § 53 Absatz 1 der Strafprozessordnung dienen. Absatz 4 Sätze 2 und 4 gilt entsprechend.

(7) In Wohnungen darf eine Maßnahme nach Absatz 6 nur zur Abwehr einer Gefahr für Leib oder Leben von Vollzugsbediensteten oder Dritten durchgeführt werden. Darüber hinaus ist auf Verlangen der von der Maßnahme betroffenen Person, die die Wohnung innehat, aufzuzeichnen, soweit nicht ein anders gerichtetes Verlangen weiterer betroffener Personen, die die Wohnung innehaben, entgegensteht oder sich hierdurch eine Gefahr für Leib und Leben von Vollzugsbediensteten oder Dritten ergibt oder erhöht. Die weitere Verarbeitung einer Aufzeichnung nach Satz 1 zur Gefahrenabwehr oder zur Strafverfolgung ist nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme und die Nichtbetroffenheit des Kernbereichs richterlich festgestellt wurde. Für das Verfahren zur Herbeiführung der Feststellung nach Satz 3 gilt § 22 Absatz 3 Sätze 10 bis 13 entsprechend. Soweit Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt worden sind, gilt § 21 Absatz 3 Sätze 7 bis 11 entsprechend.

(8) Die Polizei darf in öffentlich zugänglichen Bereichen personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen verarbeiten, wenn dies zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist. Absatz 4 Sätze 2 und 4 gilt entsprechend.“

c) Der bisherige Absatz 6 wird Absatz 9.

9. In § 21 Absatz 4 Satz 2 werden hinter dem Wort „Amt“ die Wörter „oder die Polizeiführerin oder den Polizeiführer vom Dienst“ eingefügt.

10. § 22 wird wie folgt geändert:

a) Absatz 6 erhält folgende Fassung:

„(6) Stellt sich nach Auswertung der Daten heraus, dass diese einem Vertrauensverhältnis mit Berufsgeheimnisträgerinnen oder Berufsgeheimnisträgern zuzuordnen sind, dürfen sie nicht verwendet werden.“

b) Absatz 8 Satz 7 wird gestrichen.

c) In Absatz 9 Satz 2 werden hinter dem Wort „Landeskriminalamtes“ die Wörter „oder die Vertretung im Amt“ eingefügt.

11. § 23 Absatz 3 erhält folgende Fassung:

„(3) Auf Grund der Anordnung einer Datenerhebung nach Absatz 1 oder einer Maßnahme nach Absatz 2 hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), nach Maßgabe der Regelungen des Telekommunikationsgesetzes vom 23. Juni 2021 (BGBl. I S. 1858), zuletzt geändert am 6. Mai 2024 (BGBl. I Nr. 149 S. 1, 34), in der jeweils geltenden Fassung und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen der Polizei die Überwachung, Aufzeichnung, Unterbrechung und Verhinderung von Telekommunikationsverbindungen zu ermöglichen.“

12. § 25 Absatz 6 erhält folgende Fassung:

„(6) Nutzungsdaten sind personenbezogene Daten einer Nutzerin oder eines Nutzers von digitalen Diensten, die durch denjenigen, der geschäftsmäßig eigene oder fremde digitale Dienste zur Nutzung bereit hält oder den Zugang zur Nutzung vermittelt, erhoben werden, um die Inanspruchnahme von digitalen Diensten zu ermöglichen oder abzurechnen, insbesondere

1. Merkmale zur Identifikation der Nutzerin oder des Nutzers,
2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
3. Angaben über die von der Nutzerin oder dem Nutzer in Anspruch genommenen digitalen Dienste.“

13. § 26 wird wie folgt geändert:

    a) Absatz 3 erhält folgende Fassung:

    „(3) Daten, bei denen sich nach der Auswertung herausstellt, dass sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit Berufsgeheimnisträgern zuzuordnen sind, dürfen nicht verwendet werden.“

    b) Absatz 5 Satz 6 wird gestrichen.

14. § 27 wird wie folgt geändert:

    a) In Absatz 1 Satz 1 und Absatz 3 Satz 1 wird jeweils das Wort „Telemediendienste“ durch die Wörter „digitale Dienste“ ersetzt.

    b) Absatz 2 erhält folgende Fassung:

    „(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse sowie weiterer zur Individualisierung erforderlicher technischer Daten verlangt werden, wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse liegt, erforderlich ist. Die Entscheidungsgrundlagen für das Auskunftsbegehren sind zu dokumentieren.“

    c) Absatz 4 Satz 2 erhält folgende Fassung:

    „Personen, gegen die sich die Datenerhebungen richteten, sind in den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 hierüber nach Abschluss der Maßnahme zu benachrichtigen.“

    d) Absatz 5 erhält folgende Fassung:

    „(5) Bestandsdaten im Sinne des Absatzes 1 oder 2 sind die nach § 3 Nummer 6, § 172 des Telekommunikationsgesetzes vom 23. Juni 2021 (BGBl. I S. 1858), zuletzt geändert am 6. Mai 2024 (BGBl. I Nr. 149 S. 1, 34), in der jeweils geltenden Fassung und die nach § 2 Absatz 2 Nummer 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I 2021 I, S. 1982, 2022 I S. 1045), zuletzt geändert am 12. Juli 2024 (BGBl. I Nr. 234 S. 1, 19), in der jeweils geltenden Fassung erhobenen Daten.“

15. § 28 Absatz 3 erhält folgende Fassung:

    „(3) Liegen tatsächliche Anhaltspunkte vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Ergeben sich während der Durchführung Anhaltspunkte dafür, dass der Kernbereich privater Lebensgestaltung betroffen ist, ist der Einsatz zu unterbrechen, sobald dies ohne Gefährdung für Leib, Leben oder der weiteren Verwendung als Vertrauensperson möglich ist. Unterbleibt eine Unterbrechung auf Grund einer Gefährdung nach Satz 2, sind die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und die Umstände des Fortsetzens der Maßnahme zu dokumentieren. Die Maßnahme darf fortgeführt werden, wenn zu erwarten ist, dass die Gründe, die zur Unterbrechung geführt haben, nicht mehr vorliegen. Vor der Weitergabe von Informationen hat die eingesetzte Person sowie deren polizeiliche Kontaktperson zu prüfen, ob durch die Information oder die Art und Weise, in der sie erlangt wurden, Erkenntnisse aus dem Kernbereich privater Lebensgestaltung betroffen sind. Bestehen Zweifel, ob bei einer Maßnahme Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen worden sind, entscheidet die oder der behördliche Datenschutzbeauftragte über die Verwendbarkeit und Löschung der Daten. Werden der Person, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist, Erkenntnisse aus dem Kernbereich privater Lebensgestaltung bekannt, gilt § 21 Absatz 3 Sätze 7 bis 11 entsprechend.“

16. § 29 Absatz 5 erhält folgende Fassung:

    „(5) Liegen tatsächliche Anhaltspunkte vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Ergeben sich während der Durchführung Anhaltspunkte dafür, dass der Kernbereich privater Lebensgestaltung betroffen ist, ist der Einsatz zu unterbrechen, sobald dies ohne Gefährdung für Leib, Leben oder der weiteren Verwendung als Verdeckter Ermittler möglich ist. Unterbleibt eine Unterbrechung auf Grund einer Gefährdung nach Satz 2, sind die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und die Umstände des Fortsetzens der Maßnahme zu dokumentieren. Die Maßnahme darf fortgeführt werden, wenn zu erwarten ist, dass die Gründe, die zur Unterbrechung geführt haben, nicht mehr vorliegen. Vor der Weitergabe von Informationen hat die eingesetzte Person zu prüfen, ob durch die Information oder die Art und Weise, in der sie erlangt wurden, Erkenntnisse aus dem Kernbereich privater Lebensgestaltung betroffen sind. Bestehen Zweifel, ob bei einer Maßnahme Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen worden sind, entscheidet die oder der behördliche Datenschutzbeauftragte über die Verwendbarkeit und Löschung der Daten. Soweit Erkenntnisse aus dem Kernbereich privater Lebensgestaltung durch eine Maßnahme

erlangt worden sind, gilt § 21 Absatz 3 Sätze 7 bis 11 entsprechend.“

17. § 30 wird wie folgt geändert:
    a) Absatz 1 Satz 1 wird wie folgt geändert:
        aa) Hinter den Wörtern „bei sich zu führen“ wird die Textstelle „,die Anlegung und Wartung des technischen Mittels zu dulden“ eingefügt.
        bb) In Nummer 3 wird der Punkt am Ende durch das Wort „oder“ ersetzt.
        cc) Es wird folgende Nummer 4 angefügt:
            „4. die Person, der gegenüber die Anordnung getroffen werden soll, nach polizeilichen Erkenntnissen bereits eine Straftat nach § 238 Absatz 1 Nummer 1 des Strafgesetzbuchs begangen hat und bestimmte Tatsachen die Annahme rechtfertigen, dass sie erneut eine Straftat nach § 238 Absatz 1 Nummer 1 des Strafgesetzbuchs begehen wird.“
    b) Absatz 4 Satz 1 erhält folgende Fassung:

        „Die Anordnung nach Absatz 3 ist sofort vollziehbar und auf höchstens drei Monate zu befristen.“
18. § 31 Absatz 1 erhält folgende Fassung:
    a) In Satz 1 werden die Wörter „vorbeugenden Bekämpfung“ durch das Wort „Verhütung“ ersetzt.
    b) Es wird folgender Satz 2 eingefügt:

        „Handelt es sich bei der in Bezug genommenen Straftat in Satz 1 Nummer 1 oder 2 um eine Vorfeldstraftat ist die Maßnahme nur zulässig, wenn eine konkrete oder konkretisierte Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt.“
    c) In dem bisherigen Satz 2 wird hinter der Textstelle „Satz 1“ die Textstelle „und Satz 2“ eingefügt.
19. § 34 erhält folgende Fassung:

„§ 34

Grundsätze der Zweckbindung und Zweckänderung

(1) Die Polizei darf personenbezogene Daten, die sie selbst erhoben hat, verarbeiten, wenn dies

1. zur Erfüllung derselben Aufgabe und
2. zum Schutz derselben Rechtsgüter oder sonstigen Rechte oder zur Verhütung derselben Straftat erforderlich ist.

Eine Verarbeitung für andere Zwecke liegt nicht vor, soweit diese der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Durchführung von Organisationsuntersuchungen, der Datensicherung, Datenschutzkontrolle oder der Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dient. Dies gilt auch für die Verarbeitung personenbezogener Daten zu Aus- und Fortbildungszwecken.

(2) Eine Verarbeitung personenbezogener Daten zu anderen Zwecken, als denjenigen, zu denen sie erhoben worden sind, ist unter Berücksichtigung der jeweiligen Erhebungsschwellen zulässig, wenn

1. mindestens
    a) vergleichbar schwerwiegende Straftaten oder Ordnungswidrigkeiten verhütet oder verfolgt oder
    b) vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte geschützt werden sollen und
2. sich im Einzelfall konkrete Ermittlungsansätze
    a) zur Verhütung oder Verfolgung solcher Straftaten oder Ordnungswidrigkeiten ergeben oder
    b) zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte erkennen lassen,

soweit Vorschriften dieses Gesetzes oder andere Rechtsvorschriften die zweckändernde Weiterverarbeitung nicht besonders regeln. Abweichend von Satz 1 können die vorhandenen der Identifizierung dienenden Daten einer Person, wie insbesondere Namen, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Anschrift (Grunddaten), auch weiterverarbeitet werden, um diese Person zu identifizieren.

(3) Für die Verarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen nach § 22 Absatz 1 erhoben wurden, gelten die Absätze 1 und 2 mit der Maßgabe, dass eine dringende Gefahr im Sinne des § 22 Absatz 1 vorliegen muss. Zu Zwecken der Strafverfolgung dürfen personenbezogene Daten im Sinne des Satzes 1 weiterverarbeitet werden, wenn sie auch dafür unter Einsatz entsprechender strafprozessualer Befugnisse hätten erhoben werden dürfen. Erfolgt die Weiterverarbeitung zweckändernd, ist dies zu dokumentieren. Personenbezogene Daten, die durch Herstellung von Lichtbildern oder Bildaufzeichnungen über eine Person im Wege eines verdeckten Einsatzes technischer Mittel in oder aus Wohnungen erlangt wurden,

dürfen nicht zu Strafverfolgungszwecken verarbeitet werden.

(4) Eine Verarbeitung personenbezogener Daten zu anderen als den ursprünglichen Zwecken ist auch zulässig, wenn

1. eine gesetzliche Vorschrift dies für den Geltungsbereich dieses Gesetzes vorsieht oder zwingend voraussetzt,
2. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die Verteidigung oder die nationale Sicherheit erforderlich ist,
3. sie zur Vollstreckung oder zum Vollzug von Strafen oder von Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Erledigung eines gerichtlichen Auskunftsersuchens erforderlich ist und gesetzliche Regelungen nicht entgegenstehen,
4. dies erforderlich ist, um Angaben der betroffenen Person zu überprüfen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. bei Teilnahme am Privatrechtsverkehr oder zur Durchsetzung öffentlich-rechtlicher Forderungen ein rechtliches Interesse an der Kenntnis der zu verarbeitenden Daten vorliegt und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Personen an der Geheimhaltung überwiegt,
6. offensichtlich ist, dass dies im Interesse der betroffenen Person liegt und sie in Kenntnis des anderen Zwecks ihre Einwilligung erteilen würde,
7. die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen werden durften oder entnommen werden dürfen oder die Daten verarbeitende Stelle sie veröffentlichen dürfte, es sei denn, dass schutzwürdige Interessen der betroffenen Personen offensichtlich entgegenstehen,
8. sie der Bearbeitung von Eingaben, parlamentarischen Anfragen oder Aktenvorlageersuchen der Bürgerschaft dient und überwiegende schutzwürdige Interessen der betroffenen Personen nicht entgegenstehen.

(5) Unterliegen die personenbezogenen Daten einem Berufsgeheimnis und sind sie von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufspflicht übermittelt worden, findet Absatz 4 keine Anwendung.

(6) Bei der Weiterverarbeitung von personenbezogenen Daten ist durch organisatorische und technische Vorkehrungen sicherzustellen, dass die Absätze 1 bis 3 und 5 beachtet werden.

(7) Personenbezogene Daten dürfen nach Maßgabe gesetzlicher Regelungen auch für gemeinsame Dateien des Bundes und der Länder auf den Gebieten des Staatsschutzes und der organisierten Kriminalität in Fällen von erheblicher Bedeutung einschließlich der Vorfeldbeobachtung verarbeitet werden; dies gilt auch für Dateien, die nicht in der Verantwortung von Polizeibehörden errichtet werden. Daten, die nach § 14 erhoben wurden, dürfen für andere Zwecke nur verarbeitet werden, soweit dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist oder Anhaltspunkte dafür vorliegen, dass die Verfolgung einer Straftat von erheblicher Bedeutung ansonsten aussichtslos oder wesentlich erschwert wäre.

(8) Werden wertende Angaben in Dateisystemen gespeichert, muss feststellbar sein, bei welcher Stelle die den Angaben zugrunde liegenden Informationen vorhanden sind. Das Gleiche gilt, wenn in einem Dateisystem Kurzinformationen über bestimmte Sachverhalte gespeichert werden. Wertende Angaben dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen wurden.

(9) In den Fällen, in denen bereits Daten zu einer Person vorhanden sind, können zu dieser Person auch personengebundene Hinweise, die zum Schutz dieser Person oder zum Schutz der Bediensteten der Gefahrenabwehr- und der Bediensteten der Polizeibehörden erforderlich sind, und weitere Hinweise, die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen, verarbeitet werden. Bei personengebundenen Hinweisen, die zugleich den besonderen Kategorien personenbezogener Daten entsprechen, sind die Vorgaben des § 4 zu beachten.

(10) Für die Planung von Maßnahmen der Kriminalitätsbekämpfung kann die Polizei vorhandene personenbezogene Daten über Vermisstenfälle, auswertungsrelevante Straftaten und verdächtige Wahrnehmungen zur Erstellung eines Kriminalitätslagebildes verarbeiten. Ein Kriminalitätslagebild darf Daten von Geschädigten, Zeugen sowie anderen nicht tatverdächtigen Personen nur enthalten, soweit dies zur Zweckerreichung erforderlich ist. Die automatisiert verarbeiteten personenbezogenen Daten sind spätestens am Ende des der Speicherung folgenden Jahres zu löschen.“

20. § 36 Absatz 2 wird wie folgt geändert:

    a) In Satz 1 wird hinter dem Wort „Daten“ die Textstelle „nach Maßgabe von § 34 Absätze 2 und 3“ eingefügt.

    b) Satz 2 wird gestrichen.

21. In § 38 Absatz 1 erhalten die Sätze 1 und 2 folgende Fassung:

    „Die Polizei darf personenbezogene Daten, soweit gesetzlich nichts anderes bestimmt ist, nach Maßgabe von § 34 übermitteln. Die Beachtung der Maßgaben des § 34 gilt auch bei Anwendung der §§ 39 bis 46.“

22. § 47 Absatz 1 Satz 1 wird wie folgt geändert:

    a) In Nummer 1 wird das Komma am Ende durch das Wort „oder“ ersetzt.

    b) In Nummer 2 wird das Komma am Ende durch einen Punkt ersetzt.

    c) Nummer 3 wird gestrichen.

23. Hinter § 47 wird folgender § 47a eingefügt:

„§ 47a

Datenübermittlung an Beratungsstellen bei häuslicher Gewalt und Unterstützungsbedarf bei Distanzierungs- und Ausstiegsberatung

(1) Erlangt die Polizei von Handlungen häuslicher Gewalt Kenntnis, darf sie die für eine Kontaktaufnahme erforderlichen personenbezogenen Daten der volljährigen Personen, von denen häusliche Gewalt ausgegangen ist (betroffene Personen), an eine von der für Soziales zuständigen Behörde bestimmte Beratungsstelle übermitteln. Die Polizei protokolliert die Datenübermittlung an die Beratungsstelle. Die Beratungsstelle darf die Daten ausschließlich und nur einmalig dazu nutzen, den betroffenen Personen unverzüglich Beratung zur Verhütung weiterer Handlungen häuslicher Gewalt anzubieten.

(2) Liegen der Polizei tatsächliche Anhaltspunkte dafür vor, dass bei einer betroffenen Person Unterstützungsbedarf besteht für die Distanzierung von Personen, welche die Begehung von Straftaten befürworten, fördern, unterstützen, vorbereiten, planen oder beabsichtigen, darf die Polizei die für eine Kontaktaufnahme erforderlichen personenbezogenen Daten der betroffenen Person an eine von der für Soziales zuständigen Behörde bestimmte Beratungsstelle übermitteln. Die Übermittlung der Daten an eine geeignete zuständige Beratungsstelle zum Zwecke der Kontaktaufnahme erfolgt mit dem Ziel der Vermittlung in die entsprechenden Unterstützungsangebote. Absatz 1 Sätze 2 bis 3 gilt entsprechend.“

24. § 49 erhält folgende Fassung:

„§ 49

Automatisierte Anwendung zur Auswertung vorhandener Daten

(1) Die Polizei darf rechtmäßig gespeicherte personenbezogene Daten auf einer Analyseplattform automatisiert zusammenführen. Sie darf diese zusammengeführten Daten, auch gemeinsam mit weiteren rechtmäßig erhobenen personenbezogenen Daten, verknüpfen, aufbereiten und auswerten sowie für statistische Zwecke anwenden (automatisierte Anwendung zur Datenanalyse). Die automatisierte Anwendung zur Datenanalyse erfolgt immer anhand anlassbezogener und zielgerichteter Suchkriterien. Sie wird manuell ausgelöst und läuft regelbasiert auf einer von Menschen definierten Abfolge von Analyse- und Verarbeitungsschritten ab.

(2) Die Polizei darf gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse weiterverarbeiten,

1. wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist,
2. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten nach § 100b der Strafprozessordnung begangen werden sollen und dies zur Verhütung oder Verhinderung dieser Straftaten erforderlich ist.

Handelt es sich bei der in Bezug genommenen Straftat in Satz 1 Nummer 2 um eine Vorfeldstraftat ist die Maßnahme nur zulässig, wenn eine konkrete oder konkretisierte Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt. Zum Zweck der automatisierten Anwendung zur Datenanalyse können Vorgangsdaten, Falldaten, Daten aus den polizeilichen Auskunftssystemen, Verkehrsdaten, Nutzungsdaten, Telekommunikationsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch zusammengeführt werden. Datensätze aus gezielten Abfragen in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen können ergänzend einbezogen werden. Eine direkte Anbindung an Internetdienste ist ausgeschlossen. Bei einer Maßnahme nach Satz 1 Nummer 2 dürfen Verkehrsdaten nicht automatisiert in die Analyse einbezogen werden. In die automatisierte Anwendung zur Datenanalyse dür-

fen keine personenbezogenen Daten einbezogen werden, die aus Wohnraumüberwachung und Online-Durchsuchung gewonnen wurden.

(3) Bei der Anwendung zur automatisierten Datenanalyse gilt §34 Absätze 1 und 2 entsprechend. Es ist ein Rollen- und Rechtekonzept und ein Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten zu erstellen. Das Rollen- und Rechtekonzept regelt die zweckabhängige Verteilung sachlich eingeschränkter Zugriffsrechte anhand von Phänomenbereichen. Das Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten regelt, welche personenbezogenen Daten in welcher Weise in die automatisierte Analyse einbezogen werden dürfen. Zum Schutz Unbeteiligter werden deren personenbezogene Vorgangsdaten in eine automatisierte Datenanalyse nicht einbezogen. Das Nähere regelt eine zu veröffentlichende Verwaltungsvorschrift, die insbesondere für Verkehrsdaten eine Speicherfrist von regelmäßig zwei Jahren in der Analyseplattform vorsieht.

(4) Der Zugang zur automatisierten Anwendung zur Datenanalyse ist reglementiert (Zugriffskontrolle). Die Zugriffe unterliegen hierbei der ständigen Protokollierung. Jeder Fall der automatisierten Anwendung zur Datenanalyse ist von der Anwenderin oder dem Anwender zu begründen. Die oder der behördliche Datenschutzbeauftragte ist zur Durchführung stichprobenartiger Kontrollen berechtigt.

(5) Die Einrichtung und wesentliche Änderung einer automatisierten Anwendung erfolgen durch Anordnung der Polizeipräsidentin oder des Polizeipräsidenten oder der Vertretung im Amt. Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist vor der Einrichtung oder wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen. Im Übrigen bleiben die Aufgaben und Befugnisse der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit unberührt."

25. In §51 werden die Sätze 3 bis 6 durch folgende Sätze ersetzt:

„Die Überprüfung erfolgt anhand eines Datenabgleichs mit den Dateisystemen

1. der Polizeien des Bundes und der Länder,
2. der Strafverfolgungsbehörden und Gerichte, wenn Erkenntnisse über Strafverfahren vorliegen,
3. des Verfassungsschutzes,
4. des Bundesamtes für Migration und Flüchtlinge, sofern die zu überprüfende Person die ausländische Staatsangehörigkeit besitzt, sowie
5. der zuständigen Polizeien im Ausland, sofern die zu überprüfende Person ihren Wohnsitz im Ausland hat und dies im Einzelfall erforderlich ist.

Die ersuchte Polizei übermittelt die zum Zwecke der Durchführung der Zuverlässigkeitsüberprüfungen erforderlichen personenbezogenen Daten an die in Satz 3 benannten Stellen. Zur Sammlung der Ergebnisse und deren weitere Verarbeitung übermitteln diese Stellen ihre Rückmeldung an die Polizei. Soweit die Polizei die Berechtigung zum automatisierten Abruf hat, ist auch ein automatisierter Datenabgleich mit den Dateisystemen der in Nummer 1 bis 5 genannten Stellen zulässig. Die ersuchende Stelle hat die betroffene Person vor der schriftlichen Zustimmung über den konkreten Inhalt der Übermittlung und das Verfahren zu belehren und darüber aufzuklären, dass sie die Zustimmung verweigern sowie jederzeit widerrufen kann. Sie ist ferner über die ihr gegenüber den in Satz 3 benannten Stellen zustehenden Rechte auf Auskunft, Berichtigung, Löschung sowie Einschränkung der Verarbeitung sie betreffender Daten zu informieren und darauf hinzuweisen, dass sie sich jederzeit an die Hamburgische Beauftragte für Datenschutz und Informationsfreiheit oder den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit wenden kann."

26. §52 Absatz 3 erhält folgende Fassung:

„(3) Auftragsverarbeiter dürfen ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen keine weiteren Auftragsverarbeiter hinzuziehen. Hat der Verantwortliche dem Auftragsverarbeiter eine allgemeine schriftliche Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, hat der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung unverzüglich zu informieren. Der Verantwortliche kann in diesem Fall die Hinzuziehung oder Ersetzung untersagen."

27. Die Überschrift von §57 erhält folgende Fassung:

„Datenschutz-Folgenabschätzung".

28. §62 Absatz 1 Satz 4 erhält folgende Fassung:

„Neben den nach §54 Absatz 3 zu treffenden Maßnahmen zur Datensicherung sind Maßnahmen zu treffen, die eine stichprobenweise Kontrolle der Zulässigkeit der Abrufe sowie deren stichprobenweise Überprüfung zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen für die Zwecke der Datenschutzkontrolle und der Eigenüberwachung nach §63 ermöglichen, so-

weit der damit verbundene Aufwand in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten steht.“

29. § 63 Absatz 3 erhält folgende Fassung:

„Die Protokolldaten dürfen nur für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung, durch eine dazu befugte öffentliche Stelle, sowie für die Eigenüberwachung, die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten sowie für die Verfolgung von Ordnungswidrigkeiten und die Verhütung oder Verfolgung von Straftaten verwendet werden. Die Protokolldaten sind 36 Monate nach ihrer Generierung zu löschen, es sei denn, dass sie für den in Satz 1 genannten Zweck noch erforderlich sind.“

30. § 65 erhält folgende Fassung:

„§ 65

Kennzeichnung von Daten

(1) Bei der Speicherung in polizeilichen Datei- und Informationssystemen sind personenbezogene Daten wie folgt zu kennzeichnen:

1. Angabe des Mittels der Erhebung einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden,
2. Angabe der Kategorie betroffener Personen bei denjenigen Personen, zu denen zu Identifizierung dienende Daten, wie insbesondere Name, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit oder Anschrift angelegt wurden,
3. Angabe der Rechtsgüter, deren Schutz die Erhebungsvorschrift bezweckt oder der Straftaten oder Ordnungswidrigkeiten, deren Verfolgung oder Verhütung die Erhebungsvorschrift bezweckt,
4. Angabe der Stelle, die die Daten erhoben hat.

Die Kennzeichnung kann durch die Angabe der Rechtsgrundlage ergänzt werden.

(2) Bei einer Übermittlung an eine andere Stelle ist die empfangende Stelle darauf hinzuweisen, dass die Kennzeichnung aufrechtzuerhalten ist.

(3) Absätze 1 bis 2 gelten nicht, soweit eine Kennzeichnung tatsächlich nicht möglich ist. Die Absätze 1 bis 2 gelten bis zum Ablauf des 31. Dezembers 2032 ebenfalls nicht, soweit eine Kennzeichnung aus technischen Gründen nicht möglich ist oder einen unverhältnismäßigen Aufwand erfordern würde.“

31. § 68 Absatz 3 wird wie folgt geändert:

a) Satz 2 erhält folgende Fassung:

„Im Falle des § 22 beträgt die Frist sechs Monate.“

b) Satz 5 erhält folgende Fassung:

„Das Gericht bestimmt die Dauer der weiteren Zurückstellung, im Falle des § 22 jedoch nicht länger als sechs Monate.“

32. In § 75 Satz 3 wird die die Textstelle „Absatz 8“ durch die Textstelle „Absatz 9“ ersetzt.

33. § 78 wird aufgehoben.

Artikel 2

Änderung des Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung

Das Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung vom 14. März 1966 (HmbGVBl. S. 77), zuletzt geändert am 16. April 2024 (HmbGVBl. S. 97), wird wie folgt geändert:

1. § 13 Absatz 1 wird wie folgt geändert:

a) In Nummer 4 wird das Wort „oder“ durch ein Komma ersetzt.

b) In Nummer 5 wird der Punkt am Ende durch das Wort „oder“ ersetzt.

c) Es wird folgende Nummer 6 angefügt:

„6. unerlässlich ist, um eine Anordnung der elektronischen Aufenthaltsüberwachung nach § 30 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) vom 12. Dezember 2019 (HmbGVBl. S. 485), zuletzt geändert am … [einzusetzen sind die Daten der Änderung des Gesetzes über die Datenverarbeitung der Polizei durch Artikel 1 des vorliegenden Gesetzes] (HmbGVBl. S. …), in der jeweils geltenden Fassung durchzusetzen.“

2. In § 14 Absatz 5 Satz 1 wird hinter dem Wort „verwertet“ der Punkt durch ein Semikolon ersetzt und die Textstelle „§ 979 Absatz 1 bis 1b des Bürgerlichen Gesetzbuches gilt entsprechend.“ angefügt.

Artikel 3

Änderung des Hamburgischen Hafensicherheitsgesetzes

In § 27 Satz 1 des Hamburgischen Hafensicherheitsgesetzes vom 11. Mai 2021 (HmbGVBl. S. 311) wird die Textstelle „§§ 76 bis 78“ durch die Textstelle „§§ 76 und 77“ ersetzt.

Begründung

A.

Allgemeines

Dieses Gesetz dient dazu, die Vorgaben des Bundesverfassungsgerichtes zur sog. Bestandsdatenauskunft im Beschluss vom 27. Mai 2021 (1 BvR 1873/13, 1 BvR 2618/13; Bestandsdatenauskunft II) umzusetzen. Ferner ergibt sich Anpassungsbedarf aus dem Beschluss des Bundesverfassungsgerichtes vom 9. Dezember 2022 (1 BvR 1345/21) und aus dem Urteil des Bundesverfassungsgerichtes vom 16. Februar 2023 (1 BvR 2634/20).

Daneben sieht der Gesetzentwurf insbesondere nachfolgende Änderungen vor.

Durch eine Änderung in §15 PolDVG soll die derzeit dem Wortlaut nach auf Anrufe beschränkte Möglichkeit der Aufzeichnung von Notrufen begrifflich die gesamte Kommunikation erfassen, also beispielweise auch dann möglich sein, wenn ein Notruf per NotrufApp einginge.

Die Zulässigkeit der Identitätsfeststellung mittels DNA-Untersuchung wird zur besseren Lesbarkeit zum einen aus dem bisherigen §16 PolDVG herausgelöst und als neuer §16a geregelt. Zum anderen wird der Tatbestand weiter gefasst, um zukünftig einen DNA-Abgleich auch bei einer reinen Vermisstensuche zu ermöglichen, ohne dass zugleich ein unbekannter Toter vorliegt.

Angelehnt an §24 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) wird in einem neuen §16b eine ausdrückliche Regelung für den Aufbau und das Führen einer Referenzdatenbank zur Erkennung von DNA-Trugspuren geschaffen.

Ferner sieht der Gesetzentwurf eine Anpassung der Regelungen für die offene Bild- und Tonaufzeichnung bei Anhalte- und Kontrollsituationen in Fahrzeugen der Polizei entsprechend der bis 2015 bestehenden Rechtslage vor und soll das sog. Pre-Recording beim Einsatz der Body-Cam ermöglichen.

Mit diesem Gesetzentwurf wird das vom Bundesverfassungsgericht entwickelte Kriterium der sog. hypothetischen Datenneuerhebung umgesetzt (siehe BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 u.a., juris Rn. 284 ff.). Die Regelungen orientieren sich an den Formulierungen in §12 BKAG und der Mehrzahl derjenigen Bundesländer, die diese Umsetzung in deren Polizeigesetzen schon vollzogen haben.

Durch einen neuen §47a wird die Übermittlung von Kontaktdaten von Personen, die häusliche Gewalt ausüben, an geeignete Beratungsstellen gesetzlich geregelt.

In §51 PolDVG soll für Zuverlässigkeitsüberprüfungen auf Ersuchen einer öffentlichen oder nichtöffentlichen Stelle der Abfrageumfang erweitert werden.

Daneben sieht der Gesetzentwurf redaktionelle Anpassungen des PolDVG vor. Bei der auf die Novellierung in 2019 folgenden Anpassung von Polizeidienstvorschriften sind redaktionelle Unschärfen im nun geltenden Recht aufgefallen, die bereinigt werden sollen

Schließlich bedingen Anpassungen im Bundesrecht, Folgeänderungen im Landesrecht. Dies betrifft Verweise auf bundesrechtliche Regelungen wie das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG), aber auch die mit dem Erlass des Cannabisgesetz eingetretene Folge, dass die für cannabisbezogene Handlungen bislang geltenden Strafvorschriften der §29ff des Gesetzes über den Verkehr mit Betäubungsmitteln (BtMG) nicht mehr gelten.

B.

Begründung im Einzelnen

I.

Artikel 1 (Gesetz über die Datenverarbeitung der Polizei)

Zu Nummer 1

Es handelt sich um eine redaktionelle Anpassung der Inhaltsübersicht. Auf Grund der gesonderten Regelung der molekulargenetischen Untersuchung zur Identitätsfeststellung ändern sich die Überschriften der Vorschriften. Statt Datenschutz-Folgeabschätzung muss es in §57 Datenschutz-Folgenabschätzung heißen.

Zu Nummer 2

a) Die Ergänzung des Wortes „Cannabis“ in §2 Absatz 2 Nummer 2 lit. b ist eine notwendige Folgeänderung. Mit dem Gesetz zum kontrollierten Umgang mit Cannabis und zur Änderung weiterer Vorschriften (Cannabisgesetz – CanG) wird Cannabis, so wie es bislang in den Anlagen des BtMG definiert war, aus den Anlagen des BtMG entnommen und in das neue Konsumcannabisgesetz (KCanG) und das Medizinal-Cannabisgesetz (MedCanG) überführt. Damit ist Cannabis kein Betäubungsmittel mehr und unterliegt nicht mehr den Vorschriften des BtMG (vgl. BR-Drucksache 367/23, S. 178).

Die für cannabisbezogene Handlungen bislang geltenden Strafvorschriften der §29ff BtMG gelten daher nicht mehr. Stattdessen sehen das KCanG (§34 KCanG) und das MedCanG (§25 MedCanG) Strafvorschriften vor, deren Einteilung in Grundtatbestand, besonders schwere Fälle und Qualifikationstatbestände sich grundsätzlich an den Vorgaben des BtMG orientiert. Deren Bezeichnung der strafbar bleibenden Handlungsformen (Anbau, Handeltreiben, Besitz, Herstellen) orientiert sich grundsätzlich an den Vorgaben des BtMG.

Entsprechende Folgeänderungen hat der Bundesgesetzgeber zum Beispiel bereits bei §104 StPO vorgenommen.

b) Mit der Einfügung eines neuen Absatzes 23 wird ein Gleichlauf mit den bundesgesetzlichen Änderungen durch das Digitale-Dienste-Gesetz vorgenommen. Dieses ersetzt in einer Vielzahl von Fachgesetzen wie der StPO, dem BKAG und dem BPolG den Begriff „Telemedien“ oder „Telemediendienst“ durch den Begriff „digitale Dienste“. Der Telemedienbegriff wird insoweit nicht mehr fortgeführt. Diese Definition entspricht §1 Absatz 4 Nummer 1 des Digitalen-Dienste-Gesetzes, die hier übernommen wurde, anstatt zur Definition auf §1 Absatz 4 Nummer 1 des Digitalen-Dienste-Gesetzes zu verweisen, dass wiederum auf Artikel 1 Absatz 1 Buchstabe b der Richtline (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. September 2015, S. 1) verweist. Hier wie im Digitalen-Dienste-Gesetz wird der Begriff des „digitalen Dienstes“ verwendet, dem wiederum der in der relevanten EU-Gesetzgebung maßgebliche „Dienst der Informationsgesellschaft“, d.h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, zugrunde liegt, vgl. Artikel 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 oder bereits Artikel 2 Buchstabe a der Richtlinie 2000/31/EG i.V.m Artikel 1 Nummer 2 Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48 EG (vgl. BT-Drucksache 20/10031, S. 67).

Mit Absatz 24 wird der Begriff der Vorfeldstraftaten, wie er im Sinne dieses Gesetzes zu verstehen ist, definiert. Hintergrund hierfür ist das Urteil des BVerfG vom 9. Dezember 2023 (1 BvR 1345/21). Damit hat das Bundesverfassungsgericht bestimmte Teile einzelner Vorschriften des SOG MV, die heimliche Überwachungsmaßnahmen vorsehen, für verfassungswidrig erklärt. Zwar sei es dem Gesetzgeber verfassungsrechtlich nicht verwehrt an die Gefahr der Begehung von Vorfeldstraftatbeständen anzuknüpfen. Er müsse dann aber eigens sicherstellen, dass in jedem Einzelfall eine konkrete oder konkretisierte Gefahr für die durch den Straftatbestand geschützten Rechtsgüter vorliegt. Knüpft der Gesetzgeber an die Begehung solcher Straftaten an, muss er also zusätzlich fordern, dass damit bereits eine konkretisierte oder konkrete Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt (BVerfG, a.a.O., Rn. 92). Beispielhaft kann hier auf §89a Absatz 2 StGB verwiesen werden (vgl. BVerfG, a.a.O. Rn. 50). Soweit in diesem Gesetz nachfolgend der Begriff Vorfeldstraftaten verwendet wird, dient Absatz 24 der Definition dieses Begriffs.

Zu Nummer 3

§4 PolDVG diente mit seiner Einfügung in 2019 der Umsetzung von Artikel 10 der DS-RL. Absatz 1 legt fest, unter welchen Voraussetzungen die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig ist und schafft damit eine eigene Rechtsgrundlage für diese Verarbeitungen. Besondere Kategorien personenbezogener Daten werden in §2 Absatz 20 legal definiert. Auf der Grundlage von Artikel 35 GG sowie der zugehörigen Vorschriften des Verwaltungsverfahrensrechts (§§4 ff. VwVfG) leistet die Polizei anderen hoheitlichen Stellen Amtshilfe. Nach der Legaldefinition in §4 Absatz 1 VwVfG handelt es sich hierbei um eine auf Ersuchen geleistete ergänzende Hilfeleistung. Die Amtshilfe zeichnet sich dadurch aus, dass die ersuchte Behörde außerhalb ihres eigenen Zuständigkeitskreises und besonderer Weisungsverhältnisse tätig wird, also eine fremde Aufgabe wahrnimmt. (vgl. Lisken/Denninger PolR-HdB, D. Polizeiaufgaben und Regelungsmuster des polizeilichen Eingriffsrechts (Bäcker) Rn. 40, beck-online). Die Durchführung einer Amtshilfe ist danach keine polizeiliche Aufgabe, denn es wird eine fremde Aufgabe wahrgenommen.

Insbesondere im Rahmen der Corona-Pandemie fiel auf, dass in der Konstellation einer Amtshilfeleistung in Gestalt der Informationshilfe durch die Polizei als ersuchte Behörde – hier: für die Bezirke/Gesundheitsämter als ersuchende Stelle/n – eine (Rück-) Übermittlung besonderer Kategorien personenbezogener Daten durch die Polizei bei kritischer Betrachtung nicht von §4 Absatz 1 Nummer 1 getragen sein könnte. Wie schon im Zuge der Anpassung von §11 Absatz 1 Nummer 1 PolDVG (§6 Nummer 1 PolDVG aF, Drucksache 21/17906, S. 47) kommt auch hier die Problemstellung zum Tragen, dass eine Amts-/Vollzugshilfeleistung gerade nicht zu den eigenen Aufgaben einer Behörde zählt, sondern lediglich eine ihrer Verpflichtungen darstellt.

Die Einfügung der Nummer 3 steht mit Unionsrecht im Einklang. Nach Artikel 10 der DS-RL ist die Verarbeitung besonderer Kategorien personenbezo-

gener Daten erlaubt, wenn sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist, der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat. Gemäß Artikel 9 Absatz 2 lit. b DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten erlaubt, wenn die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. §4 PolDVG stellt im Anwendungsbereich der DSGVO gemäß §1 Absatz 3 Satz 2 PolDVG eine spezifische Bestimmung dar (vgl. §1 Absatz 3 Satz 2 PolDVG).

Zu Nummer 4

Mit der Novellierung 2019 wurde, wie in Artikel 3 Nummer 2 der DS-RL gefordert, der neue Begriff der „Verarbeitung“ als Oberbegriff für Vorgänge, die den umfassenden Umgang mit personenbezogenen Daten bezeichnen, eingeführt. Die Begrifflichkeiten „Löschung“, „Einschränkung der Verarbeitung“ (als neuer Begriff der Sperrung), „Berichtigung“ und „Datenübermittlung“ wurden jedoch daneben als weitere konkretisierende Unterbegrifflichkeiten des Oberbegriffs „Verarbeitung“ verwendet. Vor diesem Hintergrund wurde der Begriff der „Verarbeitung“ verwendet, soweit dies aus Gründen der Systematik und der Verständlichkeit erfolgen kann. Im Übrigen wurden insbesondere die präzisierenden und teils handlungsbegrenzenden Begriffe „Datenerhebung“, „Datenübermittlung“, „Datenabgleich“, „Einschränkung der Verarbeitung“, „Löschung“ und „Berichtigung“ weiterverwendet. Dies sollte auch der Verständlichkeit und Anwendungsfreundlichkeit des Gesetzes für die Polizei dienen.

Der Begriff „Verarbeitung“ fand im Zuge dessen auch Eingang in §11 PolDVG, vormals §6 PolDVG a.F., indem der Begriff „Erhebung“ in der Überschrift und in Satz 1 1. Halbsatz durch den Begriff „verarbeiten“ ersetzt wurde. Danach darf die Polizei unter den in den jeweiligen Nummer 1-7 genannten Voraussetzungen personenbezogene Daten im umfassenden Sinne verarbeiten. Dabei ist versäumt worden, den Begriff „Erhebung“ auch in §11 Absatz 1 Nummer 6 PolDVG zu ersetzen. Für diese Nummer lautet die Norm aktuell, dass die Polizei personenbezogene Daten verarbeiten darf, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person künftig Straftaten begehen wird, und die Erhebung zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist. Dies soll mit der Änderung redaktionell und im Interesse der Schlüssigkeit angepasst werden.

Mit §11 Absatz 2 PolDVG wurde seinerzeit die vormals in §5 Absatz 1 Nummer 2 HmbDSG a.F. geregelte Möglichkeit der Einwilligung, die mit der unmittelbaren Geltung von Artikel 6 Absatz 1 Satz 1 Buchstabe a DS-VO und deren Streichung in der Neufassung des HmbDSG weggefallen ist, ausdrücklich in das PolDVG übernommen. In dieser Konstellation wird es zwar grundsätzlich als ausreichend, aber auch erforderlich angesehen, dass die Person in die Erhebung eingewilligt hat. Auch an dieser Stelle sollte ebenfalls der Begriff „Erhebung“ durch „Verarbeitung“ ersetzt werden. Dies auch deswegen, weil die Voraussetzungen für eine wirksame Einwilligung in §5 normiert werden. In §5 wird durchgehend auf die Verarbeitung Bezug genommen, zB auch dergestalt, dass die betroffene Person für eine wirksame Einwilligung auf den Zweck der Verarbeitung hinzuweisen ist.

Zu Nummer 5

Im Rahmen der Befassung mit der Einführung einer Notruf-App fiel auf, dass die geltende Vorschrift sich begrifflich auf die Aufzeichnung von Anrufen im Notfall beschränkt. Sie ist somit dem Wortlaut nach auf Sprachtelefonie beschränkt. Sie deckt damit nicht den aktuellen Bedarf ab, bereits verfügbare und genutzte andere Kommunikationskanäle aufzuzeichnen (insbesondere auch nummernunabhängiger interpersoneller Telekommunikationsdienste, vgl. §164 Absatz 4 TKG, beispielsweise die NotrufApp); zusätzlich müssen hier auch Chatverläufe berücksichtigt werden, die aufzuzeichnen sind, um diese für mögliche Strafverfahren zugänglich zu machen. Daher soll mit der Änderung begrifflich die gesamte Kommunikation erfasst werden. Klarstellend wird hier erwähnt, dass damit sämtliche mit dem Notruf (technisch untrennbar) in Verbindung stehenden Daten gemeint sind (beispielsweise: Standortdaten, IP-Adressen, Sprachaufzeichnung, vgl. §164 TKG i.V.m. §4 Absatz 2, 4 NotrufV).

Zu Nummer 6

Die molekulargenetische Untersuchung zur Identitätsfeststellung wird zukünftig gesondert in einem §16a geregelt. Die bisher in §16 Absatz 4 PolDVG geregelte Identifizierung unbekannter Toter durch DNA-Material ist daher aufzuheben.

Zu Nummer 7

a) Die Polizei Hamburg hat Ende 2020 das Thema Langzeitvermisste neu bewertet und als Ergebnis eine besondere Dienststelle im LKA für „Vermiss-

tenfälle und Altfallermittlungen“ gegründet, um den gewachsenen Anforderungen bei der Vermisstensachbearbeitung gerecht zu werden und die Prozesse zu optimieren. Die gesetzlichen Änderungen sollen hierzu einen Betrag leisten.

Die Zulässigkeit der Identitätsfeststellung mittels DNA-Untersuchung wird zur besseren Lesbarkeit zum einen aus dem bisherigen §16 PolDVG herausgelöst und als neuer §16a geregelt. Zum anderen wird sie in der Sache erweitert, indem der Tatbestand weiter gefasst wird.

Die Rechtsprechung hat unter Hinweis auf den Wortlaut der Norm, die eine Sicherstellung von DNA-Material und eine molekulargenetische Untersuchung zur „Identitätsfeststellung unbekannter Toter“ erlaubt, einen DNA-Abgleich vermisster Personen an einen unbekannten Toten gekoppelt. Im konkreten Einzelfall müsste also beides vorliegen. Dies entspricht aber nicht der Praxis und war so nicht beabsichtigt. In der Vermisstensachbearbeitung liegt nicht immer zugleich auch ein unbekannter Toter vor, dessen DNA dann mit Spurenmaterial des Vermissten abgeglichen werden könnte. In der Praxis führte dies dazu, dass kein Abgleich bei einer reinen Vermisstensache möglich ist. Daher soll zukünftig eine molekulargenetische Untersuchung zur Identitätsfeststellung unbekannter Toter, hilfloser Personen oder vermisster Personen ermöglicht werden. Zu diesem Zweck können von unbekannten Toten oder hilflosen Personen Körperzellen entnommen werden. Von vermissten Personen ist dies naturgemäß nicht möglich. In diesen Fällen kann daher auf Spurenmaterial an Gegenständen zurückgegriffen werden.

Daneben soll es zukünftig auch möglich sein, die DNA von Verwandten im Sinne des §1589 des Bürgerlichen Gesetzbuches vermisster Personen sicherzustellen und molekulargenetisch zu untersuchen. In der Praxis stimmen die Berechtigten zwar oftmals der Sicherstellung von DNA-Material zu, da sie das Schicksal der vermissten Person schnellstmöglich geklärt wissen wollen. Es gibt aber auch Fälle in denen auf Grund von Streitigkeiten kein Kontakt mehr zu dem Vermissten gewünscht wird. Nicht immer kann dann noch auf Spurenmaterial an Gegenständen der vermissten Person zurückgegriffen werden, sodass die DNA nah verwandter Personen die einzige Möglichkeit wäre, einen Abgleich mit anderen DNA-Identifizierungsmustern vorzunehmen.

Bei der Inanspruchnahme von Angehörigen muss ergänzend ein öffentliches Interesse an der Aufklärung der Identität hinzukommen. Bei der Berücksichtigung derartiger Belange des Gemeinwohls ist die Herstellung von Rechtssicherheit über den Verbleib oder das Wohl und Wehe einer vermissten Person sowie die Zugehörigkeit einer nicht identifizierten hilflosen Person ebenso von Bedeutung wie Rechtsfrieden herzustellen, indem die Identität einer unbekannte Leiche geklärt werden kann. Diese Belange sind dem Individualinteresse Verwandter gegenüberzustellen, die nicht freiwillig an einer eindeutigen Identifizierung mitwirken wollen, um die Identifizierung mit einer unbekannten Leiche oder einer unbekannten hilflosen Person zu ermöglichen.

Stimmen berechtigte bzw. betroffene Personen einer molekulargenetischen Untersuchung zu, muss auf die Befugnis nicht zurückgegriffen werden (vgl. zu §15a NPOG, BeckOK PolR Nds/Waechter, 26. Ed. 1. Februar 2023, NPOG §15a). Es bedarf dann keiner richterlichen Anordnung. Die Vorgaben des §5 PolDVG sind dabei zu berücksichtigen.

In Absatz 1 Satz 3 wird, wie aktuell in §16 Absatz 4 Satz 8, für die Entnahme der Körperzellen die entsprechende Geltung von §81a Absatz 1 S. 2 StPO angeordnet.

Eines Richtervorbehalts bedarf es hierfür aus verfassungsrechtlichen Gründen nicht, da Eingriffe in die körperliche Unversehrtheit gemäß Artikel 2 Absatz 2 Satz 2 GG nicht kraft grundgesetzlicher Anordnung unter einem Richtervorbehalt stehen (BeckOK PolR NRW/Ogorek/Traub, 24. Ed. 15. Januar 2023, PolG NRW §14a Rn. 27). Bei der nicht freiwilligen Entnahme von Körperzellen von Verwandten vermisster Personen, die bisher nicht gesetzlich geregelt war, wird hiervon abweichend in Absatz 2 gleichwohl auch die Entnahme der Körperzellen unter Richtervorbehalt gestellt. Auch insoweit gilt aber, dass hierauf nicht zurückgegriffen werden muss, wenn die betroffene Person zustimmt.

Entsprechende Rechtsgrundlagen zur Durchführung molekulargenetischer Untersuchungen finden sich auch in anderen Polizeigesetzen (vgl. §14a PolG NRW, §31a SOG MV, §19 HSOG, §183a LwVG SH, §21a ASOG Berlin, §15 NPOG).

b) Durch die Einfügung eines neuen §16b (Verarbeitung von DNA-Identifizierungsmustern zur Erkennung von DNA-Trugspuren) wird angelehnt an §24 BKAG eine ausdrückliche Regelung für den Aufbau und das Führen einer Referenzdatenbank geschaffen, indem die Erhebung von DNA-Identifizierungsmustern von Polizeibediensteten als auch von sonstigen Personen, die Umgang mit Spurenmaterial haben oder die Bereiche in ihren Liegenschaften und Einrichtungen betreten müssen, in denen mit Spurenmaterial umgegangen oder dieses gelagert wird mit schriftlicher Zustimmung der betroffenen Person gestattet wird. Dadurch sollen

sog. DNA-Trugspuren, welche durch die genannten Personen entstehen können, ausgeschlossen und damit aufwendige Ermittlungsmaßnahmen die auf Grund von DNA-Trugspuren initiiert werden, vermieden werden. (siehe ähnliche Regelungen in § 23d LSA PolG, § 30 SPolDVG, Artikel 29 BayDSG, § 17 Zollfahndungsdienstgesetz).

Unter Trugspuren versteht man dabei Spuren, die sich an Asservaten befinden, die aber von unbeteiligten Dritten oder höherer Gewalt unabsichtlich verursacht wurden. Trugspuren sind damit vor allem alle materiellen Veränderungen, die nicht im Zusammenhang mit der Begehung von Straftaten stehen. (vgl. Möllers, Wörterbuch der Polizei, Trugspuren:, beck-online, 3. Aufl. 2018).

Die DNA-Analyse nimmt für die Aufklärung von Straftaten eine wesentliche Rolle ein, ist aber wie § 16 PolDVG zeigt, auch bei der Vermisstensachbearbeitung und der Gefahrenabwehr relevant. Die Methoden haben sich dabei in den vergangenen Jahren ständig weiterentwickelt und verfeinert. Mittlerweile ist es möglich, an Kleinstmengen von DNA-Material (Nanogramm) bereits DNA-Identifizierungsmuster festzustellen. Dieser Fortschritt hat jedoch auch den Nachteil, dass die Gefahr der Kontamination solcher Spuren bzw. Spurenträger ebenfalls deutlich gewachsen ist. Es kann nie ausgeschlossen werden, dass Personen, die Spuren sichern, selber Spuren auf relevanten Asservaten hinterlassen. Ohne Vor-Kontrolle anhand einer DNA-Referenzdatenbank gelangen diese Spuren dann fälschlicherweise in die DNA-Analysedatei (DAD).

Ein besonders öffentlichkeitswirksames Beispiel für DNA-Trugspuren, was auch bei der Begründung zu § 24 BKAG genannt wurde, und allgemein verdeutlicht, welche Auswirkungen eine entsprechende Spurenkontamination haben kann, stellt der Fall des sog. „Phantoms von Heilbronn“ dar. Nachdem am 25. April 2007 in Heilbronn auf der Theresienwiese eine Polizistin getötet wurde und ihr Kollege durch einen Kopfschuss schwerste Verletzungen erlitten hatte, wurde am Tatort ein DNA-Identifizierungsmuster einer weiblichen Unbekannten entdeckt. Bei Abgleichen dieses DNA-Identifizierungsmuster mit den polizeilichen Datenbanken wurde festgestellt, dass in 40 weiteren Fällen übereinstimmende genetische Spuren gefunden wurden. Diese Feststellungen führten zu umfangreichen Ermittlungs- und Fahndungsmaßnahmen in den Jahren 2007 bis 2009 in Süddeutschland, Österreich und Frankreich. Letztendlich stellte sich heraus, dass das fragliche DNA-Identifizierungsmuster von einer Mitarbeiterin der Herstellerfirma der für die Spurensicherung eingesetzten Wattestäbchen stammte und es sich damit um eine DNA-Trugspur handelte.

Eine unter Datenschutzgesichtspunkten weniger belastende anonymisierte Speicherung der DNA-Identifizierungsmuster ist nicht möglich. Denn neben der Feststellung, dass es sich um eine Trugspur handelt, ist es von wesentlicher Bedeutung zu ermitteln, auf welche Weise das Spurenmaterial verunreinigt wurde. Nur auf diese Weise lässt sich für künftige Fälle das Risiko einer erneuten Verunreinigung minimieren. Mit einer anonymisierten Speicherung ist dies nicht möglich. (BT-Drucksache 18/11163, S. 103).

Die Verarbeitung der DNA-Identifizierungsmuster ist nur unter engen Voraussetzungen zulässig, insbesondere ist immer auch die schriftliche Zustimmung der betroffenen Person erforderlich. Die Untersuchung der Körperzellen wird strikt begrenzt; ebenfalls die anschließende Verwendung. Nach Absatz 2 erfolgt die Speicherung in einem gesonderten Dateisystem. Die DNA-Identifizierungsmuster sind nach Absatz 2 Satz 3 zu löschen, wenn sie für die genannten Zwecke nicht mehr erforderlich sind. Die Löschung hat spätestens drei Jahre nach dem letzten Umgang der betreffenden Person mit Spurenmaterial oder dem letzten Zutritt zu einem in Absatz 1 Satz 1 genannten Bereich zu erfolgen. Schließlich sind betroffene Personen nach Absatz 2 Satz 5 vor Erteilung der Zustimmung schriftlich über den Zweck und die Weiterverarbeitung sowie die Löschung der erhobenen Daten zu informieren und darüber aufzuklären, dass sie die Zustimmung verweigern sowie jederzeit mit Wirkung für die Zukunft widerrufen können; die Rechtmäßigkeit der Verarbeitung bis zum Widerruf bleibt mithin unberührt.

Zu Nummer 8

a) Mit dem Sechsten Gesetz zur Änderung des Gesetzes über die Datenverarbeitung der Polizei vom 30. Januar 2015 wurde die vormals für den Einsatz in Funkstreifenwagen geschaffene Regelung erweitert. Mit der Neuregelung in 2015 sollte die seinerzeit in § 8 Absatz 5 PolDVG aF geregelte und 2005 eingefügte Norm zur Dokumentation des Einsatzgeschehens vom Funkstreifenwagen aus auf sog. Körperkameras ausgeweitet werden (zur Historie des § 8 Absatz 5 PolDVG aF bei erstmaliger Einfügung, vgl. Drucksache 18/1487, S. 16).

Die Neuregelung in 2015 umfasste – bei gleichzeitiger Heraufsetzung der letztlich für den Einsatz der Körperkameras zugeschnittenenTatbestandsvoraussetzungen – sowohl unmittelbar am Körper getragene Personenkameras als auch die bislang bereits eingesetzten Videokameras in Streifenwagen (vgl. Drucksache 20/12895, S. 2).

In mit Videokameras ausgestatteten Streifenwagen kann in der konkreten Anhaltesituation der Betrieb der Kamera für den Betroffenen erkennbar gestartet werden. Damit soll in erster Linie die Aggressionsbereitschaft gesenkt und das Bewusstsein für Eigensicherungsmaßnahmen bei den Polizeibeamten gestärkt werden (vgl. Drucksache 18/1487, S. 16; vgl. zur Rechtslage in anderen Bundesländern zum Beispiel §30 Absatz 4 POG RPf, §15b PolG NRW).

Mit dem öffentlichen Verkehrsraum werden zum einen alle Verkehrsflächen, die nach dem Wegerecht des Bundes und der Länder oder der Kommunen dem allgemeinen Verkehr gewidmet sind (z.B. Straßen, Plätze, Brücken, Fußwege), erfasst. Ein Verkehrsraum ist darüber hinaus auch dann öffentlich, wenn er ohne Rücksicht auf eine Widmung und ungeachtet der Eigentumsverhältnisse entweder ausdrücklich oder mit stillschweigender Duldung des Verfügungsberechtigten für jedermann oder aber zumindest für eine allgemein bestimmte größere Personengruppe zur Benutzung zugelassen ist und auch tatsächlich so genutzt wird (BGH, Beschluss vom 30. Januar 2013 – 4 StR 527/12 –, Rn. 4, juris).

Mit den Änderungen in Absatz 5 und dem neuen Absatz 6 werden die Voraussetzungen für Bild- und Tonaufzeichnungen in Fahrzeugen der Polizei von denjenigen zum Einsatz der sog. Body-Cam getrennt. Dies dient auch der besseren Übersichtlichkeit und leichteren Anwendbarkeit in der Praxis.

Absatz 5 normiert unter Rückführung der Tatbestandsvoraussetzungen auf das damalige Niveau vor dem 30. Januar 2015 zukünftig wieder nur den offenen Einsatz technischer Mittel in Fahrzeugen der Polizei.

Der neue Absatz 6 wird bei den vergleichsweise höheren Voraussetzungen zum Einsatz der körpernah getragenen Bild- und Tonaufzeichnungsgeräte nicht geändert. D.h. es muss auch weiterhin nach den Umständen zum Schutz von Vollzugsbediensteten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich sein (vgl. zur Einführung der Norm und zur Begründung der Erforderlichkeit, Drucksache 20/12895). Die Beurteilung zur fachlichen Notwendigkeit hat sich insoweit nicht geändert. Neben dem primären Ziel der Deeskalation konflikthafter Situationen werden polizeiliche Einsatzsituationen, die zu strafrechtlichen Verfahren führen, transparenter. In diesen Fällen lassen sich Geschehensabläufe objektiv rekonstruieren.

Neu ist die Zulassung des sog. Pre-Recordings in Satz 4. Beim Pre-Recording zeichnet eine angeschaltete Body-Cam automatisiert im Dauerbetrieb das Geschehen auf. Derartige Aufzeichnungen werden aber nach 60 Sekunden, die als fachlich ausreichend, aber auch erforderlich angesehen werden, automatisiert durch Überschreiben gelöscht, wenn die Aufzeichnung der Bodycam nicht manuell gestartet wird. Erfolgt eine Aufnahme mittels der Bodycam, dürfen die durch die Pre-Recording-Funktion erfassten Daten bis zu einer Dauer von 60 Sekunden vor dem Beginn der Aufzeichnung gespeichert werden (vgl. Satz 3). Passiert dies nicht, erfolgt also keine manuelle Aufnahme, werden die Aufnahmen im Pre-Recording-Modus ständig automatisch überschrieben. Ein isolierter Zugriff auf die im Bereitschaftsbetrieb erfolgende Aufnahme des Pre-Recording ist technisch unterbunden.

Das Pre-Recording dient dazu, das Geschehen, das zur Auslösung der Aufnahme führte, vollständig zu dokumentieren. Dies kann für die Beurteilung des jeweiligen Sachverhalts bedeutsam sein. Indem der Geschehensablauf vor der Aufnahme erfasst wird, wird zugleich die Transparenz polizeilichen Handelns weiter erhöht, da das Entstehen der Situation besser nachvollziehbar ist.

b) In Absatz 7 wird erstmals der Einsatz der Body-Cam in Wohnungen geregelt. Danach darf eine Maßnahme nach Absatz 6, also der offene Einsatz mittels körpernah getragener Bild- und Tonaufzeichnungsgeräte, auch in Wohnungen durchgeführt werden, wenn dies zur Abwehr einer Gefahr für Leib oder Leben von Vollzugsbediensteten oder Dritten erforderlich ist.

Nach Satz 2 ist auf Verlangen der von der Maßnahme betroffenen Person, die die Wohnung innehat, aufzuzeichnen, soweit nicht das anders gerichtete Verlangen weiterer betroffener Personen, die die Wohnung innehaben, entgegensteht oder sich hierdurch eine Gefahr für Leib und Leben von Vollzugsbediensteten oder Dritten ergibt oder erhöht. Der Einsatz von Bodycams in Wohnungen verstärkt den Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung. Das Recht, die Aufzeichnung der Situation zu verlangen, kann die empfundene Belastung der Situation reduzieren und damit einen deeskalierenden Effekt haben, wodurch die präventive Funktion der Bodycam gestärkt wird. Im Einsatzgeschehen kann es aber auch divergierende Auffassungen von Wohnungsinhabern zum Einschalten der BodyCam auf Verlangen geben. Zudem sind Situationen denkbar, in denen die die Aufzeichnung verlangende Person sich hiermit zu einem weiteren eskalativen Verhalten motiviert sieht. Jedoch darf die Umsetzung der Aufzeichnung auf Verlangen nicht dazu führen, dass sich

hierdurch eine Gefahr für Leib oder Leben von Vollzugsbediensteten oder Dritten ergibt oder erhöht. Vor diesem Hintergrund sieht Satz 2, 2. Halbsatz Ausnahmen vor, in denen dem Verlangen einer maßnahmebetroffenen Person nicht entsprochen werden muss. Bei einer Aufzeichnung auf Verlangen bedarf es schließlich nicht der anschließenden gerichtlichen Entscheidung über die weitere Verwendung der Daten, da hier der Eingriff in Artikel 13 durch das Verlangen selbst gerechtfertigt wurde. Aus diesem Grund nimmt Satz 3, der die weitere Verarbeitung einer Aufzeichnung zur Gefahrenabwehr oder zur Strafverfolgung nur zulässt, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt wurde, auch nur auf die Aufzeichnung nach Satz 1 Bezug.

Die weitere Verarbeitung einer Aufzeichnung nach Satz 1 zur Gefahrenabwehr oder zur Strafverfolgung ist nach Satz 3 nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme und die Nichtbetroffenheit des Kernbereichs richterlich festgestellt wurde. Für das Verfahren zur Herbeiführung der Feststellung nach Satz 2 gilt § 22 Absatz 3 Sätze 10 bis 13 entsprechend, d.h. zuständig hierfür ist das Amtsgericht Hamburg.

Der Schrankenregelung des Artikel 13 Absatz 7 GG wurde durch die Eingriffsvoraussetzungen dergestalt Rechnung getragen, dass es sich bei Leib und Leben um besonders gewichtige Rechtsgüter handelt. Dringend im Sinne des Artikel 13 Absatz 7 GG bezieht sich nicht auf die Wahrscheinlichkeit des Schadenseintritts, sondern auf den Umfang des drohenden Schadens. Gemeint ist mithin keine Steigerung auf der Wahrscheinlichkeitsebene, sondern erforderlich ist die hinreichende Wahrscheinlichkeit eines Schadens an einem wichtigen Rechtsgut. Leib und Leben sind solche Rechtsgüter.

Eine Kernbereichsregelung auf der Erhebungsebene ist für diese Maßnahme verfassungsrechtlich nicht erforderlich. Der Einsatz der BodyCam ist eine offene Maßnahme. Anders als bei einer verdeckten Datenerhebung durchbricht die offene Aufzeichnung in Gegenwart des Polizeivollzugsdienstes den geschützten Bereich nicht, sondern dokumentiert lediglich das Geschehen in dem durch die Polizeipräsenz bereits durchbrochenen, sonst üblichen Rahmen. Geschützt vom Kernbereich privater Lebensgestaltung ist insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden, wie es insbesondere bei Gesprächen im Bereich der Wohnung der Fall ist (BVerfG, Beschluss vom 9. Dezember 2022 – 1 BvR 1345/21 –, Rn. 102). Gespräche in Anwesenheit staatlicher Hoheitsträger sind weder eine nichtöffentliche Kommunikation noch ist die Annahme berechtigt, dass diese für niemanden hörbar ist.

Die betroffenen Personen haben es daher als Gegenüber der uniformierten Beamtinnen und Beamten und angesichts der erkennbar laufenden Aufzeichnungsgeräte sowie der grundsätzlich vorzunehmenden Mitteilung der Aufzeichnungen selbst in der Hand, den Kernbereich der privaten Lebensgestaltung dadurch zu schützen, dass privateste, intimste Informationen nicht preisgegeben werden. Auf der Verwertungsebene wird dem Kernbereich durch eine entsprechende Regelung Rechnung getragen.

c) Während sich die bisherigen Regelungen in § 18 auf bestimmte Beobachtungsorte (zB. eine Gewahrsamseinrichtung oder ein Kriminalitätsschwerpunkt) bzw. Anlässe (öffentliche Veranstaltung, bei der Durchführung von Maßnahmen zur Gefahrenabwehr) beschränken, wird mit dem neuen Absatz 8 davon unabhängig die Verarbeitung von Bild- und Tonaufzeichnungen erlaubt (vgl. insoweit Artikel 33 Absatz 2 Nummer 1 PAG). Allerdings ist dies nur unter hohen Tatbestandsvoraussetzungen zulässig. Erforderlich ist insoweit eine Gefahr für Leib, Leben oder Freiheit einer Person. Eine solche (konkrete) Gefahr liegt vor, wenn eine Sachlage festgestellt werden kann, die bei ungehindertem Geschehensablauf in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einem Schaden führen wird. Die hier benannten Schutzgütern sind zudem besonders gewichtig. Der Eingriffsanlass ist mithin eng gefasst.

Hierfür besteht, neben den bereits bestehenden Ermächtigungen auch ein eigener Regelungsbedarf. So ist beispielsweise die Suche nach vermissten Personen, sei es zu Land oder zu Wasser, mittels an einem Hubschrauber oder Drohnen befestigten Bild- und Tonaufnahmegeräten ein solcher möglicher Anwendungsfall. Sollten technische Mittel zur Anfertigung von Bild- und Tonaufnahmen (luft-)beweglich gemacht werden, zum Beispiel unter Zuhilfenahme einer Drohne (vgl. BeckOK PolR Nds/Albrecht NPOG § 32 Rn. 15-18), muss auf die Offenheit der Maßnahme gegebenenfalls gesondert hingewiesen werden, zum Beispiel durch Hinweisschilder, auf der Kleidung der die Drohne führenden Person oder durch entsprechende Einstellung an der Drohne selbst (akustische oder optische Hinweise).

Zu Nummer 9

§ 21 Absatz 4 Satz 2 PolDVG wird sprachlich neu gefasst, indem als anordnungsbefugt für den Einsatz von Personenschutzsendern neben der Leitung des Landeskriminalamtes oder der Vertretung im Amt

auch die Polizeiführerin oder der Polizeiführer vom Dienst ist. Dies entspricht in der Sache der Regelung der Anordnungsbefugnis wie sie in §22 Absatz 9 Satz 2 PolDVG (Einsatz von Personenschutzsendern innerhalb von Wohnungen, §10a Absatz 8 PolDVG a.F.) zum Ausdruck kommt und wie sie bei der Einführung von §21 Absatz 4 PolDVG im Dezember 2019 ausweislich der Gesetzesbegründung auch beabsichtigt war (vgl. Begründung zu §21 Absatz 4 in Drucksache 21/17906, S. 53).

In der Begründung zu §21 Absatz 4 hieß es seinerzeit: „Mit dem neuen Absatz 4 soll klar gestellt werden, dass es einer solchen Anordnung nicht bedarf, wenn technische Mittel ausschließlich zum Schutz der bei einem polizeilichen Einsatz tätigen Personen mitgeführt oder verwendet werden. Wie bei dem bisherigen §10a Absatz 8 PolDVG darf der Einsatz durch die Leitung des Landeskriminalamtes oder die Polizeiführerin oder den Polizeiführer vom Dienst angeordnet werden.“ (vgl. Drucksache 21/17906, S. 53). Tatsächlich findet sich aber die Polizeiführerin oder der Polizeiführer vom Dienst als anordnungsbefugte Person versehentlich nicht im Gesetzestext. §22 Absatz 9 PolDVG wurde im Vergleich zu §10a Absatz 8 PolDVG a.F. nur sprachlich geschlechterneutral dahingehend geändert, dass es statt Leiter des Landeskriminalamtes nunmehr heißt, dass die Leitung des Landeskriminalamtes anordnungsbefugt ist. Der Polizeiführer vom Dienst war daneben schon in der alten Fassung von §10a Absatz 8 anordnungsbefugt. Diese redaktionelle Unstimmigkeit soll mit der Änderung behoben werden.

Zu Nummer 10

a) Dies ist eine Folgeänderung zur Regelung der hypothetischen Datenneuerhebung in §34 und der besonderen Regelung für die Verwendung von Daten aus einer Wohnraumüberwachung im dortigen Absatz 3. Mit der Rechtsprechung des Bundesverfassungsgerichtes galten bisher und gelten auch weiterhin besondere Vorgaben für die Verarbeitung von personenbezogenen Daten aus Wohnraumüberwachungen (vgl. BVerfG, Urteil v. 20. April 2026, a.a.O., Rn. 283). Da diese Vorgaben in §34 Absatz 3 Berücksichtigung finden, sind die bisherigen Sätze 1, 2, 4 und 5 in §22 Absatz 6 folglich zu streichen.

   Als Vorgabe zur Verwendung von Daten aus einer Wohnraumüberwachung über das für die Datenerhebung maßgebende Verfahren hinaus, hat das Bundesverfassungsgericht entschieden, dass es ausreichend, aber auch erforderlich sei, dass eine den Erhebungsvoraussetzungen entsprechende dringende Gefahr vorliege. Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer solchen Gefahr komme nicht in Betracht (vgl. BVerfG, a.a.O., Rn. 283.). Eine erneute gerichtliche Entscheidung über die Verwendung, wie sie bisher in §22 Absatz 6 Satz 5 geregelt ist, bedarf es mit der Rechtsprechung des Bundesverfassungsgerichtes aber nicht, weswegen sie hier ebenfalls gestrichen wird.

b) Folgeänderung zur Streichung in Absatz 6 und der zentralen Regelung zur Verwendung der Daten in §34. Denn die Löschungsregelung in Absatz 8 Satz 7 nimmt wiederum Bezug auf die Verwendungsregelung in Absatz 6 Satz 4. Sind die Daten nicht mehr zur Aufgabenerfüllung erforderlich, sind sie im Übrigen gemäß §22 Absatz 8 Satz 1 PolDVG zu löschen.

c) Wie auch bei den anderen Vorschriften zur Anordnungsbefugnis wird daneben klarstellend bei §22 Absatz 9 PolDVG die Vertretung im Amt ebenfalls mitbenannt. Schon derzeit wird die Leitung des Landeskriminalamtes in dessen Abwesenheit durch die Vertretung im Amt wahrgenommen, weshalb es sich in der Sache nur um eine sprachliche Präzisierung handelt.

Zu Nummer 11

Hierbei handelt es sich um eine redaktionelle Anpassung in §23 Absatz 3 PolDVG, denn des Telekommunikationsgesetz ist neu erlassen worden und die Zitierung nebst Fundstelle im Bundesgesetzblatt hat sich folglich geändert.

Zu Nummer 12

Ersetzung des Begriffs „Telemedien“. Gleichlauf mit den durch das Digitale-Dienste-Gesetz vorgenommen bundesgesetzlichen Änderungen. Dieses ersetzt in einer Vielzahl von Fachgesetzen wie der StPO, dem BKAG und dem BPolG den Begriff „Telemedien“ oder „Telemediendienst“ durch den Begriff „digitale Dienste“. Der Telemedienbegriff wird insoweit nicht mehr fortgeführt. Eine Definition findet sich in einem neuen §2 Absatz 23.

Zu Nummer 13

a) Hierbei handelt es sich um eine Folgeänderung zur Regelung der hypothetischen Datenneuerhebung in §34. Die Verwendung der Daten wird auch für die nach den §23 bis 25 erlangten Daten nunmehr in §34 als zentrale Vorschrift zur Weiterverarbeitung von personenbezogenen Daten geregelt.

   Dies gilt auch, soweit der bisherige §26 Absatz 3 Satz 6 PolDVG auf den bisherigen §22 Absatz 5 Satz 5 PolDVG verweist, wobei hier zu berücksichtigen ist, dass auf Grund eines redaktionellen Versehens der Verweis fehl geht. Tatsächlich sollte im bisherigen §26 Absatz 3 Satz 6 auf den §22 Absatz 6 Satz 5 PolDVG verwiesen werden, der

wiederum festlegt, dass für die Verwendung der Daten eine gerichtliche Entscheidung notwendig ist. Eine solche gerichtliche Entscheidung ist aber mit der Rechtsprechung nach den Maßstäben des Bundesverfassungsgerichtes zur hypothetischen Datenneuerhebung verfassungsrechtlich gerade nicht erforderlich (vgl. insoweit die Ausführungen zu §34 PolDVG-E).

b) Dies ist eine Folgeänderung zur Streichung in Absatz 3 und der zentralen Regelung zur Verwendung der Daten in §34. Denn die Löschungsregelung in Absatz 5 Satz 6 nimmt wiederum Bezug auf die Verwendungsregelung in Absatz 3 Satz 3. Die Anpassungen bei der Verwendung von Daten wirken sich auch bei den Löschungsregelungen aus. Sind die Daten nicht mehr zur Aufgabenerfüllung erforderlich, sind sie im Übrigen gemäß §26 Absatz 5 Satz 1 PolDVG zu löschen.

Zu Nummer 14

a) Die Ersetzung des Wortes „Telemedien“ in Absatz 1 durch die Wörter „digitale Dienste“ geschieht im Gleichlauf mit den durch das Digitale-Dienste-Gesetz vorgenommen bundesgesetzlichen Änderungen. Zur Begründung siehe bereits oben.

b) Das Bundesverfassungsgericht hat mit Beschluss vom 27. Mai 2020 (BVerfGE 155, 119; 1 BvR 1873/13, 1 BvR 2618/13; Bestandsdatenauskunft II) den §113 des Telekommunikationsgesetzes (TKG) und mehrere Fachgesetze des Bundes, die die manuelle Bestandsdatenauskunft regeln, für verfassungswidrig erklärt. Die Erteilung einer Auskunft über Bestandsdaten sei, so das Bundesverfassungsgericht, grundsätzlich verfassungsrechtlich zulässig. Übermittlungs- und Abrufregelungen müssten aber die Verwendungszwecke der Daten hinreichend begrenzen, indem sie insbesondere tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz vorsähen. Der Senat hat ferner klargestellt, dass die allgemeinen Befugnisse zur Übermittlung und zum Abruf von Bestandsdaten trotz ihres gemäßigten Eingriffsgewichts für die Gefahrenabwehr grundsätzlich einer im Einzelfall vorliegenden konkreten Gefahr und für die Strafverfolgung eines Anfangsverdachts bedürfen. Findet eine Zuordnung dynamischer Internetprotokolladressen (IP-Adressen) statt, muss diese im Hinblick auf ihr erhöhtes Eingriffsgewicht darüber hinaus auch dem Schutz oder der Bewehrung von Rechtsgütern von zumindest hervorgehobenem Gewicht dienen. Im Übrigen hat der Senat wiederholend festgestellt, dass eine Auskunft über Zugangsdaten nur dann erteilt werden darf, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind.

In §27 Absatz 1 Satz 1 PolDVG ist für den Abruf von Bestandsdaten des für eine Gefahr Verantwortlichen oder (unter den Voraussetzungen des §10 SOG) eines Dritten geregelt, dass die Auskunft zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist. Hinzu tritt die weitere Einschränkung in §27 Absatz 1 Satz 2 PolDVG für den Fall, dass das Auskunftsverlangen nach Satz 1 auf Daten bezogen ist, mittels derer ein Zugriff auf Endgeräte oder hiervon räumlich getrennte Speichereinrichtungen geschützt ist (Zugangsdaten): Dann müssen auch die gesetzlichen Voraussetzungen für die Nutzung der erlangten Daten vorliegen.

Absatz 1 genügt damit den Vorgaben des Bundesverfassungsgerichtes, da Voraussetzung für den Abruf im Einzelfall das Vorliegen einer Gefahr für die öffentliche Sicherheit ist und der Abruf von Zugangsdaten darüber hinaus an das Vorliegen der Voraussetzung der Nutzungsnorm geknüpft ist (vgl. BVerfG, a.a.O., Rn. 234 f.).

Hingegen besteht Anpassungsbedarf im Hinblick auf §27 Absatz 2 PolDVG. Die Regelung für den Abruf von IP-Adressen entspricht nicht den Anforderungen des Bundesverfassungsgerichtes, denn Absatz 2 verweist lediglich auf Absatz 1 und hat folglich identische Eingriffsvoraussetzungen. Danach darf die Auskunft nach Absatz 1 auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse sowie weiterer zur Individualisierung erforderlicherer technischer Daten verlangt werden.

Im Hinblick auf das erhöhte Eingriffsgewicht der Zuordnung dynamischer IP-Adressen muss im Einklang mit der Rechtsprechung des Bundesverfassungsgerichtes in §27 Absatz 2 PolDVG die Auskunft dahingehend eingegrenzt werden, dass diese dem Schutz oder der Bewahrung von Rechtsgütern von hervorgehobenem Gewicht dienen.

Um diesen Anforderungen zu entsprechen werden in einem zweiten Halbsatz des Absatzes 2 Rechtsgüter von hervorgehobenem Gewicht benannt. Dies sind als besonders gewichtige Rechtsgüter jedenfalls der Bestand oder die Sicherheit des Bundes oder eines Landes sowie Leib, Leben oder Freiheit einer Person, aber auch Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt (vgl. BVerfGE Band 141, 220). Letzteres sind insbesondere wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen.

In einem neuen Satz 2 wird klargestellt, dass die Entscheidungsgrundlagen für das Auskunftsbegehren zu dokumentieren sind. Dies entspricht ebenfalls einer Vorgabe des Bundesverfassungsgerichts, wonach eine Pflicht zur Dokumentation vorzusehen ist (vgl. BVerfG, a.a.O, Rn. 248f). Zwar folgt bereits aus dem Rechtsstaatsprinzip, dass nur durch Aktenführung und -vorhaltung eine nachprüfbare und nachvollziehbare Grundlage einer Entscheidung entsteht und die gebotene Transparenz gesichert werden kann (vgl. Stelkens/Bonk/Sachs/Kallerhoff/Mayen, 9. Aufl. 2018, VwVfG §29 Rn. 30). Eine Dokumentation des Verwaltungsvorgangs bedürfte damit nicht zwingend eines Ausspruchs im Gesetz. In Umsetzung der ausdrücklichen Forderung des Bundesverfassungsgerichtes im Zusammenhang mit dem Abruf anhand dynamischer IP-Adressen erfolgt dies an dieser Stelle gleichwohl.

c) Die Ersetzung des Wortes „Telemediendienst“ in Absatz 3 durch die Wörter „digitale Dienste“ geschieht im Gleichlauf mit den durch das Digitale-Dienste-Gesetz vorgenommen bundesgesetzlichen Änderungen. Zur Begründung siehe bereits oben.

d) Hiermit wird ein redaktionelles Versehen berichtigt. Der Verweis auf §21 Absatz 3 PolDVG in §27 Absatz 4 Satz 2 PolDVG, wonach für Benachrichtigungen der §21 Absatz 3 PolDVG entsprechend gilt, geht fehl. Die Vorgängerregelung des §27 PolDVG (§10f PolDVG aF) verwies im Hinblick auf die Benachrichtigung seinerzeit auf §9 Absatz 3 PolDVG aF, der die Datenverarbeitung durch den verdeckten Einsatz technischer Mittel regelte (§21 PolDVG). Dies war zum damaligen Zeitpunkt zutreffend, da dort vormals in §9 Absatz 3PolDVG aF die Benachrichtigung geregelt wurde. Mit der Neufassung des PolDVG im Jahr 2019 ist die Benachrichtigung betroffener Personen in §68 PolDVG nunmehr zentral geregelt worden. Durch die Regelung in einer zentralen Norm konnten die bisher in dem §9 PolDVG aF geregelten Vorgaben zur Benachrichtigung und die entsprechenden Verweise in nachfolgenden Normen gestrichen werden. Demzufolge enthält auch §21 Absatz 3 PolDVG, auf den noch fälschlicherweise in §27 Absatz 4 Satz 2 PolDVG verwiesen wird, keine Ausführungen zur Benachrichtigung von Personen, sondern zum Kernbereichsschutz und zum Berufsgeheimnisträgerschutz. Der Verweis ist damit falsch, da es dort gerade nicht um die Benachrichtigung von Personen geht.

Ausreichend aber auch erforderlich, ist die Anordnung, dass Personen, gegen die sich die Datenerhebungen richteten, nach Abschluss der Maßnahme hierüber durch die Polizei zu benachrichtigen sind. Die Art und Weise der Benachrichtigung wird zentral in §68 PolDVG geregelt.

c) Hiermit werden Verweise angepasst. Diese redaktionellen Anpassungen sind notwendig durch entsprechende Änderungen im Bundesrecht.

In §27 Absatz 5 PolDVG werden Bestandsdaten im Sinne des Telekommunikationsgesetzes und des Telemediengesetzes durch entsprechende Verweise auf diese Gesetze definiert. Das Telekommunikationsgesetz wurde zuletzt durch Artikel 1 des Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts, sog. Telekommunikationsmodernisierungsgesetz, vom 23. Juni 2021 (BGBl. I S. 1858) neu erlassen und eine Vielzahl von Paragraphen im Telekommunikationsgesetz haben sich hierdurch bereits in der Nummerierung geändert. Der Regelungsgehalt der vormaligen §§95, 111 Telekommunikationsgesetz findet sich nunmehr in den §§3 Nummer 6, 172 des Telekommunikationsgesetzes.

Der bisherige Regelungsgehalt des §14 Telemediengesetzes findet sich nunmehr in §2 Absatz 2 Nummer 2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz. Im vormaligen §14 Telemediengesetzes wurden Bestandsdaten legal definiert, als personenbezogene Daten eines Nutzers, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind. Eine entsprechende Definition findet sich nunmehr in §2 Absatz 2 Nummer 2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz, wobei der vormalige Begriff „Telemedien“ durch „digitale Dienste“ ersetzt wurde. Danach sind „Bestandsdaten“ diejenigen personenbezogenen Daten, deren Verarbeitung zum Zweck der Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Anbieter von digitalen Diensten und dem Nutzer über die Nutzung von digitalen Diensten erforderlich sind.

Die entsprechenden Verweise in §27 Absatz 5 PolDVG sind daher anzupassen.

Zu Nummer 15

Die Neufassung von §28 Absatz 3 dient der Umsetzung der Entscheidung des Bundesverfassungsgerichtes vom 9. Dezember 2022 (1 BvR 1345/21). Mit der Entscheidung hat das Bundesverfassungsgericht Konkretisierungen hinsichtlich der Einschränkungen zur Erhebung kernbereichsrelevanter Daten im Bereich des Einsatzes sog. Verdeckter Ermittler und

Vertrauenspersonen festgelegt, die der Gesetzgeber umzusetzen hat.

Nach Satz 1 ist die Maßnahme unzulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Nach den Feststellungen des Bundesverfassungsgerichtes ist auf der Ebene der Datenerhebung nach Möglichkeit auszuschließen, dass Kernbereichsinformationen miterfasst werden (BVerfG, a.a.O., Rn. 109 f).

Satz 1 betrifft die Vorgaben des Bundesverfassungsgerichtes, wonach bei verletzungsgeneigten Maßnahmen auf der Ebene der Datenerhebung durch eine vorgelagerte Prüfung sicherzustellen ist, dass die Erfassung von kernbereichsrelevanten Situationen oder Gesprächen jedenfalls insoweit ausgeschlossen ist, als sich diese mit praktisch zu bewältigendem Aufwand im Vorfeld vermeiden lässt. Das Bundesverfassungsgericht erkennt dabei jedoch an, dass es kaum vollständig vermeidbar sei, dass Vertrauenspersonen sowie Verdeckte Mitarbeitende bei ihrem Einsatz kernbereichsrelevante Informationen erhalten (BVerfG a.a.O. Rn. 111 f.). Hierbei ist nach der Rechtsprechung des Bundesverfassungsgerichts als materielle Vorgabe zu berücksichtigen, dass es absolut ausgeschlossen ist, den Kernbereich privater Lebensgestaltung zum direkten Ziel staatlicher Ermittlungen zu machen. Unzulässig sei es demnach auch, eine Beziehung zu der Zielperson aufzubauen, die bereits als solche für diese kernbereichsrelevant ist (BVerfG, a.a.O., Rn. 109 f.). Jedenfalls wenn zum Aufbau oder zum Erhalt des notwendigen Vertrauensverhältnisses intime Beziehungen oder vergleichbar engste persönliche Bindungen, die ansonsten nur Familienangehörige, Partner oder allerengste Freunde haben, begründet oder fortgeführt würden, würde dies in aller Regel schon deshalb in den Kernbereich privater Lebensgestaltung der Zielperson eingreifen, weil staatlich veranlasst privateste Beziehungen auf täuschungsbedingter Grundlage entstünden oder anhielten (BVerfG a.a.O., Rn. 107).

Mit dem neuen Satz 2 wird der Absatz 3 wird um eine Regelung ergänzt, der den Erfordernissen aus der Rechtsprechung des Bundesverfassungsgerichtes zur Gefährdung eingesetzter Personen und zur Sicherung auf der Aus- und Verwertungsebene im Rahmen der Ausnahme vom Unterbrechungsgebot bei Eindringen in den Kernbereich gerecht wird (BVerfG, a.a.O., Rn. 119 ff., Rn. 122 f.). Das Bundesverfassungsgericht entschied, dass grundsätzlich die Unterbrechung der Maßnahme vorzusehen ist, wenn erkennbar wird, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt. Dann ist jedoch nicht zwangsläufig der gesamte Einsatz zu beenden. Je nach den konkreten Umständen kann es zur Vermeidung eines Eindringens in den Kernbereich genügen, dass unter Fortsetzung des Gesamteinsatzes lediglich die kernbereichsrelevante Kommunikation oder Interaktion abgebrochen wird (vgl. BVerfG, a.a.O., Rn. 113). Bei Vertrauenspersonen und Verdeckten Mitarbeitenden besteht indes die Möglichkeit, dass bei einem unvermittelten Abbruch bzw. Unterbrechung der Datenerhebung vor Ort wegen des Eindringens in den Kernbereich die Zielperson Verdacht schöpft. Eine sofortige Unterbrechung könnte zu einer Enttarnung führen und damit zugleich eine erhebliche Gefahr für Leib und Leben der Person begründen (BVerfG, a.a.O., Rn. 114). Vor diesem Hintergrund könne eine Ausnahme vom Unterbrechungsgebot verfassungsrechtlich zu rechtfertigen sein. Das gälte jedenfalls, wenn ansonsten Leib oder Leben der Vertrauenspersonen und Verdeckten Mitarbeitenden in Gefahr gerieten. Verfassungsrechtlich anzuerkennen sei aber auch das ermittlungstechnische Bedürfnis, den weiteren Einsatz von Vertrauenspersonen und Verdeckten Mitarbeitenden zu sichern (BVerfG, a.a.O., Rn. 115). Neben der Gefährdung von Leib oder Leben eingesetzter Personen kann ein Absehen von einer Unterbrechung daher auch gerechtfertigt sein, wenn die Enttarnung zu einer Gefährdung des weiteren Einsatzes im Rahmen der Maßnahme oder der zukünftigen Verwendung der eingesetzten Person führen würde.

Außerdem setzt die Verfassungsmäßigkeit der Ausnahme vom Unterbrechungsgebot voraus, dass weitere Schutzvorkehrungen auf der Auswertungs- und Verwertungsebene bestehen. Ausdrücklich geregelt werden müssten jedenfalls die Pflicht der verdeckt Ermittelnden und der Vertrauenspersonen und ihrer V-Person-Führer, im Fall einer unterbliebenen Unterbrechung die Kernbereichsrelevanz vor der Weitergabe der Information zu überprüfen, gegebenenfalls die fehlende Unterbrechung zu dokumentieren, etwa festgehaltene kernbereichsrelevante Informationen sofort zu löschen oder auf sonstige Weise zu vernichten und dies ebenfalls zu dokumentieren. Ohne solche Sicherungen auf der Aus- und Verwertungsebene ist die Ausnahme vom Unterbrechungsgebot verfassungswidrig. (BVerfG, a.a.O., Rn. 122). Entsprechende Vorgaben werden mit Satz 3 und Satz 6 umgesetzt.

Nach Satz 3 ist auch die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und sind die Umstände des Fortsetzens der Maßnahme zu dokumentieren, wenn ein Abbruch auf Grund einer Gefährdung nach Satz 2 unterbleibt.

Satz 5 setzt die Vorgaben des Bundesverfassungsgerichtes zu spezifischen Prüfpflichten der Vertrauenspersonen und deren polizeilicher Kontaktpersonen hinsichtlich gewonnener Informationen auf kern-

bereichsrelevante Erkenntnisse um und legt den eingesetzten Personen sowie den polizeilichen Kontaktpersonen die Verpflichtung auf, vor der Weitergabe von Informationen zu prüfen, ob durch die Informationen oder die Art und Weise, in der sie erlangt wurden, Erkenntnisse aus dem Kernbereich privater Lebensgestaltung betroffen sind. Entsprechende Erkenntnisse dürfen nicht zur Verwertung weitergeben werden. Denn bei positiver Feststellung eines Kernbereichsbezugs gilt im Übrigen die Regelung in Absatz 5 Satz 7.

Der neu eingefügte Satz 6 setzt die Forderung des BVerfG um, dass in Zweifelsfällen eine Klärung der Kernbereichsrelevanz der gewonnenen Erkenntnisse zumindest durch eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragen zu erfolgen habe (BVerfG, a.a.O., Rn. 119). Bei positiver Feststellung eines Kernbereichsbezugs gilt auch hier im Übrigen die Regelung in Absatz 5 Satz 7. Dieser entspricht der bisherigen Regelung in § 28 Absatz 3. Das heißt, Erkenntnisse aus dem Kernbereich privater Lebensgestaltung dürfen nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsache der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des zweiten Kalenderjahres, das dem Jahr der Dokumentation folgt.

Zu Nummer 16

Mit diesen Änderungen werden die Vorgaben des Bundesverfassungsgerichtes aus dem Beschluss vom 9. Dezember 2022 (1 BvR 1345/21) zum Kernbereichsschutz beim Einsatz verdeckter Ermittler umgesetzt. Hinsichtlich der näheren Begründung wird auf die Ausführungen zu § 28 Absatz 3 PolDVG-E verwiesen, die hier jeweils entsprechend gelten.

Zu Nummer 17

Mit dem textlichen Einschub in Absatz 1 Satz 1, wonach die Anlegung und Wartung des technischen Mittels zu dulden ist, wird eine sprachliche Klarstellung vorgenommen.

Am Beispiel von § 34 c Absatz 2 Nummer 2 PolG NRW wird mit der neuen Nummer 4 in Absatz 1 Satz 1 eine weitere Tatbestandsvariante eingefügt. Danach darf die Polizei eine Person zum Tragen einer elektronischen Aufenthaltsüberwachung verpflichten, wenn die Person, der gegenüber die Anordnung getroffen werden soll, nach polizeilichen Erkenntnissen bereits eine Straftat nach § 238 Absatz 1 Nummer 1 des Strafgesetzbuchs begangen hat und bestimmte Tatsachen die Annahme rechtfertigen, dass sie erneut eine Straftat nach § 238 Absatz 1 Nummer 1 des Strafgesetzbuchs begehen wird. Nach § 238 Absatz 1 Nummer 1 Strafgesetzbuch macht sich strafbar, wer einer anderen Person in einer Weise unbefugt nachstellt, die geeignet ist, deren Lebensgestaltung nicht unerheblich zu beeinträchtigen, indem er wiederholt die räumliche Nähe dieser Person aufsucht. Einer vorherigen strafrechtlichen Verurteilung als tatbestandliche Voraussetzung für die Anordnung bedarf es nicht, da das Abwarten zum Ausgang eines strafrechtlichen Ermittlungsverfahrens unter Umständen mit der Begehung weiterer entsprechender Straftaten einhergeht. Dies kann in Betracht kommen, wenn die konkreten Umstände des Falles und die vorliegenden Erkenntnisse über die beteiligten Personen zu der begründeten Annahme führen, dass trotz anderweitig getroffener Maßnahmen die Gefahr fortbesteht. Diese Annahme kann sich zum Beispiel ergeben, wenn andere gefahrenabwehrende Maßnahmen, wie ein Wohnungsverweis, Rückkehr- bzw. Annäherungsverbot oder eine temporäre Ingewahrsamnahme nicht zum Erfolg geführt haben. Dies gilt insbesondere dann, wenn die Behörden zuvor eine – erfolglose – Gefährderansprache gegenüber der betreffenden Person durchgeführt haben.

Der neu gefasste Absatz 4 Satz 1 erklärt die Anordnung für sofort vollziehbar.

Zu Nummer 18

Die Einschränkung im Tatbestand dient der Umsetzung des Beschlusses des Bundesverfassungsgerichtes vom 9. Dezember 2022 (1 BvR 1345/21) zum Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommerns (SOG MV). § 31 Absatz 1 PolDVG regelt die sog. polizeiliche Beobachtung. Diese ist nach § 31 Absatz 1 PolDVG bei Vorliegen weiterer Voraussetzungen zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung zulässig. Die vorbeugende Bekämpfung von Straftaten umfasst nach § 1 Absatz 1 PolDVG die Verhütung von Straftaten und die Vorsorge für die Verfolgung künftiger Straftaten.

Zu § 35 Absatz 1 SOG MV (Ausschreibung zur polizeilichen Beobachtung) hat das Bundesverfassungsgericht mit Beschluss vom 9. Dezember 2022 entschieden, dass dieser mangels Gesetzgebungskompetenz des Landesgesetzgebers formell verfassungswidrig ist, soweit § 35 Absatz 1 Satz 1 Alternative 2 in Verbindung mit § 7 Absatz 1 Nummer 4 SOG MV die Vorsorge für die Verfolgung künftiger Straftaten umfasst. Dem Land fehlt die Gesetzgebungskompetenz für eine Regelung, welche die Polizei zur Vorsorge für die Verfolgung künftiger Straftaten zur Ausschreibung zur polizeilichen Beobachtung ermächtigt, weil der Bund insoweit mit § 163e StPO von seiner konkurrierenden Gesetzgebungskompetenz abschließend Gebrauch gemacht hat.

Da auch § 31 Absatz 1 iVm § 1 Absatz 1 Nummer 1 PolDVG die Ausschreibung zu polizeilichen Beobachtung zur Vorsorge für die Verfolgung künftiger Straftaten erlaubt, besteht mithin Anpassungsbedarf.

Schließlich erfolgt mit dem neuen Satz 2 eine weitere Umsetzung der Entscheidung des Bundesverfassungsgerichtes statt BVerfG vom 9. Dezember 2023 (vgl. BVerfG, a.a.O., Rn. 95). Handelt es sich bei der in Bezug genommenen Straftat in Satz 1 Nummer 1 oder 2 um eine sog. Vorfeldstraftat ist die Maßnahme nur zulässig, wenn eine konkrete oder konkretisierte Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt. Die Vorfeldstraftat im Sinne dieses Gesetzes wird im neuen § 2 Absatz 24 definiert.

Zu Nummer 19

In § 34 PolDVG wird u.a. der Grundsatz der hypothetischen Datenneuerhebung aus dem Urteil des Bundesverfassungsgerichtes vom 20. April 2016 eingeführt.

Zu Absatz 1:

Das Bundesverfassungsgericht hat in seinem Urteil festgestellt, dass sich die Anforderungen an die Nutzung und Übermittlung staatlich erhobener Daten nach den Grundsätzen der Zweckbindung und Zweckänderung und sich die Reichweite der Zweckbindung nach der jeweiligen Ermächtigung für die Datenerhebung richten.

Im Urteil vom 20. April 2016 (BVerfGE 141, 220 Rn. 278 f., 282) heißt es: „Der Gesetzgeber kann eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus als weitere Nutzung im Rahmen der ursprünglichen Zwecke dieser Daten erlauben. Er kann sich insoweit auf die der Datenerhebung zugrundeliegenden Rechtfertigungsgründe stützen und unterliegt damit nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung. Die zulässige Reichweite solcher Nutzungen richtet sich nach der Ermächtigung für die Datenerhebung. Die jeweilige Eingriffsgrundlage bestimmt Behörde, Zweck und Bedingungen der Datenerhebung und definiert damit die erlaubte Verwendung. Die Zweckbindung der auf ihrer Grundlage gewonnenen Informationen beschränkt sich folglich nicht allein auf eine Bindung an bestimmte, abstrakt definierte Behördenaufgaben, sondern bestimmt sich nach der Reichweite der Erhebungszwecke in der für die jeweilige Datenerhebung maßgeblichen Ermächtigungsgrundlage. Eine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung kommt damit nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich.

(...) Folglich widerspricht es nicht von vornherein dem Gebot einer dem ursprünglichen Erhebungszweck entsprechenden Verwendung, wenn die weitere Nutzung solcher Daten bei Wahrnehmung derselben Aufgabe auch unabhängig von weiteren gesetzlichen Voraussetzungen als bloßer Spurenansatz erlaubt wird. Die Behörde kann die insoweit gewonnenen Kenntnisse zum Schutz derselben Rechtsgüter und im Rahmen derselben Aufgabenstellung – allein oder in Verbindung mit anderen ihr zur Verfügung stehenden Informationen – als schlichten Ausgangspunkt für weitere Ermittlungen nutzen. (…) Für die Wahrung der Zweckbindung kommt es demnach darauf an, dass die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt.“

Absatz 1 Satz 1 stellt klar, dass die Verarbeitung von personenbezogenen Daten zur Erfüllung derselben Aufgabe und zum Schutz derselben Rechtsgüter oder zur Verfolgung oder Verhütung derselben Straftat durch die Polizei nicht den Anforderungen an eine Zweckänderung unterliegt. Die Fassung des Absatzes 1 Satz 1 lehnt sich an § 12 BKAG an. Geregelt wird damit die Weiterverarbeitung von Daten, die von der Polizei erhoben wurden und auch von dieser weiterverarbeitet werden.

Satz 1 regelt damit die Weiterverarbeitung nicht nur im Rahmen der dem Einzelfall für die Datenerhebung maßgeblichen Gefahrenlage, sondern auch, soweit die zuständige Behörde im Rahmen der Erfüllung derselben Aufgabe zur Bewältigung anderer Gefahrenlagen handelt. Erforderlich aber auch ausreichend ist dann nur, dass es um den Schutz derselben Rechtsgüter oder um die Verhütung derselben Straftaten geht, wobei sich die Identität von Rechtsgütern oder Straftaten nicht auf den ursprünglichen Erhebungsanlass bezieht, sondern auf die Schutzzweck der Datenerhebungsnorm. Die Weiterverarbeitung kann also dem Schutz derjenigen Rechtsgüter oder der Verhütung derjenigen Straftaten dienen, um deren Schutz oder Verhütung es in der Rechtsgrundlage geht, auf die die Datenerhebung gestützt wird. (Vgl. BVerfG, a.a.O., Rn. 281). Nicht erforderlich ist eine bestimmte Gefahrenlage. Das Bundesverfassungsgericht (a.a.O., Rn. 280) führt insoweit aus: „Nicht zu den Zweckbindungen, die für jede weitere Nutzung der Daten seitens derselben Behörde je neu beachtet werden müssen, gehören grundsätzlich die für die Datenerhebung maßgeblichen Anforderungen an Einschreitschwellen, wie sie traditionell die hinreichend konkretisierte Gefahrenlage im Bereich der Gefahrenabwehr und der hinreichende Tatverdacht im Bereich der Strafverfolgung darstellen.

Das Erfordernis einer hinreichend konkretisierten Gefahrenlage oder eines qualifizierten Tatverdachts bestimmt den Anlass, aus dem entsprechende Daten erhoben werden dürfen, nicht aber die erlaubten Zwecke, für die die Daten der Behörde dann zur Nutzung offen stehen."

Satz 2 entspricht dem bisherigen Satz 2 von §34 Absatz 1. Wie schon zu den in §34 Absatz 1 Satz 2 genannten Zwecken, die überwiegend der Aufsicht, Kontrolle oder Datenschutzüberwachung dienen, wird mit dem neuen Satz 3 klargestellt, dass auch die Verarbeitung personenbezogener Daten zu Aus- und Fortbildungszwecken keine Zweckänderung darstellt. Der unveränderte §37 PolDVG, der sich auf Artikel 4 Absatz 3 der DS-RL stützen kann, regelt die Voraussetzungen der Verarbeitung.

Eine dem Satz 3 entsprechende Regelung findet sich auch in §6 Absatz 1 Satz 2 Hamburgisches Datenschutzgesetz (HmbDSG) und §10 Absatz 1 Satz 2 Hamburgisches Gesetz zum Schutz personenbezogener Daten im Justizvollzug (HmbJVollzDSG).

Zu Absatz 2:

In Absatz 2 wird das vom Bundesverfassungsgericht entwickelte Kriterium der sog. hypothetischen Datenneuerhebung umgesetzt (siehe BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 u.a., juris Rn. 284 ff.). Auch diese Regelungen orientieren sich maßgeblich an den Formulierungen in §12 Bundeskriminalamtgesetz (BKAG). Zwar hatte das Bundesverfassungsgerichtsurteil zum BKAG die (besonders) eingriffsintensiven und verdeckten Maßnahmen des BKAG aF zum Gegenstand. Allerdings sind die Ausführungen des Bundesverfassungsgerichts zum Datenschutz und zur Frage, unter welchen Voraussetzungen Daten zu einem anderen Zweck weiterverarbeitet werden dürfen als zu dem, für den sie ursprünglich erhoben wurden, als allgemeiner Grundsatz zu verstehen. Daher werden in diesem Gesetzesentwurf diese Ausführungen des Bundesverfassungsgerichts als allgemeine Grundsätze ausgestaltet, die bei jeder Datenweiterverarbeitung der Polizei zu berücksichtigen sind, soweit gesetzlich nichts besonderes bestimmt ist. So erfolgte auch die Umsetzung im BKAG und der überwiegenden Anzahl der Bundesländer anhand der vom Bundesverfassungsgericht dargelegten Kriterien. Dies auch vor dem Hintergrund, dass auf Grund der erforderlichen engeren Zusammenarbeit zwischen den Gefahrenabwehrbehörden des Bundes und der Länder der zulässige Datenaustausch eine zunehmend wichtigere Bedeutung erlangt (vgl. §29 Absatz 3 und 4 des BKAG). Um daher auch in Zukunft zuverlässig Daten mit den Bundeskriminalamt und den Gefahrenabwehrbehörden anderer Länder austauschen zu können, orientiert sich der Gesetzentwurf, wie ausgeführt, an den nach den Vorgaben des Bundesverfassungsgerichtes überarbeiteten Regelungen des BKAG und den entsprechenden Regelungen in den Polizeigesetzen derjenigen Bundesländer, welche die hypothetische Datenneuerhebung bereits umgesetzt haben.

Der Begriff der Verarbeitung wird auch hier weiterhin in §2 Absatz 8 definiert und umfasst das Erheben, Erfassen aber auch die Übermittlung.

Zum Grundsatz der hypothetischen Datenneuerhebung hat das Bundesverfassungsgericht (BVerfG, a.a.O., Rn. 288f) ausgeführt:

„Voraussetzung für eine Zweckänderung ist danach aber jedenfalls, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (…) Nicht in jedem Fall identisch sind die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hingegen hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts. Die diesbezüglichen Anforderungen bestimmen unter Verhältnismäßigkeitsgesichtspunkten primär den Anlass nur unmittelbar für die Datenerhebung selbst, nicht aber auch für die weitere Nutzung der erhobenen Daten. Als neu zu rechtfertigender Eingriff bedarf aber auch die Ermächtigung zu einer Nutzung für andere Zwecke eines eigenen, hinreichend spezifischen Anlasses. Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend, ist insoweit, dass sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergibt.

Der Gesetzgeber kann danach – bezogen auf die Datennutzung von Sicherheitsbehörden – eine Zweckänderung von Daten grundsätzlich dann erlauben, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist."

Absatz 2 normiert diese verfassungsrechtlichen Vorgaben und erlaubt eine Verarbeitung personenbezogener Daten zu anderen als den ursprünglichen Zwecken, wenn mindestens vergleichbar gewichtige Straftaten oder Ordnungswidrigkeiten verhütet bzw. verfolgt oder mindestens vergleichbar gewichtige Rechtsgüter geschützt werden sollen und sich im Einzelfall konkrete Anhaltspunkte zur Verhütung solcher Straftaten oder Ordnungswidrigkeiten oder zur Abwehr von in einem übersehbaren Zeitraum drohenden

Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter erkennen lassen.

Nummer 1 regelt die Anforderungen an die Zwecke der Datenverarbeitung, d.h. an das Gewicht der zu schützenden Rechtsgüter oder der zu verhütenden Straftaten.

Mit der Formulierung „vergleichbar gewichtig“ werden keine gleichgewichtigen Zwecke vorausgesetzt, sondern die „Vergleichbarkeit“ folgt aus den jeweiligen Erhebungsschwellen. Dies wird durch die Formulierung „unter Berücksichtigung der jeweiligen Erhebungsschwellen“ im Gesetzestext zum Ausdruck gebracht. Damit wird verdeutlicht wird, dass sich eine Vergleichbarkeit nicht auf die im Einzelfall bei der Datenerhebung verfolgten Zwecken bezieht, sondern auf die Zwecke, die nach der Rechtsgrundlage für die Datenerhebung maßgeblich sein können. Wenn etwa bei einer Telekommunikationsüberwachung, die nach §23 PolDVG zur Abwehr einer Lebensgefahr erfolgte, Zufallserkenntnisse zu einem anderen Lebenssachverhalt mit Anhaltspunkten für eine Freiheitsgefahr anfallen, kann auch diese andere Gefahr mit diesem Spurenansatz weiter erforscht werden. Das Rechtsgut „Freiheit“ erscheint zwar gegenüber dem Rechtsgut „Leben“ nicht gleichgewichtig, es ist jedoch mit Blick auf die Erhebungsschwelle der Art der jeweiligen Maßnahme (hier nach §23 Absatz 1 PolDVG: Leib, Leben, Freiheit einer Person) vergleichbar gewichtig.

Insbesondere bei offenen Maßnahmen ist eine solche Betrachtungsweise unumgänglich, da hier auf Grund der regelmäßig niedrigeren Eingriffsschwellen kein Grund besteht, die Verwendung von etwa zum Schutz eines bedeutsamen bzw. hochwertigen Rechtsgutes (zB Leib oder Leben) durch eine offene Maßnahme erhobenen Daten auch für ein weniger bedeutsames Rechtsgut (z.B. Eigentum) auszuschließen. Unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift ist beispielsweise bei einer Befugnisnorm zur offenen Datenerhebung, die keine Beschränkung auf bestimmte Rechtsgüter enthält, jedes Rechtsgut vergleichbar bedeutsam, sodass entsprechend erhobene Daten beim Vorliegen der übrigen Voraussetzungen des Satzes 1 weiterverarbeitet werden können.

Die in Absatz 2 Satz 1 Nummer 2 verwendete Formulierung „in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter“ erfordert, dass sich etwa eine Gefahr für mindestens vergleichbar bedeutsame Rechtsgüter, zu deren Schutz die ursprüngliche Datenerhebung vorgenommen wurde, nicht nur abstrakt, sondern in vielmehr als eine in ersten Umrissen absehbare und konkretisierte Möglichkeit eines Schadenseintritts für ein solches Rechtsgut darstellt.

Der letzte Halbsatz „soweit Rechtvorschriften dieses Gesetzes oder andere Rechtsvorschriften die zweckändernde Weiterverarbeitung nicht besonders regeln“, dient dem Ausschluss von Gesetzeskonkurrenzen. Bedeutsam kann dies etwa im Bereich der Strafprozessordnung sein. Wenn also personenbezogene Daten, die im Rahmen der Gefahrenabwehr erhoben wurden, als Beweis im Strafverfahren genutzt werden sollen (vgl. §100e Absatz 6 Nummer 3 StPO, dessen Regelungsgehalt in Absatz 3 Satz 2 auch explizit zum Ausdruck kommt). Daneben gibt es auch innerhalb dieses Gesetzes Rechtsvorschriften, wie zum Beispiel §51 PolDVG, welche die zweckändernde Weiterverarbeitung besonders regeln.

Der Satz 2 regelt, dass die strengen Vorgaben der Zweckbindung und der Grundsatz der hypothetischen Datenneuerhebung nicht gelten, wenn die vorhandenen der Identifizierung dienenden Daten einer Person (sog. Grunddaten) zu Identifizierungszwecken verwendet werden sollen. Dies ist nicht gleichzusetzen mit der polizeilichen Maßnahme einer Identitätsfeststellung im Sinne von §13 Absatz 1 PolDVG. Die Grunddaten dürfen herangezogen werden, um zu prüfen, ob die betroffene Person im Informationssystem bereits bekannt ist, um so ihre Identität zweifelsfrei festzustellen. Die zweifelsfreie Klärung der Identität einer Person ist notwendig, um Identitätsverwechslungen auszuschließen und damit zu verhindern, dass Eingriffe in die Grundrechte von unbeteiligten Personen stattfinden.

Zu Absatz 3:

Bei Daten aus Wohnraumüberwachungen reicht die Zweckbindung allerdings weiter. Dies wird durch Absatz 3 berücksichtigt, der den besonderen Anforderungen des Bundesverfassungsgerichts an die Zweckbindung für Daten aus Maßnahmen durch den Einsatz besonderer Mittel und Methoden in oder aus Wohnungen Rechnung (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 u.a., juris Rn. 291). Auf Grund des besonderen Eingriffsgewichts solcher Datenerhebungen gilt hier eine besonders enge Bindung der weiteren Nutzung der bei diesen Maßnahmen gewonnenen Daten an die Voraussetzungen und Zwecke der Datenerhebung (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 u.a., juris Rn. 283). Für die Verarbeitung von personenbezogenen Daten, die aus Maßnahmen durch den Einsatz besonderer Mittel und Methoden in oder aus Wohnungen nach §22 Absatz 1 erlangt wurden, sieht Absatz 3 daher vor, dass eine dringende Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person vorliegen muss.

In Satz 2 wird der Regelungsgehalt von §100e Absatz 6 Nummer 3 StPO, der insoweit auch eine andere Rechtsvorschrift ist, welche die zweck-

ändernde Weiterverarbeitung besonders regelt (vgl. § 34 Absatz 2 Satz 1 am Ende PolDVG-E), aus Klarstellungsgründen ausdrücklich wiedergegeben.

Satz 3 ist eine Übernahme von § 22 Absatz 6 S. 2, 2. Halbsatz, wonach eine zweckändernde Verarbeitung von durch eine Maßnahme nach § 22 erlangten Daten zu dokumentieren ist.

Die Regelung an dieser Stelle führt zu einer Folgeänderung in § 22 Absatz 6.

Der neue Satz 4 untersagt, dass Erkenntnisse aus optischen Wohnraumüberwachungen zu Strafverfolgungszwecken verwertet werden dürfen. Hintergrund ist, dass zur Verfolgung von Straftaten nach Artikel 13 Absatz 3 GG nur eine akustische Wohnraumüberwachung eingesetzt werden darf. Diese Beschränkung darf nicht durch eine Verwendung von Daten aus einer präventiv angeordneten optischen Wohnraumüberwachung unterlaufen werden (vgl. BVerfGE 141, 220, 317). Satz 4 dient damit der Umsetzung der Vorgaben des Bundesverfassungsgerichtes zum Verbot der Verwendung von personenbezogenen Daten aus der optischen Wohnraumüberwachung für die Strafverfolgung.

Zu Absatz 4:

Der bisheriger Absatz 2 wird Absatz 4 und bleibt bis auf die Einfügung des Wortes „auch“ im Wesentlichen unverändert. Das Wort „auch“ verdeutlicht, dass dies neben Absatz 2 eine weitere Regelung zur Zweckänderung ist. Anders als bei Absatz 2 kommt es hier nicht auf die Berücksichtigung der jeweiligen Erhebungsschwellen an. Absatz 4 normiert, wie bisher auch der Absatz 2, die Zulässigkeit einer zweckändernden Datenverarbeitung nach Maßgabe der dort genannten Voraussetzungen bzw. Sachverhaltskonstellationen.

Die zulässige Zweckänderung „zur Verfolgung von Straftaten und Ordnungswidrigkeiten“ geht in Absatz 2 auf und wird daher in Nummer 3 gestrichen.

Zu Absatz 5:

Der bisherige Absatz 3 zu personenbezogenen Daten, die einem Berufsgeheimnis unterliegen wird inhaltlich unverändert Absatz 5.

Zu Absatz 6:

In Absatz 6 wird neu die Verpflichtung zur Sicherstellung der Beachtung der Absätze 1 bis 3 und 5 durch organisatorische und technische Maßnahmen nach dem Vorbild des § 12 Absatz 5 BKAG normiert, um die Einhaltung der Grundsätze der hypothetischen Datenneuerhebung in polizeilichen Datei- und Informationssystemen zu gewährleisten. Diese Verpflichtung wird in speziellen Regelungen zur Kennzeichnung (§ 65 PolDVG) und Zugriffsberechtigung (§ 54 PolDVG) näher ausgestaltet. Absatz 4 wird in der Aufzählung nicht genannt, da dort gerade nicht die hypothetische Datenneuerhebung geregelt ist.

Zu Absatz 7:

Der bisherige Absatz 4 Satz 1, der bestimmt, dass Daten, die mit besonderen Mitteln nach den §§ 20 bis 31 sowie nach § 50 erhoben wurden, für andere Verfahren nur verarbeitet werden dürfen, wenn sie auch dafür unter Einsatz dieser Befugnisse hätten erhoben werden dürfen, ist mit der Regelung der hypothetischen Datenneuerhebung obsolet. Erforderlich für die Nutzung der Daten in einem anderen Verfahren ist bisher, dass alle Voraussetzung der Rechtsgrundlage vorliegen müssen, also so, als wenn die Daten erstmals neu erhoben werden müssten. Diese strengen Vorgaben werden mit der Einführung der hypothetischen Datenneuerhebung abgelöst, weswegen der Satz 1 zu streichen ist.

Der bisherige Satz 2 ist infolge der Streichung von Satz 1 redaktionell anzupassen.

Zu Absatz 8 bis 10:

Die bisherigen Absätze 6 bis 8 werden inhaltlich unverändert Absätze 8 bis 10.

Zu Nummer 20

§ 36 Absatz 2 erfährt durch die Bezugnahme auf die § 34 Absätze 2 und 3 in Satz 1 und die Streichung von Satz 2 eine Anpassung im Hinblick auf die Einführung der hypothetischen Datenneuerhebung. Auf den bisherigen Satz 2, der als Voraussetzung für die Verwendung der Daten fordert, dass mittels spezieller Erhebungsmethoden nach der StPO erlangte Daten, die denjenigen in den §§ 20 bis 31 und § 51 PolDVG genannten Befugnissen entsprechen nur dann verarbeiten werden dürfen, wenn man diese Methoden auch bei der Datenerhebung bei der Gefahrenabwehr hätte einsetzen dürfen, wird infolgedessen verzichtet. In Satz 1 wird insoweit klargestellt, dass sich diese Weiterverarbeitung nach § 34 Absätze 2 und 3 richtet. Bei der Verwendung von repressiv erhobenen Daten zu präventiven Zwecken gilt zunächst, wie bisher auch, dass mögliche Verwendungsregelungen der Strafprozessordnung zu beachten sind (zB § 100e Absatz 6 Nummer 2 StPO) und im Anschluss die Vorschriften zur zweckändernden Weiterverarbeitung in den Polizeigesetzen anzuwenden sind (vgl. § 481 StPO).

Zu Nummer 21

In Absatz 1 wird der Grundsatz der hypothetischen Datenneuerhebung sowohl allgemein als auch im Hinblick auf die Datenübermittlungen nach §§ 39 bis 46 umgesetzt. Über die Bezugnahme auf § 34 gilt, dass bei Datenübermittlungen die Vorgaben des § 34 bzw. der Grundsatz der hypothetischen Datenneuerhebung

zu berücksichtigen ist. Andere gesetzliche Regelungen, die eine Datenübermittlung erlauben, bleiben auch weiterhin unberührt („soweit gesetzlich nichts anderes bestimmt ist"). Satz 2 verdeutlicht, dass bei Datenübermittlungen nach den § 39 bis 46 die Vorgaben des § 34 ebenso zu berücksichtigen sind, diese also nicht für sich eine andere gesetzliche Bestimmung im Sinne des Satzes 1 sind.

Zu Nummer 22

Wie schon bei der Streichung der vormaligen § 21 Absatz 1 Nummer 3 PolDVG aF (vgl. 21/17906, S. 70), wonach die Polizei personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln durfte, soweit der Auskunftsbegehrende ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und die schutzwürdigen Interessen des Betroffenen nicht überwiegen, wird auch hier angenommen, dass diese Regelung in den Anwendungsbereich der Verordnung (EU) 2016/679 (DSG-VO) fällt, deren Rechtfertigungstatbestand für die Datenverarbeitung in diesem Falle Artikel 6 Absatz 1 lit. f DSG-VO ist. Die Verarbeitung ist danach rechtmäßig, wenn dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. In der polizeilichen Praxis fallen hierunter häufig Anträge außerhalb des § 69 PolDVG auf Akteneinsicht in bzw. Auskunftserteilung aus polizeilichen Vorgängen.

Die Datenverarbeitung nach der DSG-VO ist eine solche im Sinne des § 34 Absatz 4 Nummer 1 PolDVG-E, der dem bisherigen § 34 Absatz 2 Nummer 1 PolDVG entspricht. Die Zweckänderung ist daher zulässig. Die Zulässigkeit einer Übermittlung auch für Zwecke außerhalb des Anwendungsbereichs der Richtlinie (EU) 2016/680 ergibt sich aus Artikel 9 Absatz 1 der Richtlinie (EU) 2016/680. Nach Artikel 9 Absatz 2 Satz 2 der Richtlinie (EU) 2016/680 gilt für die Verarbeitung für Zwecke, die vom Anwendungsbereich der Verordnung (EU) 2016/679 erfasst ist, das Recht dieser Verordnung (vgl. ebenso § 10 Absatz 3 Nummer 1 HmbJVollzDSG). In § 1 Absatz 3 PolDVG findet sich im Übrigen die Feststellung, dass die DSG-VO sowie das HmbDSG in der jeweils geltenden Fassung unmittelbar gelten (vgl. zur Abgrenzung der jeweiligen Anwendungsbereiche auch Drucksache 21/17906, S. 43f).

Zu Nummer 23

Der neu eingefügte § 47a sieht in Absatz 1 die Übermittlung von Kontaktdaten von Personen, die häusliche Gewalt ausüben, an geeignete Beratungsstellen durch die Polizei vor. Häusliche Gewalt in diesem Sinne beinhaltet alle Formen körperlicher, sexueller oder psychischer Gewalt und umfasst familiäre sowie partnerschaftliche Gewalt. Häusliche Gewalt liegt vor, wenn die Gewalt zwischen Personen stattfindet, die in einer familiären oder partnerschaftlichen Beziehung zusammenwohnen. Sie liegt auch vor, wenn sie unabhängig von einem gemeinsamen Haushalt innerhalb der Familie oder in aktuellen oder ehemaligen Partnerschaften geschieht (vgl. die Definition Häusliche Gewalt, Bundeslagebild 2022, BKA, S. 1).

Die Regelung soll eine wirksame Intervention in Fällen häuslicher Gewalt ermöglichen, um Gewaltkreisläufe zu durchbrechen. Täter und Täterinnen sollen lernen, für ihr Verhalten Verantwortung zu übernehmen, sich besser zu kontrollieren und mit Beziehungskonflikten gewaltfrei umzugehen. Gewaltausübenden Menschen sollen Wege aus der Gewalttätigkeit aufgezeigt werden.

An die entsprechende Fachstabsstelle im Landeskriminalamt, die als solche für Grundsatzfragen der polizeilichen Intervention bei Beziehungsgewalt und in dieser Funktion unter anderem auch Ansprechstelle für andere Behörden und nichtbehördliche Organisationen ist, ist von verschiedenen Seiten vermehrt der Wunsch herangetragen worden, auch in Hamburg einen proaktiven Ansatz in Bezug auf die gewaltausübenden Personen bei Beziehungsgewalt zu etablieren, damit diesen – nach einem erfolgten Polizeieinsatz – von einer Täterberatungsstelle proaktiv ein Hilfe- und Beratungsangebot gemacht werden kann.

Bislang werden zumindest die Daten von Opfern mit deren Einwilligung an eine Interventionsstelle weitergeleitet, damit von dort aus proaktiv mit den Geschädigten Kontakt zum Zweck der Beratung aufgenommen werden kann. Nach Einschätzung der Polizei dürfte sich ein proaktiver Ansatz auch bezüglich des Gewaltausübenden positiv auf die gewaltbelastete Beziehung auswirken. Im Idealfall würden weitere Gewalttaten verhindert werden. Insofern ist dies als eine Maßnahme der Gefahrenabwehr und des Opferschutzes anzusehen. Zudem hat sich der in Hamburg seit langem etablierte proaktive Ansatz in Bezug auf die gewaltbetroffenen Personen bewährt und wird von den beteiligten Stellen genauso wie von den gewaltbetroffenen Personen als zielführende Maßnahme eines aktiven Opferschutzes angesehen. Hieran wird festgehalten.

Die Norm erlaubt der Polizei vor diesem Hintergrund, die Übermittlung personenbezogener Daten betroffener Personen, die Gewalt ausüben, an eine von der für Soziales zuständigen Behörde bestimmte Beratungsstelle. Hierbei kann es sich um eine öffentliche oder um eine nicht-öffentliche Stelle handeln. Die

für Soziales zuständige Behörde hat zuvor die Eignung der Beratungsstelle geprüft und teilt das Ergebnis der Polizei mit. Die für Soziales zuständige Behörde kann hierbei mehrere Beratungsstellen für unterschiedliche sachliche Anwendungsbereiche und Orte empfehlen. Die Polizei darf die Übermittlung der Kontaktdaten nur an für geeignet befundene Beratungsstellen übermitteln. Die Eignung wird von dieser Stelle jeweils bis auf Weiteres, d.h. bis zur Aufhebung der Eignungsentscheidung, festgestellt.

Absatz 2 regelt in Anlehnung an Absatz 1 die Datenübermittlung seitens der Polizei zum Zwecke der Distanzierungs- und Ausstiegsberatung etwa aus Gruppen im Bereich des Rechtsextremismus, des religiös begründeten Extremismus oder anderer Organisationsstrukturen, ihre Mitglieder in Abhängigkeiten halten. Tatsächliche Anhaltspunkte sind Erkenntnisse, die eine entsprechende polizeiliche Prognose tragen können und die von reinen Spekulationen, hypothetischen Erwägungen, fallunabhängigen Vermutungen sowie allgemeinen Erfahrungssätze als Grundlage einer Prognose und von einem Handeln ins Blaue hinein abzugrenzen sind. Anhaltspunkte können aus polizeilichen oder staatsanwaltschaftlichen Ermittlungen stammen oder auch auf Hinweisen Dritter basieren.

Die Ausgestaltung der Datenweitergabe und damit zusammenhängenden Kontaktaufnahme wird in einer noch auszugestaltenden Kooperationserklärung zwischen der für Inneres zuständigen Behörde/Polizei, der für Soziales zuständigen Behörde und gegebenenfalls den Beratungsstellen erarbeitet, um Inhalt und Verfahren der Datenweitergabe und Kontaktaufnahme zu bestimmen. Durch diese Kooperationserklärung wird sichergestellt, dass bereits bestehende Strukturen genutzt und die Bedürfnisse aller Beteiligten, wie etwaige Sicherheitsinteressen der Beratungsstellen, Berücksichtigung finden.

Die geeigneten Beratungsstellen werden von der für Soziales zuständigen Behörde bestimmt. Nach §47a Absatz 2 Satz 3 PolDVG gilt Absatz 1 Sätze 2 und 3 entsprechend. Danach protokolliert die Polizei die Datenübermittlung und die Beratungsstelle darf die Daten nur einmalig dazu nutzen, den betroffenen Personen die entsprechenden Unterstützungsangebote anzubieten.

Zu Nummer 24

Nachdem das Bundesverfassungsgericht mit Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – die Bestimmung des §49 Absatz 1 Alternative 1 PolDVG teilweise für verfassungswidrig erklärt hat, besteht die Notwendigkeit einer Neuregelung. Dies gilt insbesondere für eine Datenanalyse bereits im Gefahrenvorfeld (BVerfG, a.a.O., Rn. 153 ff.). Abhängig vom Eingriffsgewicht dieser Maßnahme (BVerfG, a.a.O., Rn. 75 ff.) können sich unterschiedliche Anforderungen sowohl an ihren Anlass als auch ihr Ziel ergeben (BVerfG, a. a. O, Rn. 103 ff.), sofern eine Maßnahme nicht bereits durch die Grundsätze der Zweckbindung und Zweckänderung gerechtfertigt ist (BVerfG, a.a.O., Rn. 55 ff.).

Das Bundesverfassungsgericht hat in seinem Urteil bestätigt, dass die Bestimmung des §49 PolDVG, ebenso wie §25a HSOG, dem legitimen Zweck dient, vor dem Hintergrund informationstechnischer Entwicklungen die Wirksamkeit der vorbeugenden Bekämpfung schwerer Straftaten zu steigern, indem Anhaltspunkte für bevorstehende schwere Straftaten gewonnen werden, die im Datenbestand der Polizei ansonsten unerkannt blieben. Auch sei die Regelung des §49 PolDVG zur Steigerung der Wirksamkeit der vorbeugenden Straftatenbekämpfung geeignet und erforderlich. Denn durch eine automatisierte Datenanalyse könnten für die Verhütung von Straftaten relevante Erkenntnisse erschlossen werden, die auf andere, grundrechtsschonendere Weise nicht gleichermaßen zu gewinnen wären (BVerfG, a.a.O., Rn. 52 f.). Allerdings ist die Regelung des §49 PolDVG derzeit nicht präzise genug gefasst, um die Verhältnismäßigkeit einer Datenanalyse in jedem Einzelfall sicherstellen zu können (BVerfG, a.a.O., Rn. 123 ff., 152 ff.). Dies soll mit der Neuregelung behoben werden.

Der Vorschlag ist angelehnt an den auf Grund der Entscheidung des Bundesverfassungsgerichtes geänderten §25a HSOG.

Absatz 1 Sätze 1 und 2 beschreiben im Sinne einer Legaldefinition das technische Verfahren einer automatisierten Datenanalyse. Es besteht aus zwei logisch aufeinander aufbauenden, aber praktisch zeitgleich stattfindenden Schritten, nämlich dem Zusammenführen unterschiedlicher „Datentöpfe“ auf der Analyseplattform und der sich daran anschließenden Recherche innerhalb des so zusammengeführten Datenbestands. Der erste Schritt überwindet das strukturelle Problem, dass in den Beständen der Polizei Daten in unterschiedlichen Formaten und disparaten Dateien gespeichert und damit nicht im selben Bearbeitungskontext gleichzeitig verfügbar sind, der zweite führt zu der verfassungsrechtlich relevanten Frage, was genau die Polizei mit den so zusammengeführten Daten machen darf und was nicht.

Die automatisierte Anwendung zur Datenanalyse ist ein technisches Hilfsmittel, das es den Polizeibehörden bei der Erfüllung ihrer Aufgaben nach Maßgabe des §49 PolDVG ermöglichen soll, ihre Bewertungen, Prognosen und Entscheidungen auf der Grundlage möglichst verlässlicher Tatsachenfeststellungen zu treffen.

Die Eigenschaft des Analysetools als ein vom Menschen hergestelltes und von ihm kontrolliertes Hilfsinstrument wird auch durch die Vorgabe des Satzes 4 abgesichert, wonach die automatisierte Datenanalyse manuell ausgelöst wird und weitere Verarbeitungsschritten von Menschen veranlasst werden oder von ihnen vorher festgelegt worden sind. Der Analysevorgang selbst besteht aus einer Reihe simultan ausgelöster und miteinander in Verbindung gesetzter, auf Wenn-Dann-Operatoren beruhender Suchaktionen über den zuvor zusammengeführten Datenbestand. Als regelbasierte oder, gleichbedeutend, deterministische (vgl. BVerfG, a.a.O., Rn. 101) Datenanalyse folgt sie einem klar definierten, unveränderlichen Ablauf und erzeugt deshalb auch konsistente und reproduzierbare Ergebnisse, die einer Gegenkontrolle leichter zugänglich sind als die Datenanalyse unter Einbeziehung selbstlernender Systeme. Die in Satz 3 skizierten Kriterien der Anlass-, Fall- und Zielbezogenheit als Voraussetzung für die Nutzung dieses Instruments stellen sicher, dass eine Analysesoftware nicht etwa ein wie immer geartetes Eigenleben oder gar eigene Gesetzmäßigkeiten entwickelt, sondern dass sie ein bloßes Hilfsinstrument bleibt.

In Absatz 2 werden zwei Tatbestandsalternativen für die Anwendung der automatisierten Datenanalyse geregelt. Absatz 2 Satz 1 Nummer 1 entspricht dem bisherigen §49 Absatz 1 Satz 1 2. Alternative. Dieser Anwendungsfall war nicht Gegenstand der Entscheidung des Bundesverfassungsgerichtes vom 16. Februar 2023. Wie schon bisher ist hier Voraussetzung, dass eine konkrete Gefahr für die in Nummer 1 genannten besonders gewichtigen Rechtsgüter vorliegt.

Absatz 2 Satz 1 Nummer 2 setzt tatsächliche Anhaltspunkte voraus, die die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten im Sinne des §100b Absatz 2 der Strafprozessordnung begangen werden sollen und dies zur Verhütung bzw. Verhinderung dieser Straftaten erforderlich ist. Tatsächliche Anhaltspunkte sind Erkenntnisse, die eine polizeiliche Prognose tragen können und die von reinen Spekulationen, hypothetischen Erwägungen, fallunabhängigen Vermutungen sowie allgemeinen Erfahrungssätze als Grundlage einer Prognose und von einem Handeln ins Blaue hinein abzugrenzen sind. Diese Erkenntnisse müssen sich auf die Begehung von Straftaten im Sinne des §100b Absatz 2 der Strafprozessordnung beziehen, also besonders schwere Straftaten. Gegengewicht zur Eingriffsschwelle unter das Maß der konkretisierten Gefahr ist hier die Beschränkung des Maßnahmezwecks auf den Schutz besonders gewichtiger Rechtsgüter, wie sie auch in der insoweit zulässigen Bezugnahme auf einen Straftatenkatalog zum Ausdruck kommen kann. Anknüpfungspunkt sind die in §100b Absatz 2 StPO genannten schweren Straftaten, welche als Äquivalent zur Benennung besonders gewichtiger, zu schützender Rechtsgüter in jedem Fall geeignet sind. Das eine Anknüpfung an den Straftatenkatalog des §100b Absatz 2 Strafprozessordnung unter bestimmten Einschränkungen geeignet ist, hat das Bundesverfassungsgericht in den Übergangsbestimmungen bereits deutlich gemacht (BVerfG, a.a.O., Rn. 176). Und die Erkenntnisse müssen, bezogen auf die Straftat, ein zumindest ihrer Art nach konkretisiertes Geschehen erkennen lassen. Die Eingriffsschwelle wurde im Vergleich zur bisherigen Norm insoweit angehoben.

Räumt der Gesetzgeber diese Art der Befugnis im Vorfeld einer konkretisierten Gefahr ein, hier zur Verhütung von Straftaten, muss er zur Wahrung der Verhältnismäßigkeit die Eingriffsintensität der Maßnahme reduzieren (vgl. BVerfG, a.a.O., Rn. 112). Die Begrenzung von Art und Umfang der Daten (vgl. Absatz 2 Satz 3, Satz 7), der Verarbeitungsmethoden (vgl. Absatz 1 Satz 2, 3, Absatz 2 Satz 5) sowie der Verpflichtung technisch-organisatorische Maßnahmen (vgl. Absatz 3, Absatz 4) vorzusehen, die ohnehin für die Nummer 1 und Nummer 2 von Absatz 2 gelten, werden für die Nummer 2 noch dahingehend gesetzgeberisch begrenzt, dass gemäß Absatz 2 Satz 6 Verkehrsdaten nicht automatisiert in die Analyse einbezogen werden dürfen.

Schließlich wird mit Absatz 2 Satz 2 eine weitere Einschränkung im Hinblick auf sog. Vorfeldstraftaten bestimmt. Handelt es sich bei der in Bezug genommenen Straftat in Satz 1 Nummer 2 um eine Vorfeldstraftat ist die Maßnahme nur zulässig, wenn eine konkrete oder konkretisierte Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt (vgl. BVerfG, Beschluss vom 9. Dezember 2023, Rn. 95). Die Vorfeldstraftat im Sinne dieses Gesetzes wird im neuen §2 Absatz 24 definiert.

In Absatz 2 Satz 3 werden die für die automatisierte Anwendung zur Datenanalyse verwendbaren Datenquellen festgelegt.

Vorgangsdaten ergeben sich aus der Vorgangsverwaltung, die mittels Vorgangsbearbeitungssystemen erfasst und mittels Vorgangsverwaltungssystemen dokumentiert und verwaltet werden. Dies sind EDV-gestützte Anzeigenaufnahme- und Vorgangsverwaltungsprogramme zur Bewältigung des alltäglichen Dienstgeschäftes. Ziel der Vorgangsverwaltung und -bearbeitung ist es, die bei einer Dienststelle anfallenden Informationen, wie etwa Vermerke, Anfragen, Anzeigen, in geordneter Form zu erfassen und aufzubewahren und ein Wiederauffinden zu ermöglichen. Ein „Vorgang“ umfasst dabei sämtliche Unterlagen, die im Zusammenhang einer polizeilichen Tätigkeit über eine bestimmte Person, Sache oder sonstigen Gegenstand polizeilichen Handelns geführt werden vgl. (Lis-

ken/Denninger PolR-HdB, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht Rn. 832, beck-online). Das aktuell von der Hamburger Polizei verwendete Vorgangsbearbeitungssystem heißt ComVor. Das entsprechende Vorgangsverwaltungssystem ist der ComVor-Index.

Falldaten ergeben sich aus Fallbearbeitungssystemen. Dabei handelt es sich um Verfahren zur strukturierten Bearbeitung von umfangreichen Ermittlungsverfahren. Die Hamburger Polizei verwendet zur Fallbearbeitung aktuell eine Software namens Crime.

Polizeiliche Auskunftssysteme enthalten personenbezogene Informationen und bestehen aus unterschiedlichen Datengruppen. Das bei der Hamburger Polizei aktuell verwendete Auskunftssystem heißt POLAS. Es dient dem Nachweis und der Auskunft über Personen, die bspw. zur Fahndung ausgeschrieben sind, die einer erkennungsdienstlichen Behandlung unterzogen wurden, die inhaftiert sind bzw. waren oder über die eine Kriminalakte bei einer kriminalaktenführenden Dienststelle der Polizei geführt wird. Daneben enthalten polizeiliche Auskunftssysteme die zur Fahndung ausgeschrieben Fahrzeuge und sonstige Gegenstände mit alpha-nummerischer Kennzeichnung, nach denen gefahndet wird.

Die mit dem Begriff Verkehrsdaten erfassten polizeilichen Datenbestände enthalten personenbezogene Informationen, die auf strafprozessualer Grundlage (vgl. §100g StPO) oder auf Grund polizeirechtlicher Vorschriften (vgl. §25 PolDVG) erhoben wurden. Zu den in §3 Nr. 70 TKG definierten Verkehrsdaten – Daten, deren Erhebung, Verarbeitung oder Nutzung eines bei der Erbringung eines Telekommunikationsdienstes erforderlich sind – gehören auch die Standortdaten (vgl. §9 Absatz 1 Nummer 1 TTDSG), deren Erhebung auf der Grundlage von §25 Absatz 3 PolDVG ermöglicht wird (für den strafprozessualen Bereich vgl. gemäß §100g Absatz 3 StPO als Funkzellenabfrage bzw. gemäß §100i Absatz 1 Nummer 2 StPO).

Die mit dem Begriff Nutzungsdaten erfassten polizeilichen Datenbestände enthalten personenbezogene Informationen, die auf strafprozessualer Grundlage (vgl. §100k StPO) oder auf Grund polizeirechtlicher Vorschriften (vgl. §25 PolDVG) erhoben wurden. Nutzungsdaten sind personenbezogene Daten einer Nutzerin oder eines Nutzers von digitalen Diensten, die durch denjenigen, der geschäftsmäßig eigene oder fremde digitale Dienste zur Nutzung bereit hält oder den Zugang zur Nutzung vermittelt, erhoben werden, um die Inanspruchnahme von digitalen Diensten zu ermöglichen oder abzurechnen, insbesondere Merkmale zur Identifikation der Nutzerin oder des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen digitalen Dienste (vgl. §25 Absatz 6 PolDVG, §2 Absatz 2 Nummer 3 TDDDG)

Der Begriff Telekommunikationsdaten bezeichnet die gesondert gespeicherten Datenbestände, in denen Daten aus polizeilichen Telefonüberwachungsmaßnahmen gemäß §100a StPO und §23 PolDVG zusammengeführt werden.

Asservate im Sinne dieser Bestimmung sind amtlich in Verwahrung genommene und als Beweismittel in Frage kommende Gegenstände, soweit sie zur Aufbewahrung personenbezogener Daten dienende Daten aus Asservaten, wie bspw. USB-Sticks und Festplatten. Die hieraus gewonnenen Daten werden, nicht zuletzt, weil es sich um vergleichsweise unstrukturierte Daten handelt, in einem gesonderten Datentopf zusammengeführt.

Unter Daten aus dem polizeilichen Informationsaustausch ist das bundesweit webbasierte Fernschreibsystem EPOST810 zu verstehen.

Satz 4 regelt die der Einbeziehung von Daten aus staatlichen Registern in die automatisierte Datenanalyse. Daten aus staatlichen Registern sind beispielsweise Daten aus dem Melderegister, dem Zentralen Verkehrsinformationssystem (ZEVIS) oder dem Waffenregister, welche über die Analyseplattform auf direktem Weg abgefragt werden können, wenn dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. Die Regelung dient der Klarstellung. Die Befugnis zur Abfrage als solcher ergibt sich bereits aus den speziellen Übermittlungsregelungen (z.B. §34 Absatz 2 Nr. 1 BMG, §35 StVG, §§13 ff. WaffG). So können Abfragen in ZEVIS dazu dienen, sich über die Mobilität einer Anlassperson Klarheit zu verschaffen. Hat diese Person außerdem eine Waffenerlaubnis, kann darin ein gefahrerhöhendes Indiz gesehen werden. Die Funktionalität der Analyseplattform stellt sicher, dass solche Informationen schnell zusammengeführt und bewertet werden können.

Mit Blick auf die Regelung des Satzes 5, wonach eine Anbindung an das Internet ausgeschlossen ist, dient Absatz 2 Satz 4, wonach gesondert gespeicherte Datensätze aus Internetquellen in die automatisierte Datenanalyse einbezogen werden dürfen, der Klarstellung. Es handelt sich bei diesen Datensätzen vor allem um die Ergebnisse polizeilicher Recherchen in für jedermann offenen sozialen Netzwerken. Vorstellbar sind Fallkonstellationen, in denen auf sozialen Netzwerken ein Amoklauf angekündigt wird oder Verabredungen zu gemeinsamen Aktionen getroffen werden, die den Tatbestand des Landfriedensbruchs erfüllen würden.

Satz 5 enthält ein ausdrückliches und striktes Verbot der Anbindung des Analysetools an das Internet,

weil damit die automatisierte Verarbeitung einer unüberschaubar großen Zahl personenbezogener Daten Unbeteiligter verbunden wäre (vgl. BVerfG, a.a.O., Rn. 88). Auch dieses Verbot hat insofern programmatischen Charakter, als es sichtbar machen will, dass eine Analyseplattform die Nutzbarmachung lediglich der von der Polizei zulässigerweise gespeicherten Daten verbessern will. Erforderlichenfalls können aber die bei der Bearbeitung eines konkreten Fallkomplexes gezielt ermittelten und zuvor von den Polizeibehörden gespeicherten Daten, die bei einer Internetrecherche angefallen sind, in die automatisierte Datenanalyse einbezogen werden (vgl. Absatz 2 Satz 3).

Nach Satz 6 dürfen Verkehrsdaten nicht zur vorbeugenden Straftatenbekämpfung gemäß Absatz 1 Satz 1 Nummer 2 im Wege der automatisierten Datenanalyse weiterverarbeitet werden, d.h. sie dürfen bei einer Recherche auf der Grundlage dieser Tatbestandsvariante nicht zusammen mit den anderen Datenbeständen auf der Analyseplattform zusammengeführt werden. Bei Maßnahmen nach dieser Variante fällt die zeitliche Komponente im Verhältnis zur Grundrechtsrelevanz weniger ins Gewicht, weshalb Effektivitätseinbußen aus Gründen des hier im Vordergrund stehenden Schutzes Unbeteiligter – Verkehrsdaten enthalten typischerweise eine Vielzahl personenbezogener Daten von Personen, die keinen objektiv zurechenbaren Anlass für polizeiliche Ermittlungen geben (vgl. BVerfG, a.a.O., Rn. 77) – hinzunehmen sind.

Satz 7 von Absatz 2 regelt zur Verringerung der Eingriffsintensität der automatisierten Datenanalyse, dass die Weiterverarbeitung von personenbezogenen Daten, die aus Wohnraumüberwachungen oder Online-Durchsuchung gewonnenen Daten nicht in eine automatisierte Datenanalyse einbezogen werden dürfen (vgl. hierzu BVerfG, a.a.O., Rn. 81).

Um Unklarheiten vorzubeugen, erklärt Absatz 3 Satz 1 die Bestimmungen über die zweckwahrende und zweckändernde Weiternutzung personenbezogener Daten der Absätze 1 und 2 des §34 PolDVG ausdrücklich für anwendbar. Dies lässt, so das Bundesverfassungsgericht, bereits das Eingriffsgewicht von Maßnahmen nach §49 PolDVG sinken (vgl. BVerfG, a.a.O., Rn. 130).

Mit den Vorgaben zu Art und Umfang der Daten in Absatz 2 hat der Gesetzgeber dem Grunde nach auch schon in hinreichender Weise vorgeben, welche Datenbestände einbezogen werden dürfen. Dadurch hat er, entsprechend der Vorgaben des Bundesverfassungsgerichtes die Eingriffsintensität, insbesondere für den Anwendungsfall von Absatz 2 Nummer 3, weiter verringert.

Die Absätze 3 und 4 enthalten daneben zusätzliche technisch-organisatorische Vorgaben.

So wird in Absatz 3 Satz 2 festgelegt, dass ein Rollen- und Rechtekonzept sowie ein Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten zu erstellen ist. Gemäß Satz 3 regelt dieses die zweckabhängige Verteilung sachliche eingeschränkter Zugriffsrechte anhand von Phänomenbereichen. Das Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten regelt anhand der Maßstäbe des Veranlassungszusammenhangs und der Grundrechtsrelevanz, welche personenbezogenen Daten in welcher Weise in die automatisierte Analyse einbezogen werden dürfen. Hierfür hat der Gesetzgeber in Teilen schon Vorgaben gemacht (vgl. Absatz 2 sowie Absatz 3 Satz 4).

Ein Zusammenführen von Daten zieht keine Verlängerung der Speicherfristen in den Quellsystemen nach sich. Vielmehr kommt es zu einem Durchgreifen der allgemeinen Prüffristen und Löschungspflichten aus den jeweiligen Quellsystemen (vgl. §35, 59 PolDVG). Bereits auf der Ebene der Gesetzgebung verlangt das Bundesverfassungsgericht bei der Einbeziehung von Verkehrsdaten in den für die automatisierte Datenanalyse oder -auswertung bereitstehenden Datenpool, dass eine Höchstspeicherdauer zu regeln ist (vgl. BVerfG, a.a.O., Rn. 85). Daher legt Absatz 3 Satz 5 fest, dass für Verkehrsdaten eine Speicherfrist von regelmäßig zwei Jahren in der Analyseplattform vorzusehen ist. Vergleichbar mit der Aussonderungsprüffrist gemäß §35 Absatz 2 PolDVG steht sie allerdings unter dem Vorbehalt, dass die Daten nach Ablauf der Frist nicht zu löschen sind, wenn sie für die Fallbearbeitung ausnahmsweise noch erforderlich sind.

Absatz 4 enthält Regelungen zur Gewährleistung von Kontrolle und Transparenz (vgl. hierzu BVerfG, a.a.O., Rn. 109). Ein zentrales Element ist die Zugriffskontrolle. Die Zugriffe unterliegen zudem einer Protokollierung. Mit der Zugriffskontrolle wird gewährleistet, dass nur berechtigte – und damit auch entsprechend qualifizierte – Personen eine automatisierte Datenanalyse vornehmen können. Die Protokollierung sichert die nachträgliche aufsichtliche Kontrolle gemäß Satz 4.

Das Bundesverfassungsgericht hat zudem deutlich gemacht, dass es für eine effektive Kontrolle unerlässlich ist, dass eigenständig ausformulierte Begründungen dafür gegeben werden, warum bestimmte Datenbestände zur Verhütung bestimmter Straftaten im Wege der automatisierten Anwendung analysiert werden. Die in Satz 3 geregelte Begründungspflicht dient der Umsetzung dieser verfassungsgerichtlichen Vorgabe.

Satz 4 regelt die Befugnis der oder des behördlichen Datenschutzbeauftragten, stichprobenartige Kontrollen vorzunehmen. Insoweit wird die ohnehin

bestehende Befugnis der oder des unabhängigen Datenschutzbeauftragten, wie sie in §72 PolDVG zum Ausdruck kommt, aber in Absatz 5 Satz 2 geregelt bzw. Satz 3 klargestellt wird, eine effektive, zwischen behördlichem und unabhängigem Datenschutzbeauftragten aufgeteilte Kontrolle (vgl. hierzu BVerfG, a.a.O., Rn. 109).

Der neue Absatz 5 entspricht im Wesentlichen dem bisherigen Absatz 3.

Zu Nummer 25

§51 PolDVG regelt, unter welchen Voraussetzungen die Polizei auf Ersuchen einer öffentlichen oder einer nicht öffentlichen Stelle personenbezogene Daten für Zwecke einer sog. Zuverlässigkeitsüberprüfung verarbeiten darf. Voraussetzung ist neben dem entsprechenden Ersuchen, zum einen die Zustimmung der betroffenen Person und zum anderen, dass dies im Hinblick auf den Anlass dieser Überprüfung, insbesondere den Zugang der betroffenen Person zu einer besonders gefährdeten Veranstaltung, und mit Rücksicht auf ein berechtigtes Interesse des Empfängers erforderlich ist.

Die Überprüfung beschränkt sich in der geltenden Fassung auf eine Abfrage der personenbezogenen Daten in Dateisystemen der Polizei. Eine Abfrage insbesondere der Daten der Verfassungsschutzbehörden sieht §51 PolDVG nicht vor. Insbesondere die Ausgestaltung der Zuverlässigkeitsüberprüfungen zur UEFA EURO 2024 haben aber gezeigt, dass ein praktisches Bedürfnis besteht, diese Einbindung normenklar zu regeln.

Vor diesem Hintergrund soll der Abfrageumfang maßvoll erweitert werden und insbesondere die Einbindung des Verfassungsschutzes sowie im Falle von Erkenntnissen über Strafverfahren der Strafverfolgungsbehörden und der Gerichte vorsehen. Sofern die zu überprüfende Person Ausländer ist oder ihren Wohnsitz im Ausland hat, kann der Datenabgleich auch mit den Datenbeständen des Bundesamtes für Migration und Flüchtlinge (Ausländerzentralregister) und der zuständigen Polizeien im Ausland erfolgen.

In dem neuen Satz 4 wird klar gestellt, dass die Polizei die zum Zwecke der Durchführung der Zuverlässigkeitsüberprüfungen erforderlichen personenbezogenen Daten an die in Satz 3 benannten Stellen übermittelt. Dies ist schon mit dem Begriff der Verarbeitung impliziert, die die Übermittlung erfasst. Andernfalls würde der neue Satz 3 auch ins Leere gehen. Die Übermittlung ist mithin schon notwendig, um die in Satz 3 erlaubte Einbindung überhaupt erst zu ermöglichen. Auch der neue Satz 5 regelt dem Grunde nach nur klarstellend, dass zur Sammlung der Ergebnisse und deren weitere Verarbeitung die in Satz 3 benannten Stellen ihre Rückmeldungen an die Polizei übermitteln. In einem neuen Satz 6 wird klargestellt, dass auch ein automatisierter Abruf zulässig ist. Danach gilt, dass auch ein automatisierter Datenabgleich mit den Dateisystemen der in Nummer 1 bis 5 genannten Stellen zulässig ist, soweit die Polizei die Berechtigung zum Abruf hat.

Nach dem bisherigen §51 Satz 6 gilt, dass die Beschränkungen des §34 Absatz 4 Satz 1, auch in Verbindung mit §38 Absatz 1 Satz 2, keine Anwendung finden. Hintergrund für die Regelung in Satz 6 war der Gedanke, dass der in §34 Absatz 4 Satz 1 kodifizierte hypothetische Ersatzeingriff für Zuverlässigkeitsüberprüfungen nicht gelten soll. Denn die Effizienz einer Zuverlässigkeitsüberprüfung hängt wesentlich davon ab, dass in die Bewertung des Sicherheitsrisikos auch solche Erkenntnisse einfließen können, die aus eingriffsintensiven polizeilichen Maßnahmen wie z.B. der längerfristigen Observation oder dem Einsatz Verdeckter Ermittler gewonnen wurden. Anderenfalls wäre die Bewertungsgrundlage gerade in den sicherheitsrelevanten Bereichen Organisierte Kriminalität und Terrorismus entscheidend verkürzt, und die Polizei wäre gezwungen, dem Betroffenen wider besseres Wissen das Fehlen eines Sicherheitsrisikos zu attestieren. Dies sollte mit Satz 6 sichergestellt werden (vgl. Drucksache 21/17906, S. 71 mit Verweis auf Drucksache 18/2288, Anlage 9). Da §34 Absatz 4 Satz 1 und der darin geregelte hypothetische Ersatzeingriff mit diesem Gesetzentwurf gestrichen wird, ist auch der entsprechende Verweis darauf in §51 Satz 6 zu streichen.

Der mit dem Verweis zum Ausdruck gebrachte Gedanke der Gewährleistung einer effizienten Zuverlässigkeitsprüfung gilt aber fort, denn der in §34 Absatz 2 PolDVG neu eingeführte Grundsatz der hypothetischen Datenneuerhebung gilt bei §51 PolDVG nicht. §51 PolDVG ist insoweit eine Vorschrift dieses Gesetzes, welche die zweckändernde Weiterverarbeitung besonders regelt (vgl. §34 Absatz 2, letzter Halbsatz PolDVG-E und oben stehende Begründung dazu).

Zu Nummer 26

§52 PolDVG, der die Modalitäten der Auftragsdatenverarbeitung regelt, ist mit dem Gesetz über die Datenverarbeitung der Polizei vom 12. Dezember 2019 (HmbGVBl. S. 485) eingefügt worden. Vorgaben zur Auftragsdatenverarbeitung waren bis dato im HmbDSG (vgl. §3 HmbDSG a.F.) geregelt. Diese sind dort aber im Zuge der Anpassung an die DS-GVO weggefallen. Zugleich setzte die Norm die Regelungen des Artikels 22 der DS-RL um. Dabei wurden Elemente des bisherigen §3 Absatz 1 bis 3 HmbDSG a.F. aufgegriffen. Die Ausgestaltung orientierte sich im Wesentlichen an §62 BDSG, mit dem im Bundes-

datenschutzgesetz Artikel 22 der DS-RL umgesetzt wird.

Abweichend von der Regelung in §62 Absatz 3 BDSG ist bisher nach §52 Absatz 3 PolDVG immer eine vorherige schriftliche Genehmigung erforderlich, wenn der Auftragsverarbeiter weitere Auftragsverarbeiter (sog. Unterauftragsverarbeiter) hinzuzieht. Eine allgemeine schriftliche Genehmigung, wie sie nach Artikel 22 Absatz 2 Satz 1 2. Alt DS-RL möglich und in der Mehrzahl der datenschutzrechtlichen Regelungen auch im Wortlaut umgesetzt ist (vgl. z.B. §62 Absatz 3 BDSG, §45 Absatz 5 BDSG, §52 Absatz 1 Satz 1 DSG NRW, §48 Absatz 3 BlnDSG, §38 Absatz 3 LDSG SH, §51 Absatz 3 LDSG RPf, §48 Absatz 3 ThürDSG, §28 Absatz 2 Nummer 3 BayDSG, §27 Absatz 5 BbgPJMDSG, §57 Absatz 3 HDSIG, §3 DSG M-V iVm Artikel 28 Absatz 2 DS-GVO, §53 Absatz 1 SächsPVDG iVm §18 Absatz 3 SächsDSUG, §18 Absatz 3 DSUG LSA, §57 Absatz 3 SPolDVG, §78 Absatz 3 PolG HB), kommt mithin bisher nicht zur Anwendung.

Dies soll aber mit der Neufassung des Absatzes 3 von §52 PolDVG ermöglicht werden. Der Wortlaut entspricht dabei §62 Absatz 3 BDSG.

Danach eröffnet die Neuregelung in §52 Absatz 3 Satz 2 PolDVG dem Verantwortlichen die Möglichkeit, die Hinzuziehung weiterer Auftragsverarbeiter abseits der konkreten Genehmigung im Einzelfall auch im Allgemeinen zu genehmigen. In diesem Fall hat der Auftragsverarbeiter den Verantwortlichen allerdings über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren. Korrespondierend dazu kann der Verantwortliche gem. §52 Absatz 3 Satz 4 die Hinzuziehung oder Ersetzung untersagen (vgl. zum wortlautidentischen §62 BDSG, Paschke/Scheurer, in: Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, §62 Rn. 16).

Während nach aktueller Rechtslage die vorherige schriftliche gesonderte Genehmigung erforderlich ist, besteht im Falle der dann auch möglichen vorherigen allgemeinen schriftlichen Genehmigung eine Informationspflicht des Auftragsverarbeiters für den Fall der Hinzuziehung weiterer Auftragsverarbeiter und das Recht des Auftragsgebers die Hinzuziehung des Unterauftragsverarbeiters zu untersagen. Damit besteht auch im Falle einer vorherigen allgemeinen schriftlichen Genehmigung eine Einwirkungsmöglichkeit des Verantwortlichen.

Zu Nummer 27

Es handelt sich um eine redaktionelle Anpassung. Statt Datenschutz-Folgeabschätzung muss es Datenschutz-Folgenabschätzung heißen.

Zu Nummer 28

Nachdem die Innenrevision und der Hamburgische Datenschutzbeauftragte im Tätigkeitsbericht 2008/2009 (vgl. Drucksache 19/5867, S. 39ff) die Kontrolle der Zugriffsprotokollierungen kritisiert hatten, wurde durch die Polizei ein ergänzendes Stichprobenverfahren „Kontrolle der Kontrolleure“ im Rahmen der Eigenüberwachung innerpolizeilich eingeführt.

Mit der vorgeschlagenen Regelung soll klargestellt werden, dass bis zum Abschluss des ergänzenden Stichprobenverfahrens eine zeitlich befristete Verarbeitung gerade auch der Protokolldaten zum Abfragenden und zum Abgefragten in einer gesicherten technischen Umgebung außerhalb der Protokolldatenbank mitumfasst ist und dies keine unzulässige Mehrfachspeicherung darstellt. Letztlich dient die erweiterte Stichprobe trotz der andauernden Verarbeitung der personenbezogenen Daten des Betroffenen und der Belastung dessen Rechts auf informationelle Selbstbestimmung der Kontrolle der Wirksamkeit der technisch-organisatorischen Maßnahme der sogenannten Zufallsprotokollierung und damit nicht nur der Minimierung der Risiken der Rechte und Freiheiten, sondern auch der Gewährleistung und Stärkung des Rechts auf informationelle Selbstbestimmung der Betroffenen.

Zu Nummer 29

Neben einer redaktionellen Änderung in Absatz 3 Satz 1 wird im Einklang mit der Begründung zur Neufassung des §63 PolDVG in 2019 bereits im Wortlaut der Norm hervorgehoben, dass die Protokolldaten auch für die Verhütung von Straftaten verwendet werden dürfen. Im Hinblick auf Absatz 3 hieß es in der Begründung seinerzeit, dass Absatz 3 Satz 1 Verwendungsbeschränkungen statuiere, wobei von der durch die DS-RL eröffneten Möglichkeit, die Protokolldaten über die Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung der Datensicherheit hinaus auch im Zusammenhang mit der Verhütung oder Verfolgung von Straftaten zu verwenden, Gebrauch gemacht werde (vgl. Drucksache 21/17906, S. 75). Die Norm war und ist wortlautidentisch mit §76 BDSG, der auch eine wortlautidentische Begründung aufweist, also danach auch die Verhütung von Straftaten bereits jetzt mitregeln möchte (vgl. BT-Drucksache 18/11325, S. 119).

Nach Artikel 25 Absatz 3 der DS-RL sind die Protokolle ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten sowie für Strafverfahren zu verwenden, wobei nach Erwägungsgrund 57 der DS-RL die Eigenüberwachung auch interne Disziplinarverfahren der zuständigen Behörden umfasst.

Zum Straftatenbegriff ist anzumerken, dass es sich nach Erwägungsgrund Nr. 13 der DS-RL bei dem Straftatenbegriff um einen eigenen Unionsbegriff handelt, der die Möglichkeit eröffnet, hierunter auch Ordnungswidrigkeiten zu subsumieren. Soweit also von Strafverfahren die Rede ist, schließt dies im Einklang mit der DS-RL auch Ordnungswidrigkeitenverfahren mit ein. Der Anwendungsbereich der DS-RL ist nicht auf Strafverfahren im herkömmlichen deutschen Rechtsverständnis beschränkt, sondern erfasst auch Ordnungswidrigkeitenverfahren. Aus diesem Grund steht Artikel 25 der DS-RL einer entsprechenden Regelung gerade nicht entgegen. Andere Bundesländer sehen in ihren jeweiligen Datenschutzgesetzen oder bereichspezifisch ebenfalls ausdrücklich eine derartige Verwendungsmöglichkeit vor (§ 81 Absatz 3 BremPolG, Artikel 63 Absatz 3 PAG, § 46a SOG-MV, § 52 LDSG SH).

Eine Protokolldatenauswertung auch zur Verhütung von Straftaten, lässt sich beispielhaft an Sachverhalten verdeutlichen, bei denen sich Personen in Zeugen- oder Opferschutzprogrammen befinden. Eine Protokolldatenauswertung soll Gefährdungen für diese Personen respektive Straftaten zum Nachteil dieser Personen verhindern.

In Satz des Absatzes 3 soll daneben die Löschfrist auf 36 Monate ausgedehnt werden unabhängig von dem Datum der Speicherung und damit ausgestaltet werden. Bisher sind die Protokolldaten am Ende des auf die Generierung folgenden Jahres zu löschen (vgl. § 63 Absatz 3 S. 2). Zukünftig sind die Protokolldaten 36 Monate nach deren Generierung zu löschen. Denn stellt man auf das Ende des auf die Generierung folgenden Jahres ab, können sich die Löschfristen aktuell – je nach Zeitpunkt der Speicherung (Anfang oder Ende eines Jahres) – erheblich unterscheiden. In Ermangelung einer ausdrücklichen Vorgabe in Artikel 25 der DS-RL und mit Blick auf die turnusmäßige zweijährige Prüfpflicht der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (vgl. § 73 PolDVG) wird eine Frist von 36 Monaten als angemessen erachtet. Die polizeiliche Praxis weist darauf hin, dass in Einzelfällen eine Löschung schon nach 24 Monaten zu kurz bemessen ist, weswegen stattdessen eine Frist von 36 Monaten als sachdienlich erachtet wird.

Zu Nummer 30

Aktuell sieht § 65 nur eine Kennzeichnung für die nach den § 20 bis 31 und § 50 erhobenen personenbezogenen Daten vor, also für Daten aus verdeckten und eingriffsintensiven Maßnahmen. Zur (technisch-organisatorischen) Umsetzung des vom Bundesverfassungsgericht entwickelten Grundsatzes der hypothetischen Datenneuerhebung, wie er sich in § 34 widerspiegelt, ist eine Erweiterung der Kennzeichnung erforderlich. Diese wird in Anlehnung an § 14 BKAG (Kennzeichnung) vorgenommen. Dergestalt wird damit auch den Vorgaben des § 29 Absatz 4 BKAG entsprochen, wonach über den Verweis auf § 14 BKAG die Kennzeichnung für alle Teilnehmer im polizeilichen Informationsverbund gilt.

§ 65 Absatz 1 Satz 1 sieht dementsprechend vor, dass personenbezogene Daten durch Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden (Nummer 1), bei Personen, zu denen Grunddaten angelegt wurden, durch die Angabe der Kategorie der betroffenen Person (Nummer 2), durch die Angabe der Rechtsgüter, deren Schutz die Erhebungsvorschrift bezweckt oder Straftaten, deren Verfolgung oder Verhütung die Erhebungsvorschrift bezweckt (Nummer 3) und durch die Angabe der Stelle, die die Daten erhoben hat (Nummer 4) zu kennzeichnen sind. Im Wortlaut abweichend von § 14 Absatz 1 Nummer 3 BKAG im Ergebnis aber identisch, ist mit Nummer 3 nicht nur das Rechtsgut gemeint, welches konkret bei der Erhebung der Daten geschützt werden soll, sondern gemeint sind alle Rechtsgüter, die vom Schutzzweck der Erhebungsnorm umfasst sind.

Der Begriff Dateisystem ist in § 2 Absatz 13 legal definiert. Der Begriff (polizeiliches) Informationssystem ist angelehnt an § 14 BKAG, auch die StPO verwendet diesen Begriff in § 483 StPO (vgl. Drucksache 19/4671, S. 67). Eine Legaldefinition findet sich allerdings nicht. Andere Bundesländer verwenden im Kontext der Kennzeichnungsverpflichtung zumeist den Begriff des Informationssystems (vgl. § 188b LVwG SH, § 52 BremPolG, § 53 POG RP). Danach sind polizeilichen Informationssysteme, solche, die dem polizeilichen Informationsaustausch und der Auskunft dienen und nicht etwa der Vorgangsverwaltung (vgl. zu § 188b LVwG Drucksache 19/2118, S. 101 und zu § 52 BremPolG Drucksache 20/682, S. 139f). Aber auch der Begriff Dateisystem wird verwendet (vgl. § 22b PolG NRW). Mitunter wird ohne genaue Verortung auch nur geregelt, dass zu kennzeichnen ist (vgl. Art 48 Absatz 5 BayPOG). Um jegliche aktuelle, aber auch zukünftige Ausgestaltung der Datenhaltung zu erfassen, wird insoweit der Begriff der Dateisysteme ebenso verwendet, wie der der Informationssysteme.

Absatz 2 ist zu der aktuell geltenden Regelung unverändert.

Absatz 3 regelt verschiedene Ausnahmen von der Kennzeichnungspflicht. In Satz 1 handelt es sich um die tatsächliche Unmöglichkeit einer Kennzeichnung – etwa, wenn nicht bekannt oder feststellbar ist, wer die Daten erhoben hat oder zu welchen Zwecken sie ursprünglich erhoben wurden. Die Norm trägt dem Umstand Rechnung, dass Daten vorhanden sind, für die nicht mehr alle Informationen nach Satz 1 rekons-

truiert werden können. In Satz 2 werden die Fälle der technischen Unmöglichkeit und des unverhältnismäßigen Aufwandes einer Kennzeichnung geregelt. Nach dem Vorbild von § 115 Satz 2 HSOG und § 152 Absatz 5 BremPolG soll Absatz 3 Satz 2 jedoch mit einer Befristung Anwendung finden, um die technische Unmöglichkeit und den unverhältnismäßigen Aufwand nicht unbefristet zu dulden.

Zu Nummer 31

Hiermit wird ein redaktionelles Versehen behoben. § 68 Absatz 3 PolDVG regelt das formelle Verfahren der Benachrichtigungspflicht. Gemäß dessen Satz 1 ist für die weitere Zurückstellung der Benachrichtigung zwölf Monate nach Beendigung der Maßnahme eine gerichtliche Entscheidung erforderlich. Nach Satz 2 wird diese Frist zur Einholung einer gerichtlichen Entscheidung bei Maßnahmen nach § 22 PolDVG und § 25 PolDVG auf sechs Monate verkürzt. § 22 PolDVG regelt die Datenverarbeitung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen und § 25 PolDVG die Verkehrsdatenverarbeitung, Nutzungsdatenverarbeitung und den Einsatz besonderer technischer Mittel zur Datenerhebung. Die Gleichstellung von § 22 und § 25 im Hinblick auf die Fristbemessung für die Einholung einer gerichtlichen Entscheidung einer weiteren Zurückstellung ist aber rechtlich nicht erforderlich. Auch im Bundesrecht existiert im Rahmen der StPO bei vergleichbaren Maßnahmen eine solche Frist nur für die akustische Wohnraumüberwachung und die Onlinedurchsuchung (vgl. § 101 Absatz 6 Satz 5 StPO; zur Verfassungsgemäßheit von § 101 StPO vgl. BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 u.a.). Auch das BKAG sieht eine Sechs-Monats-Frist nur für den Einsatz technischer Mittel in oder aus Wohnungen und den verdeckten Eingriff in informationstechnische Systeme vor (vgl. § 74 Absatz 3 Satz 2 BKAG).

Zu Nummer 32

In § 75 PolDVG wird die Berichtspflicht gegenüber der Bürgerschaft geregelt. Für die Berichtspflicht über Maßnahmen nach § 22 PolDVG (Datenverarbeitung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen) übt nach § 75 Satz 3 PolDVG ein von der Bürgerschaft gewähltes Gremium die parlamentarische Kontrolle aus. In Satz 3 wird auf den Einsatz technischer Mittel nach Absatz 1 und, soweit richterlich überprüfungsbedürftig, den nach § 22 Absatz 8 PolDVG erfolgten Einsatz Bezug genommen. Der Verweis auf Absatz 8 ist jedoch nicht zutreffend, da dort Löschungsvorgaben geregelt sind. Gemeint ist der Einsatz nach Absatz 9. Dort ist der Einsatz technischer Mittel zum Schutz der bei einem Polizeieinsatz tätigen Personen geregelt (sog. Personenschutzsender). Der Einsatz dieser Personenschutzsender bedarf keiner richterlichen Anordnung. Dies gilt nur dann nicht, wenn die dabei erlangten Erkenntnisse zur Gefahrenabwehr oder zur Strafverfolgung verwendet werden sollen. Hierfür ist nach § 22 Absatz 9 Satz 3 PolDVG eine richterliche Entscheidung erforderlich. Für diese Fälle der richterlichen Überprüfung beim Einsatz der Personenschutzsender, mithin also nach § 22 Absatz 9, soll das von der Bürgerschaft gewählte Gremium die parlamentarische Kontrolle ausüben. In § 75 Satz 3 PolDVG ist mithin auf § 22 Absatz 9 PolDVG und nicht auf Absatz 8 zu verweisen.

Zu Nummer 33

§ 78 regelt in Absatz 1 Ausnahmen von der Kennzeichnungspflicht nach § 65. Mit der ausdrücklich in § 65 Absatz 3 Satz 2 geregelten zeitlichen Befristung ist § 78 Absatz 1 obsolet.

Der bisherige § 78 Absatz 2 regelt eine Ausnahme von der Protokollierung im Sinne von § 63 Absatz 1, die erst bis zum 6. Mai 2023 erfolgen muss und damit durch Zeitablauf entbehrlich ist.

Der bisherige Absatz 3 von § 78 legt fest, wann der Turnus für Prüfungen nach den § 73 und Unterrichtungen nach § 75 erstmals begann, nämlich am 1. Januar 2022. Auch diese Übergangsregelung hat sich durch Zeitablauf erledigt.

II.

Artikel 2 (Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung)

Zu Nummer 1

Mit der Neufassung des Gesetzes über die Datenverarbeitung der Polizei vom 12. Dezember 2019 (HmbGVBl. S. 485) wurde in § 30 die elektronische Aufenthaltsüberwachung eingeführt. § 13 Absatz 1 Nummer 6 korrespondiert damit insoweit, als Gewahrsam nunmehr auch angeordnet werden kann, wenn dies unerlässlich ist, um eine Anordnung der elektronischen Aufenthaltsüberwachung nach § 30 PolDVG durchzusetzen.

Die Verhältnismäßigkeit der Regelung wird hier durch die hochrangigen Rechtsgüter derentwegen die zugrundeliegende Anordnung erlassen wurde, gewahrt. Der Gewahrsam muss zur Vermeidung der Gefahr, deren Verhinderung die Anordnung dient, unerlässlich sein. Zwar sieht § 35 FamFG vor, dass Zwangsmittel (Zwangsgeld, Zwangshaft) bei Nichtbefolgung der Pflichten aus der gerichtlichen Anordnung, wie sie für die elektronische Aufenthaltsüberwachung nach § 30 Absatz 3 PolDVG erforderlich ist, beantragt werden können. Ein sofortiges Handeln durch freiheitsentziehende Maßnahme wird dadurch allerdings nicht eröffnet.

Zu Nummer 2

Nach § 14 Absatz 5 SOG wird die Sache durch „öffentliche Versteigerung“ nach § 383 BGB verwertet. Der Vertragsschluss kommt durch den Zuschlag nach § 156 BGB zustande.

Diese Voraussetzungen sind bei einer Versteigerung im Internet nach der Rechtsprechung nicht erfüllt, da der Vertragsschluss bei einer Internetauktion durch Willenserklärungen der Parteien – Angebot und Annahme – gem. §§ 145 ff. BGB zu Stande kommt (BGH, Urt. v. 3. November 2004 – VIII ZR 375/03, NJW 2005, S. 53; OLG Nürnberg, Urt. v. 26. Februar 2014 – 12 U 336/13, MMR 2014, S. 592, 593, mwN).

Daher sollen mit der Ergänzung von § 979 Absatz 1 bis 1b BGB, die in § 979 Absatz 1a BGB durch Artikel 4 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2474) eingefügten Regelungen über Versteigerungen im Internet auch für die Verwertung sichergestellter Sachen nach § 14 Absatz 5 SOG Berücksichtigung finden. Zu diesem Zweck wird in Satz 1 die entsprechende Geltung von § 979 Absatz 1 bis 1b BGB angeordnet (vgl. so auch Artikel 27 Absatz 3 BayPAG).

§ 979 Absatz 1 BGB behandelt ausdrücklich die Versteigerung von Sachen durch Behörden oder Verkehrsanstalten, wobei in Absatz 1a auch die Möglichkeit einer Online-Versteigerung normiert ist.

§ 979 Absatz 1b Satz 2 BGB enthält eine Verordnungsermächtigung für die Landesregierungen, die wiederum gemäß § 979 Absatz 1b Satz 2 zweiter Halbsatz BGB auf die fachlich zuständigen obersten Landesbehörden übertragen werden können. Damit können Versteigerungsplattformen bestimmt werden. Gemäß Ziffer 2a der Verordnung zur Weiterübertragung von Verordnungsermächtigungen im Bereich des Bürgerlichen Rechts (Weiterübertragungsverordnung – Bürgerliches Recht) vom 20. August 2002 (HmbGVBl. S. 233) ist die Ermächtigungen zum Erlass von Rechtsverordnungen nach § 979 Absatz 1b Satz 2 erster Halbsatz BGB auf die Behörde für Justiz und Verbraucherschutz weiter übertragen worden. So gilt in Hamburg für den Justizbereich und die Internetversteigerung in der Zwangsvollstreckung bereits die „Verordnung über die Internetversteigerung in der Zwangsvollstreckung sowie von Fundsachen und unanbringbaren Sachen im Justizbereich (Internetversteigerungsverordnung) vom 6. April 2010 (HmbGVBl. S. 254). Danach erfolgen Versteigerungen von an Behörden im Justizbereich abgelieferten Fundsachen gemäß § 978 und § 979 Absatz 1a BGB und von im Besitz von Behörden im Justizbereich befindlichen unanbringbaren Sachen gemäß § 983 und § 979 Absatz 1a BGB über die Versteigerungsplattformen www.justiz-auktion.de oder www.zoll-auktion.de. Entsprechendes wäre dann auch für Versteigerungen von Sachen vorzusehen, die zuvor nach § 14 SOG sichergestellt wurden.

III.

Artikel 3 (Hamburgische Hafensicherheitsgesetz)

Hierbei handelt es sich um eine redaktionelle Änderung, die aus der Aufhebung des bisherigen § 78 im PolDVG resultiert.

Gestaltung und Layout: Lütcke & Wulff, Rondenbarg 8, 22525 Hamburg, Tel. (040) 23512 9-0