Inhaltsverzeichnis

Gesetzentwurf

Hannover, den 10.11.2025

Niedersächsischer Ministerpräsident

Entwurf eines Gesetzes zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes und des Niedersächsischen Verwaltungsvollstreckungsgesetzes

Frau
Präsidentin des Niedersächsischen Landtages
Hannover

Sehr geehrte Frau Präsidentin,

anliegend übersende ich den von der Landesregierung beschlossenen

> **Entwurf eines Gesetzes zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes und des Niedersächsischen Verwaltungsvollstreckungsgesetzes**

nebst Begründung mit der Bitte, die Beschlussfassung des Landtages herbeizuführen.

Federführend ist das Ministerium für Inneres, Sport und Digitalisierung.

Mit freundlichen Grüßen
Olaf Lies

Entwurf

Gesetz zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes und des Niedersächsischen Verwaltungsvollstreckungsgesetzes

Artikel 1

Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes

Das Niedersächsische Polizei- und Ordnungsbehördengesetz in der Fassung vom 19. Januar 2005 (Nds. GVBl. S. 9), zuletzt geändert durch Artikel 3 des Gesetzes vom 22. September 2022 (Nds. GVBl. S. 589), wird wie folgt geändert:

1. § 2 wird wie folgt geändert:

   a) Es wird die folgende neue Nummer 15 eingefügt:

      „15. Vorfeldstraftat:

      eine Straftat nach Nummer 14, die Verhaltensweisen erfasst, die vom Gesetzgeber als generell gefährlich für Individualrechtsgüter oder Kollektivrechtsgüter bewertet werden, aber als einzelne Handlungen in räumlicher oder zeitlicher Hinsicht noch vor einer Gefährdung oder Verletzung solcher Rechtsgüter liegen können und damit strafbewehrte Vorbereitungshandlungen darstellen;“.

   b) Die bisherigen Nummern 15 bis 17 werden Nummern 16 bis 18.

2. Der Dritte Teil wird wie folgt geändert:

   a) Die Überschrift erhält folgende Fassung:

      „Dritter Teil

      Allgemeine und besondere Befugnisse der Verwaltungsbehörden und der Polizei“.

   b) Die Überschrift

      „1. Abschnitt

      Allgemeine und besondere Befugnisse“

      wird gestrichen.

   c) In § 12 Abs. 5 Satz 1 wird die Angabe „und über ihr Auskunftsrecht nach Artikel 15 der Datenschutz-Grundverordnung und § 9 des Niedersächsischen Datenschutzgesetzes oder im Anwendungsbereich des § 23 des Niedersächsischen Datenschutzgesetzes über das Auskunftsrecht nach § 51 des Niedersächsischen Datenschutzgesetzes zu unterrichten“ gestrichen.

   d) § 15 Abs. 1 Satz 1 Nr. 1 erhält folgende Fassung:

      „1. dies für eine nach § 13 zulässige Identitätsfeststellung unerlässlich ist oder“.

   e) § 15 a Abs. 1 Satz 1 erhält folgende Fassung:

      „[1]Zur Feststellung der Identität einer hilflosen Person oder einer Leiche können deren DNA-Identifizierungsmuster mit denjenigen einer vermissten Person abgeglichen werden, wenn dies zur Feststellung der Identität unerlässlich ist.“

   f) § 17 a wird wie folgt geändert:

      aa) In Absatz 1 werden die Sätze 4 bis 6 gestrichen.

bb) Es werden die folgenden Absätze 4 und 5 angefügt:

„(4) [1]Die Polizei unterrichtet eine Person, von der eine Gefahr nach Absatz 1 Satz 1 ausgeht, über Beratungsangebote. [2]Sie kann personenbezogene Daten dieser Person auch ohne deren Einwilligung an geeignete Beratungsstellen übermitteln, damit diese ein Beratungsangebot unterbreiten können.

(5) [1]Die Polizei unterrichtet die gefährdete Person unverzüglich über die Dauer und den räumlichen Umfang einer Maßnahme nach Absatz 1 Sätze 1 und 2 sowie über Beratungsangebote und die Möglichkeit, Schutz nach dem Gewaltschutzgesetz zu beantragen. [2]Sie kann personenbezogene Daten der gefährdeten Person auch ohne deren Einwilligung an eine geeignete Beratungsstelle übermitteln, wenn dies zur Abwehr einer Gefahr erforderlich ist.“

g) § 17 c wird wie folgt geändert:

aa) Absatz 1 wird wie folgt geändert:

aaa) Der bisherige Wortlaut wird Satz 1.

bbb) Es werden die folgenden Sätze 2 und 3 angefügt:

„[2]Eine Verpflichtung nach Satz 1 kann auch erfolgen, wenn gegen die betroffene Person eine Maßnahme nach § 17 a getroffen wurde oder eine richterliche Anordnung nach § 1 des Gewaltschutzgesetzes ergangen ist und die Überwachung sowie die Erhebung, Speicherung, Veränderung und Nutzung der Daten zur Abwehr einer Gefahr für Leib, Leben, Freiheit oder die sexuelle Selbstbestimmung der gefährdeten Person erforderlich ist. [3]Die Verpflichtung nach den Sätzen 1 und 2 umfasst auch die Verpflichtung, ein zur Verfügung gestelltes technisches Mittel zur Kontaktaufnahme, insbesondere ein Mobiltelefon, ständig in betriebsbereitem Zustand bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen.“

bb) Es wird der folgende neue Absatz 2 eingefügt:

„(2) [1]Mit Zustimmung der gefährdeten Person kann dieser ein technisches Mittel zur Verfügung gestellt werden, das Zuwiderhandlungen des Täters gegen Maßnahmen nach § 17 a oder gegen richterliche Anordnungen nach § 1 des Gewaltschutzgesetzes anzeigt. [2]Über das technische Mittel können auch Zuwiderhandlungen gegen Maßnahmen nach Absatz 1 Satz 2 angezeigt werden.“

cc) Die bisherigen Absätze 2 bis 4 werden Absätze 3 bis 5.

dd) Der neue Absatz 3 wird wie folgt geändert:

aaa) Satz 4 wird wie folgt geändert:

aaaa) Es werden die folgenden neuen Nummern 2 und 3 eingefügt:

„2. zur Feststellung von Verstößen gegen eine Wegweisung oder ein Aufenthaltsverbot nach § 17 a,

3. zur Feststellung von Verstößen gegen eine Anordnung nach dem Gewaltschutzgesetz,“.

bbbb) Die bisherigen Nummern 2 bis 5 werden Nummern 4 bis 7.

bbb) Satz 5 erhält folgende Fassung:

„[5]Die Verarbeitung der Daten nach Satz 4 Nrn. 2, 3, 4 und 7 hat automatisiert zu erfolgen.“

ccc) Es wird der folgende Satz 12 angefügt:

„[12]Die Sätze 1, 3 und 4 Nrn. 2 und 3 sowie die Sätze 5 bis 11 gelten entsprechend für die Verarbeitung der Daten, die mithilfe eines technischen Mittels nach Absatz 2 erhoben und gespeichert werden.“

ee) Der neue Absatz 4 Satz 2 wird wie folgt geändert:

aaa) Es werden die folgenden neuen Nummern 3 und 4 eingefügt:

„3. die Angabe, ob die betroffene Person einer Wegweisung oder einem Aufenthaltsverbot nach § 17 a unterliegt,

4. die Angabe, ob die betroffene Person einer Anordnung nach dem Gewaltschutzgesetz unterliegt,“.

bbb) Die bisherigen Nummern 3 bis 5 werden Nummern 5 bis 7.

ff) Im neuen Absatz 5 Satz 2 wird die Angabe „Absatz 3“ durch die Angabe „Absatz 4“ ersetzt.

h) Die Überschrift

„ 2. Abschnitt

Befugnisse zur Datenverarbeitung“

wird gestrichen.

3. Nach § 29 werden die folgenden Überschriften eingefügt:

„Vierter Teil

Befugnisse zur Datenverarbeitung

1. Abschnitt

Datenerhebung“.

4. § 30 wird wie folgt geändert:

a) In Absatz 1 Satz 2 werden im einleitenden Teil nach dem Wort „Dritten“ ein Komma und die Worte „bei Behörden oder sonstigen öffentlichen Stellen“ eingefügt.

b) In Absatz 2 Satz 2 Nr. 1 wird die Angabe „und 5“ durch die Angabe „und des § 32 f“ ersetzt.

c) In Absatz 3 wird das Wort „Dateien“ durch das Wort „Dateisystemen“ ersetzt.

d) Die Absätze 4 bis 7 werden gestrichen.

5. § 31 wird wie folgt geändert:

a) In Absatz 2 werden im einleitenden Teil das Wort „darf“ durch das Wort „kann“ und die Worte „erheben über“ durch die Worte „zu folgenden Kategorien betroffener Personen erheben:“ ersetzt.

b) Es wird der folgende Absatz 5 angefügt:

„(5) Die Verwaltungsbehörden und die Polizei dürfen besondere Kategorien personenbezogener Daten im Sinne des § 24 Nr. 13 des Niedersächsischen Datenschutzgesetzes nur erheben, wenn dies für die in den Absätzen 1 bis 3 genannten Zwecke unerlässlich ist.“

6. Nach § 31 a wird die folgende Überschrift eingefügt:

„2. Abschnitt

Besondere Befugnisse und Maßnahmen der Datenerhebung“.

7. § 32 Abs. 4 erhält folgende Fassung:

„(4) [1]Die Polizei kann bei Maßnahmen nach den Absätzen 1 bis 3 auch Systeme zur automatisierten Erkennung und Auswertung von Mustern bezogen auf Gegenstände und Personen einsetzen, soweit dies die jeweilige Gefahrenlage aufgrund entsprechender Erkenntnisse erfordert. [2]Die automatisierte Auswertung von Mustern bezogen auf Personen darf nur auf das Erkennen solcher Verhaltensmuster ausgerichtet sein, die auf die Begehung einer Straftat oder den Eintritt eines Unglücksfalles im Sinne von § 323 c Abs. 1 StGB hindeuten. [3]Die automatisierte Erkennung und Auswertung ist bei Maßnahmen nach den Absätzen 1 und 3 kenntlich zu machen. [4]Automatisierte Auswertungen sind zusammen mit den Aufzeichnungen gemäß Absatz 3 Satz 5 zu löschen. [5]Das Ergebnis der automatisierten Auswertung sowie dessen Löschung sind zu dokumentieren.“

8. Nach § 32 werden die folgenden neuen §§ 32 a bis 32 e eingefügt:

„§ 32 a

Mobile Bild- und Tonaufzeichnungsgeräte

(1) [1]Die Polizei kann bei der Durchführung von Maßnahmen zur Gefahrenabwehr oder von Maßnahmen zur Verfolgung von Straftaten oder Ordnungswidrigkeiten auf öffentlichen Straßen oder Plätzen oder an anderen öffentlich zugänglichen Orten durch den Einsatz technischer Mittel, insbesondere am Körper getragener Bild- und Tonaufzeichnungsgeräte, Aufzeichnungen offen anfertigen, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Polizeibeamtinnen und Polizeibeamten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. [2]Sie soll Bild- und Tonaufzeichnungen offen anfertigen

1. bei der Androhung und Anwendung von unmittelbarem Zwang oder
2. wenn im Fall einer polizeilichen Maßnahme, die durch die Anwendung unmittelbaren Zwangs durchgesetzt werden kann, die betroffene Person dies verlangt.

[3]Durch technische Mittel kann ein automatisierter Beginn der Aufzeichnung durch am Körper getragene Bild- und Tonaufzeichnungsgeräte für jeden Fall vorgesehen werden, in dem die Dienstwaffe zu Einsatzzwecken aus der dafür vorgesehenen Tragevorrichtung entnommen wird.

(2) [1]Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. [2]Der Einsatz der technischen Mittel ist kenntlich zu machen. [3]Am Körper getragene Bild- und Tonaufzeichnungsgeräte dürfen auch im Bereitschaftsbetrieb Aufzeichnungen anfertigen. [4]Aufzeichnungen nach Satz 3 sind automatisch nach höchstens 30 Sekunden zu löschen, es sei denn, es beginnen in dieser Zeitspanne Aufzeichnungen nach Absatz 1. [5]In diesem Fall werden die Aufzeichnungen nach Satz 3 erst gemeinsam mit den Aufzeichnungen nach Absatz 1 gelöscht. [6]Aufzeichnungen nach Absatz 1 sind unverzüglich, spätestens jedoch nach sechs Wochen zu löschen, soweit sie nicht zur Verfolgung einer Straftat erforderlich oder zur Behebung einer Beweisnot unerlässlich sind. [7]Die §§ 12 und 17 des Niedersächsischen Versammlungsgesetzes bleiben unberührt.

(3) [1]In Wohnungen (§ 24 Abs. 1) sind Maßnahmen nach Absatz 1 nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Polizeibeamtinnen und Polizeibeamten oder Dritten gegen eine dringende Gefahr für Leib oder Leben erforderlich ist. [2]Absatz 1 Sätze 2 und 3 sowie Absatz 2 gelten entsprechend, wobei eine Aufzeichnung auf Verlangen der betroffenen Person nach Absatz 1 Satz 2 Nr. 2 nicht erfolgen darf, wenn diese Person offenkundig nicht die Verfügungsgewalt über die Wohnung innehat oder eine anwesende verfügungsberechtigte Person der Aufzeichnung widerspricht. [3]Ergeben sich während der Durchführung einer Maßnahme nach den Sätzen 1 oder 2 Anhaltspunkte dafür, dass der Kernbereich privater Lebensgestaltung betroffen ist, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung für Leib und Leben von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten möglich ist. [4]Unterbleibt eine Unterbrechung aufgrund einer Gefährdung nach Satz 3, sind die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und die Umstände des Fortsetzens der Maßnahme zu dokumentieren. [5]Die Maßnahme darf

fortgeführt werden, wenn keine Anhaltspunkte mehr dafür vorliegen, dass der Kernbereich privater Lebensgestaltung betroffen ist. [6]§ 33 Abs. 5 Sätze 1, 2 und 4 gilt entsprechend. [7]Die Dokumentation ist am Ende des Kalenderjahres, das der Protokollierung folgt, zu löschen. [8]Eine Verwertung der nach den Sätzen 1 und 2 gefertigten Aufzeichnungen ist zum Zweck der Gefahrenabwehr oder für die Überprüfung der Rechtmäßigkeit des polizeilichen Handelns nur zulässig, wenn zuvor die Rechtmäßigkeit der Bild- und Tonaufzeichnung richterlich festgestellt wurde. [9]Für das Verfahren gilt § 25 Abs. 1 Satz 2 entsprechend.

§ 32 b

Biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen

(1) [1]Die Polizei kann

1. zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person oder
2. zur Abwehr einer Gefahr einer terroristischen Straftat

bei Maßnahmen nach § 32 Abs. 1 bis 3 die biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zur gezielten Suche nach im Datenbestand der polizeilichen Auskunfts- und Fahndungssysteme gespeicherten Personen, die diese Gefahr verursachen, durchführen, soweit dies zur Abwehr dieser Gefahr unerlässlich ist. [2]Die Polizei kann bei den Maßnahmen nach § 32 Abs. 1 bis 3 die biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen auch zur gezielten Suche nach im Datenbestand der polizeilichen Auskunfts- und Fahndungssysteme gespeicherten bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung und gespeicherten vermissten Personen durchführen, soweit die Suche auf diese Weise unbedingt erforderlich ist.

(2) [1]Maßnahmen nach Absatz 1 bedürfen der Anordnung durch das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. [2]Im Antrag der Polizei sind anzugeben:

1. die betroffene Person, soweit möglich mit Namen und Anschrift,
2. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes,
3. der Sachverhalt und
4. eine Begründung.

[3]In der Begründung des Antrags auf Erlass einer richterlichen Anordnung sind die Voraussetzungen für die Maßnahmen nach Absatz 1 und die wesentlichen Abwägungsgesichtspunkte darzulegen. [4]Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die das Vorliegen der Voraussetzungen nach Absatz 1 begründen, und die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme darzustellen. [5]Die Anordnung ergeht schriftlich. [6]Sie muss die in Satz 2 Nrn. 1 und 2 bezeichneten Angaben sowie die wesentlichen Gründe enthalten. [7]Bei der Entscheidung über den Antrag sind die Maßgaben des Artikels 5 Abs. 3 Unterabs. 2 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über Künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024) zu beachten. [8]Für das gerichtliche Verfahren gilt § 19 Abs. 4 entsprechend.

(3) [1]Bei Gefahr im Verzuge kann die Polizei die Anordnung nach Absatz 2 Satz 1 treffen. [2]Im Übrigen gilt § 33 a Abs. 6 Sätze 3 bis 8 entsprechend mit den Maßgaben, dass die richterliche Bestätigung der Anordnung nach § 33 a Abs. 6 Satz 5 unverzüglich, spätestens innerhalb von 24 Stunden zu beantragen ist und die Verwendung der biometrischen Echtzeit-Fernidentifizierung mit sofortiger Wirkung eingestellt wird und alle Daten sowie die Ergebnisse und

Ausgaben dieser Verwendung unverzüglich gelöscht werden, wenn die Anordnung gemäß § 33 a Abs. 6 Satz 6 außer Kraft tritt.

(4) [1]Die Einrichtung und wesentliche Änderung eines biometrischen Echtzeit-Fernidentifizierungssystems erfolgen durch Anordnung der Behördenleitung. [2]Diese kann ihre Anordnungsbefugnis auf Dienststellenleiterinnen oder Dienststellenleiter sowie Beamtinnen oder Beamte der Laufbahngruppe 2 ab dem zweiten Einstiegsamt übertragen. [3]Die oder der Landesbeauftragte für den Datenschutz ist vor der Einrichtung oder wesentlichen Änderung eines Systems nach Satz 1 anzuhören. [4]Bei Gefahr im Verzuge kann auf eine Anhörung verzichtet werden; die Anhörung ist unverzüglich nachzuholen.

§ 32 c

Nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

(1) [1]Die Polizei kann biometrische Daten, insbesondere zu Gesichtern und Stimmen, die sie zur Erfüllung der ihr obliegenden Aufgaben weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat, mit öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, wenn

1. 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 für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt, zur Identifizierung oder Ermittlung des Aufenthaltsortes der betroffenen Person erforderlich ist und
2. dies zur Abwehr der Gefahr unerlässlich ist.

[2]Die Maßnahme nach Satz 1 ist auch zulässig, wenn

1. Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von erheblicher Bedeutung begehen wird und, wenn es sich bei dieser Straftat um eine Vorfeldstraftat handelt, die Verwirklichung der Straftat zu einer Gefahr für das geschützte Rechtsgut führen würde, oder
2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird,

und der nachträgliche biometrische Abgleich zur Verhütung der Straftat unerlässlich ist. [3]Ein Abgleich mit Daten nach Satz 1 aus im Internet öffentlich zugänglichen Echtzeit-Bildübertragungen ist ausgeschlossen. [4]Biometrische Daten, insbesondere zu Gesichtern und Stimmen, die aus einer Wohnraumüberwachung oder einer Online-Durchsuchung gewonnen wurden, dürfen nicht in den nachträglichen biometrischen Abgleich einbezogen werden.

(2) Die Maßnahmen nach Absatz 1 Sätze 1 und 2 dürfen nur gegen die gemäß § 6 oder § 7 Verantwortlichen, die in § 8 Abs. 1 bezeichneten Personen sowie Personen im Sinne von Absatz 1 Satz 2 durchgeführt werden.

(3) [1]Maßnahmen nach Absatz 1 Sätze 1 und 2 dürfen nur durch die Behördenleitung angeordnet werden. [2]Diese kann ihre Anordnungsbefugnis auf Dienststellenleiterinnen und Dienststellenleiter sowie Beamtinnen und Beamte der Laufbahngruppe 2 ab dem zweiten Einstiegsamt übertragen. [3]Die Anordnung ergeht schriftlich. [4]Liegen die Voraussetzungen der Anordnung nicht mehr vor, so ist die Maßnahme unverzüglich zu beenden.

(4) [1]Die Einrichtung und wesentliche Änderung eines Systems zum automatisierten nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet erfolgen durch Anordnung der Behördenleitung. [2]Diese kann ihre Anordnungsbefugnis auf Dienststellenleiterinnen oder Dienststellenleiter sowie Beamtinnen oder Beamte der Laufbahngruppe 2 ab dem zweiten Einstiegsamt übertragen. [3]Die oder der Landesbeauftragte für den Datenschutz

ist vor der Einrichtung oder wesentlichen Änderung eines Systems nach Satz 1 anzuhören. [4]Bei Gefahr im Verzuge kann auf eine Anhörung verzichtet werden; die Anhörung ist unverzüglich nachzuholen.

(5) [1]Jede Maßnahme nach Absatz 1 Satz 1 oder 2 ist zu begründen. [2]In der Begründung sind die Voraussetzungen für die Maßnahme und die wesentlichen Abwägungsgesichtspunkte darzulegen. [3]Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme sowie die Subsidiarität zu anderen Maßnahmen anzugeben.

(6) [1]Die im Rahmen des Abgleichs nach Absatz 1 Satz 1 oder 2 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen. [2]Die Weiterverarbeitung der beim Abgleich erhobenen Daten zu anderen Zwecken ist unzulässig.

§ 32 d

Einsatz von unbemannten Fahrzeugsystemen

(1) Die Polizei kann bei Maßnahmen nach den §§ 32, 32 e, 33 a, 33 b, 33 d, 35 und 35 a unter den dort genannten Voraussetzungen auch unbemannte Fahrzeugsysteme einsetzen.

(2) [1]In den Fällen des § 32 dürfen unbemannte Fahrzeugsysteme nur dann eingesetzt werden, wenn die Offenheit der Maßnahme gewahrt bleibt. [2]Die Maßnahme ist kenntlich zu machen. [3]§ 32 Abs. 2 bleibt unberührt.

(3) Soweit in den Fällen des Absatzes 1 eine richterliche Anordnung erforderlich ist, muss diese auch den Einsatz von unbemannten Fahrzeugsystemen umfassen.

§ 32 e

Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme

[1]Zur Abwehr einer Gefahr, die von unbemannten Fahrzeugsystemen ausgeht, die an Land, in der Luft oder zu Wasser betrieben werden, kann die Polizei geeignete technische Mittel gegen das System, dessen Steuerungseinheit oder Steuerungsverbindung einsetzen, wenn dies zur Abwehr der Gefahr unerlässlich ist. [2]Die Polizei kann technische Mittel zur Erkennung einer Gefahr nach Satz 1, insbesondere zur Klärung der Herkunft und Steuerung unbemannter Fahrzeugsysteme, einsetzen. [3]Maßnahmen nach den Sätzen 1 und 2 dürfen auch durchgeführt werden, wenn Dritte von einer Datenverarbeitung unvermeidbar betroffen werden.“

9. Der bisherige § 32 a wird § 32 f.

10. § 33 wird wie folgt geändert:

a) In Absatz 2 Satz 1 werden nach dem Wort „Gefährdung“ die Worte „für Leib, Leben oder der weiteren Verwendung“ eingefügt.

b) Absatz 5 wird wie folgt geändert:

aa) Es wird der folgende neue Satz 3 eingefügt:

„[3]Unterbleibt in den Fällen der §§ 36 und 36 a eine Unterbrechung der Datenerhebung aufgrund einer Gefährdung nach Absatz 2 Satz 1, sind neben der Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung auch die Tatsachen zu dokumentieren, die zum Absehen von der Unterbrechung geführt haben.“

bb) Die bisherigen Sätze 3 bis 5 werden Sätze 4 bis 6.

c) Es wird der folgende Absatz 6 angefügt:

„(6) [1]Vor der Weitergabe von Informationen hat

1. bei einer Datenerhebung nach § 36 die Vertrauensperson sowie deren polizeiliche Führungsperson oder

2. bei einer Datenerhebung nach § 36 a die verdeckte Ermittlerin oder der verdeckte Ermittler

zu prüfen, ob durch die Information oder die Art und Weise, in der sie erlangt wurde, Erkenntnisse aus dem Kernbereich der privaten Lebensführung betroffen sind. [2]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.“

11. § 33 b wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„§ 33 b

Identifizierung und Lokalisierung
von Mobilfunkkarten und -endgeräten,
Unterbrechung der Telekommunikation“

b) Absatz 1 Satz 1 erhält folgende Fassung:

„[1]Die Polizei kann unter den Voraussetzungen des § 33 a Abs. 1 durch technische Mittel

1. die Gerätenummer eines Mobilfunkendgerätes und die Kartennummer der darin verwendeten Karte sowie

2. Standortdaten eines mobilen Anschlusses

ermitteln.“

c) Es wird der folgende neue Absatz 2 eingefügt:

„(2) [1]Personenbezogene Daten Dritter dürfen anlässlich einer Maßnahme nach Absatz 1 nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Absatz 1 unvermeidbar ist. [2]Die Daten Dritter dürfen abweichend von § 39 Abs. 1 nur für den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer verwendet werden.“

d) Die bisherigen Absätze 2 und 3 werden Absätze 3 und 4.

e) Im neuen Absatz 4 Satz 1 wird die Angabe „Absätzen 1 und 2“ durch die Angabe „Absätzen 1 und 3“ ersetzt.

f) Es wird der folgende Absatz 5 angefügt:

„(5) Dient eine Ermittlung von Standortdaten eines mobilen Anschlusses nach Absatz 1 Nr. 2 ausschließlich der Ermittlung des Aufenthaltsortes einer gefährdeten Person, so kann abweichend von Absatz 4 die Polizei die Anordnung treffen; § 33 a Abs. 5 Sätze 3 und 4 gilt entsprechend.“

12. § 33 c wird wie folgt geändert:

a) Absatz 1 Satz 1 wird wie folgt geändert:

aa) Im einleitenden Satzteil wird die Angabe „§ 2 Satz 1 Nr. 1 des Telemediengesetzes (TMG)“ durch die Angabe „§ 1 Abs. 4 Nr. 5 des Digitale-Dienste-Gesetzes (Anbieter digitaler Dienste)“ ersetzt.

bb) In Nummer 1 wird die Angabe „(§ 14 TMG)“ durch die Angabe „(§ 2 Abs. 2 Nr. 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes -TDDDG)“ ersetzt.

cc) In Nummer 2 wird die Angabe „(§ 15 Abs. 1 TMG)“ durch die Angabe „(§ 2 Abs. 2 Nr. 3 TDDDG)“ ersetzt.

b) Absatz 2 Satz 1 wird wie folgt geändert:

aa) Im einleitenden Satzteil wird die Angabe „§ 3 Nr. 6 TKG“ durch die Angabe „§ 3 Nr. 1 TKG (Anbieter von Telekommunikationsdiensten)“ ersetzt.

bb) In Nummer 1 wird die Angabe „§§ 95 und 111 TKG“ durch die Angabe „§ 3 Nr. 6 und § 172 TKG“ ersetzt.

cc) In Nummer 3 wird die Angabe „§ 96 Abs. 1 TKG“ durch die Angabe „§ 3 Nr. 70 TKG“ ersetzt.

c) In Absatz 6 Satz 1 wird die Angabe „die Teilnehmerin oder der Teilnehmer (§ 3 Nr. 20 TKG)“ durch die Angabe „die Nutzerin oder der Nutzer (§ 3 Nr. 41 TKG)“ und die Angabe „(§ 3 Nr. 21 TKG)“ durch die Angabe „(§ 3 Nr. 58 TKG)“ ersetzt.

13. § 34 Abs. 1 Satz 1 Nr. 2 erhält folgende Fassung:

„2. eine Person, bei der Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise

a) eine Straftat von erheblicher Bedeutung begehen wird, und, wenn es sich bei dieser Straftat um eine Vorfeldstraftat handelt, die Verwirklichung der Straftat zu einer Gefahr für das geschützte Rechtsgut führen würde, oder

b) eine terroristische Straftat begehen wird,“.

14. § 37 Abs. 1 wird wie folgt geändert:

a) Der bisherige Wortlaut wird Satz 1.

b) Es wird der folgende Satz 2 angefügt:

„[2]Handelt es sich bei dieser Straftat um eine Vorfeldstraftat, ist die Maßnahme nach Satz 1 nur zulässig, wenn die Verwirklichung der Straftat zu einer Gefahr für das geschützte Rechtsgut führen würde.“

15. Nach § 37 b wird die folgende Überschrift eingefügt:

„3. Abschnitt

Weiterverarbeitung personenbezogener Daten“.

16. § 38 erhält folgende Fassung:

„§ 38

Weiterverarbeitung personenbezogener Daten, Zweckbindung

(1) [1]Die Verwaltungsbehörden und die Polizei können personenbezogene Daten, die sie selbst erhoben haben, zur Erfüllung derselben Aufgabe weiterverarbeiten, wenn dies zum Schutz derselben Rechtsgüter oder sonstigen Rechte oder zur Verhütung derselben Straftaten erforderlich ist. [2]Satz 1 gilt entsprechend für personenbezogene Daten, die die in Satz 1 genannten Stellen rechtmäßig zur Kenntnis erlangt haben, ohne sie erhoben zu haben. [3]Die Zweckbestimmung ist bei der Speicherung festzulegen. [4]Eine Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Eingriff in informationstechnische Systeme erlangt wurden, setzt voraus, dass die Weiterverarbeitung dieser Daten im jeweiligen Einzelfall zur Abwehr einer dringenden Gefahr nach § 33 d Abs. 1 Nr. 1 oder zur Verhütung einer in § 33 d Abs. 1 Nrn. 2 und 3 genannten Straftat unerlässlich ist. [5]Eine Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in Wohnungen erlangt wurden, setzt voraus, dass die Weiterverarbeitung dieser Daten im jeweiligen Einzelfall zur Abwehr einer dringenden Gefahr nach § 35 a Abs. 1 Nr. 1 oder 2 unerlässlich ist.

(2) [1]Die Verwaltungsbehörden und die Polizei dürfen besondere Kategorien personenbezogener Daten nur weiterverarbeiten, wenn dies zu den in Absatz 1 genannten Zwecken unerlässlich ist. [2]Die an Verarbeitungsvorgängen nach Satz 1 Beteiligten sind für die besondere Schutzwürdigkeit dieser Daten zu sensibilisieren. [3]Der Zugang zu den personenbezogenen Daten ist zu beschränken. [4]Durch geeignete technische und organisatorische Maßnahmen ist sicherzustellen, dass nachträglich überprüft werden kann, ob und von wem besondere Kategorien personenbezogener Daten abgerufen, eingegeben, verändert oder entfernt worden sind. [5]Soweit es zum Schutz besonderer Kategorien personenbezogener Daten erforderlich ist, sind ergänzend weitere angemessene und spezifische Maßnahmen im Sinne des § 17 Abs. 3 des Niedersächsischen Datenschutzgesetzes zu treffen.“

17. Nach § 38 wird der folgende § 38 a eingefügt:

„§ 38 a

Kennzeichnung in polizeilichen Informationssystemen

(1) [1]Bei der Speicherung in polizeilichen Informationssystemen sind personenbezogene Daten wie folgt zu kennzeichnen:

1. Angabe der eingesetzten Maßnahme der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden,
2. Angabe der Kategorie betroffener Personen bei denjenigen Personen, zu denen der Identifizierung dienende Daten, wie insbesondere Namen, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Anschrift (Grunddaten) angelegt wurden,
3. Angabe der
   a) Rechtsgüter, deren Schutz die Erhebung dient, oder
   b) Straftaten, deren Verhütung die Erhebung dient,
4. Angabe der Stelle, die die Daten erhoben hat.

[2]Die Kennzeichnung nach Satz 1 Nr. 1 kann auch durch Angabe der Rechtsgrundlage der jeweiligen Mittel der Datenerhebung ergänzt werden.

(2) Personenbezogene Daten, die nicht entsprechend den Anforderungen des Absatzes 1 gekennzeichnet sind, dürfen so lange nicht weiterverarbeitet oder übermittelt werden, bis eine Kennzeichnung entsprechend den Anforderungen des Absatzes 1 erfolgt ist.

(3) Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung nach Absatz 1 durch diese Stelle aufrechtzuerhalten.“

18. § 39 erhält folgende Fassung:

„§ 39

Weiterverarbeitung personenbezogener Daten
zu anderen Zwecken

(1) Die Verwaltungsbehörden können personenbezogene Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn die Daten zur Erfüllung eines anderen Zwecks der Gefahrenabwehr erforderlich sind und sie auch zu diesem Zweck mit der Maßnahme hätten erhoben werden dürfen, mit der sie erhoben worden sind.

(2) Die Polizei kann personenbezogene Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn

1. mindestens
   a) vergleichbar schwerwiegende Straftaten verhütet oder
   b) vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte geschützt

werden sollen und

2. sich im Einzelfall konkrete Ermittlungsansätze

   a) zur Verhütung solcher Straftaten ergeben oder

   b) zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte erkennen lassen.

(3) [1]Die Weiterverarbeitung personenbezogener Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, ist auch zulässig, wenn

1. die Daten zur Behebung einer Beweisnot unerlässlich sind und nicht überwiegende Interessen der betroffenen Person entgegenstehen oder

2. die betroffene Person in die Datenerhebung nach § 33 des Niedersächsischen Datenschutzgesetzes in Verbindung mit § 31 Abs. 4 eingewilligt hat.

[2]In den Fällen des Satzes 1 Nr. 2 sind die Daten für eine sonstige Verwendung in ihrer Verarbeitung einzuschränken auf die Weiterverarbeitung, zu der die betroffene Person die Einwilligung erteilt hat.

(4) Abweichend von den Absätzen 1 bis 3 können die folgenden Grunddaten einer Person stets weiterverarbeitet werden, um die Identität dieser Person festzustellen:

1. Familiennamen,
2. Vornamen,
3. Geburtsnamen,
4. sonstige Namen, wie Spitznamen und andere Namensschreibweisen,
5. Geschlecht,
6. Geburtsdatum,
7. Geburtsort,
8. Geburtsstaat,
9. derzeitige Staatsangehörigkeit und frühere Staatsangehörigkeiten,
10. gegenwärtiger Aufenthaltsort und frühere Aufenthaltsorte,
11. Wohnanschrift,
12. Sterbedatum sowie
13. abweichende Angaben zu den Nummern 1 bis 12.

(5) Für die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in Wohnungen oder einen verdeckten Eingriff in informationstechnische Systeme erlangt wurden, gilt Absatz 2 Nr. 2 Buchst. b mit der Maßgabe entsprechend, dass

1. bei personenbezogenen Daten, die durch einen verdeckten Eingriff in informationstechnische Systeme erlangt wurden, im Einzelfall eine Gefahr oder Gefahrenlage nach § 33 d Abs. 1 und

2. bei personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in Wohnungen erlangt wurden, eine dringende Gefahr nach § 35 a Abs. 1 vorliegen muss.

(6) [1]Besondere Kategorien personenbezogener Daten dürfen von der Polizei und den Verwaltungsbehörden unter den Voraussetzungen der Absätze 1 bis 3 und 5 nur zweckändernd

weiterverarbeitet werden, wenn es zur Erreichung des dort genannten jeweiligen Zwecks unerlässlich ist. [2]§ 38 Abs. 2 Sätze 2 bis 5 gilt entsprechend.

(7) [1]Die Polizei kann personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten über eine tatverdächtige Person und im Zusammenhang damit über Dritte rechtmäßig erhoben oder rechtmäßig erlangt hat, zu Zwecken der Gefahrenabwehr nach den Absätzen 2, 3 und 4 weiterverarbeiten, sofern nicht besondere Vorschriften der Strafprozessordnung entgegenstehen. [2]Zur Verhütung von Straftaten darf sie diese Daten nur weiterverarbeiten, wenn dies wegen der Art, Ausführung oder Schwere der Tat sowie der Persönlichkeit der tatverdächtigen Person zur Verhütung von vergleichbaren künftigen Straftaten dieser Person erforderlich ist. [3]Die Speicherung der nach Satz 1 über Dritte erhobenen oder erlangten Daten in Informationssystemen ist nur zulässig über die in § 31 Abs. 2 Nrn. 2, 3 und 5 genannten Personen. [4]Der Ausgang eines strafprozessrechtlichen Verfahrens ist zusammen mit den Daten nach Satz 1 zu speichern.

(8) [1]Daten, die durch Maßnahmen nach diesem Gesetz erhoben worden sind, dürfen nach den Absätzen 2, 4 und 5 zu Zwecken der Verfolgung von Straftaten weiterverarbeitet werden. [2]Personenbezogene Daten, die durch Herstellung von Bildaufzeichnungen im Sinne des § 35 a Abs. 1 Nr. 2 über eine Person im Wege eines verdeckten Einsatzes technischer Mittel in Wohnungen erlangt wurden, dürfen nicht zu Strafverfolgungszwecken weiterverarbeitet werden.

(9) Eine Weiterverarbeitung zu anderen Zwecken liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient.

(10) [1]Sind personenbezogene Daten mit technischen Mitteln ausschließlich zum Schutz der bei einem Einsatz in Wohnungen tätigen Personen erhoben worden, so dürfen sie nur zu einem in § 35 a Abs. 1 genannten Zweck der Gefahrenabwehr oder zur Verfolgung einer der in § 100 c Abs. 1 der Strafprozessordnung genannten Straftaten weiterverarbeitet werden. [2]Die Maßnahme nach Satz 1 bedarf der Anordnung durch das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. [3]Die Anordnung ergeht schriftlich. [4]Sie muss die wesentlichen Gründe enthalten. [5]Für das gerichtliche Verfahren gilt § 19 Abs. 4 entsprechend. [6]Bei Gefahr im Verzuge kann die Polizei die Anordnung treffen. [7]Die Sätze 3 und 4 gelten entsprechend mit der Maßgabe, dass die Anordnung auch eine Begründung der Gefahr im Verzuge enthalten muss; im Übrigen gilt § 33 a Abs. 6 Sätze 3 bis 8 entsprechend.“

19. § 39 a erhält folgende Fassung:

„§ 39 a

Weiterverarbeitung personenbezogener Daten
zu besonderen Zwecken

(1) [1]Die Verwaltungsbehörden und die Polizei dürfen personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken nach Maßgabe des § 25 Abs. 5 des Niedersächsischen Datenschutzgesetzes weiterverarbeiten. [2]Eine Weiterverarbeitung von personenbezogenen Daten, die aus Maßnahmen nach § 33 d oder § 35 a erlangt wurden, ist ausgeschlossen.

(2) [1]Die Polizei darf personenbezogene Daten zu statistischen Zwecken weiterverarbeiten. [2]Die Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren.

(3) [1]Die Verwaltungsbehörden und die Polizei dürfen personenbezogene Daten zu Zwecken der Ausbildung, Fortbildung und Prüfung weiterverarbeiten. [2]Die Daten sind zu anonymisieren und in ihrer Verarbeitung einzuschränken. [3]Von einer Anonymisierung kann nur abgesehen werden, wenn ihre Zwecke der Aus- oder Fortbildung entgegenstehen und die Interessen der betroffenen Person nicht offensichtlich überwiegen. [4]Die Interessen der betroffenen Person stehen in der Regel einer von Satz 2 abweichenden Verarbeitung entgegen, wenn Daten durch eine Maßnahme nach § 32 Abs. 2 oder nach den §§ 33 a bis 37 a erhoben wurden.

(4) [1]Die Polizei sowie Verwaltungsbehörden, soweit diese Aufgaben der Hilfs- und Rettungsdienste wahrnehmen, können fernmündlich an sie gerichtete Hilfeersuchen und Mitteilungen auf einen Tonträger aufnehmen. [2]Die Aufzeichnungen sind spätestens nach einem Monat zu löschen. [3]Dies gilt nicht, wenn die Daten zur Verfolgung einer Straftat oder einer nicht nur geringfügigen Ordnungswidrigkeit oder zur Verhütung einer Straftat von erheblicher Bedeutung erforderlich sind. [4]Für die Weiterverarbeitung besonderer Kategorien personenbezogener Daten gilt § 31 Abs. 5 entsprechend.“

20. Nach § 39 a wird der folgende neue § 39 b eingefügt:

„§ 39 b

Weiterverarbeitung zu Zwecken
der Vorgangsverwaltung und Dokumentation

(1) Die Verwaltungsbehörden und die Polizei können personenbezogene Daten zum Zweck der Vorgangsverwaltung, zur zeitlich befristeten Dokumentation, zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes eines Dateisystems weiterverarbeiten.

(2) [1]Daten, die ausschließlich zu den Zwecken nach Absatz 1 gespeichert werden, dürfen zu einem anderen Zweck nur weiterverarbeitet werden,

1. wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist oder

2. wenn

   a) bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat begehen wird, oder

   b) das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird,

und dies zur Verhütung der terroristischen Straftat unerlässlich ist. [2]Soweit die in Satz 1 genannten Daten durch eine Maßnahme nach § 35 a oder § 37 a erhoben worden sind, dürfen sie zu dem in Satz 1 Nr. 2 genannten Zweck nicht weiterverarbeitet werden. [3]Zur Verfolgung einer Straftat dürfen die in Satz 1 genannten Daten nur weiterverarbeitet werden, wenn sie zur Verfolgung dieser Straftat auch mit einer Maßnahme nach der Strafprozessordnung hätten erhoben werden dürfen, die der Maßnahme entspricht, durch die die Daten erhoben wurden. [4]Die Entscheidungen nach den Sätzen 1 bis 3 trifft die Behördenleitung. [5]Diese kann ihre Entscheidungsbefugnis auf Dienststellenleiterinnen und Dienststellenleiter sowie Beamtinnen und Beamte der Laufbahngruppe 2 ab dem zweiten Einstiegsamt übertragen. [6]Die Entscheidung bedarf der Schriftform; sie ist zu begründen.“

21. Nach § 39 b wird die folgende Überschrift eingefügt:

„4. Abschnitt

Datenübermittlung“.

22. § 40 erhält folgende Fassung:

„§ 40

Allgemeine Regeln der Datenübermittlung

(1) [1]Die Verwaltungsbehörden und die Polizei dürfen personenbezogene Daten unter den Voraussetzungen des § 39 sowie der §§ 41 bis 44 a übermitteln. [2]Datenübermittlungen sind zu dokumentieren. [3]Die Dokumentation muss die empfangende Stelle, den Zeitpunkt, den Anlass und den wesentlichen Inhalt der Übermittlung enthalten. [4]Die Dokumentationen sind am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu löschen. [5]Die Löschung unterbleibt, solange der Nachweis noch für eine bereits eingeleitete Datenschutzkontrolle nach § 48 erforderlich ist oder Grund zu der Annahme besteht, dass im Falle einer Löschung schutzwürdige Belange der betroffenen Person beeinträchtigt würden. [6]Die Sätze 2 bis 5 gelten nicht für mündliche Auskünfte, wenn zu der betroffenen Person keine Erkenntnisse vorliegen, und nicht für das automatisierte Abrufverfahren. [7]Bei der Übermittlung von Daten, die durch eine Maßnahme nach § 32 Abs. 2 oder nach den §§ 33 a bis 37 a erhoben wurden, dürfen die in der Dokumentation enthaltenen Daten ausschließlich zur Datenschutzkontrolle verwendet werden. [8]Sie sind zu löschen, wenn seit einer Benachrichtigung nach § 46 a Abs. 1 ein Jahr vergangen ist oder es einer Benachrichtigung gemäß § 46 a Abs. 6 endgültig nicht bedarf, frühestens jedoch zwei Jahre nach der Dokumentation, es sei denn, die oder der Landesbeauftragte für den Datenschutz zeigt an, dass die Daten zur Erfüllung ihrer oder seiner Aufgaben weiterhin benötigt werden.

(2) Wertende Angaben über eine Person, Daten über die in § 31 Abs. 2 Satz 1 Nrn. 2 bis 5 genannten Kategorien betroffener Personen sowie nach § 37 Abs. 3 übermittelte Daten über eine Person, die mit einer ausgeschriebenen Person angetroffen worden ist, dürfen nur Polizei- und Strafverfolgungsbehörden übermittelt werden.

(3) [1]Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde Stelle. [2]Sie prüft die Zulässigkeit der Datenübermittlung. [3]Erfolgt die Datenübermittlung aufgrund eines Ersuchens des Empfängers, hat dieser der übermittelnden Stelle die zur Prüfung erforderlichen Angaben zu machen. [4]Bei Ersuchen von öffentlichen Stellen prüft die übermittelnde Stelle nur, ob das Ersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, im Einzelfall besteht Anlass zur Prüfung der Rechtmäßigkeit des Ersuchens. [5]Erfolgt die Datenübermittlung durch automatisierten Abruf, trägt die Verantwortung für die Rechtmäßigkeit des Abrufs der Empfänger.

(4) [1]Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere personenbezogene Daten der betroffenen Person oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit einem unverhältnismäßig großen Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen der betroffenen Person oder eines Dritten an der Geheimhaltung offensichtlich überwiegen. [2]Eine Verwendung dieser Daten ist unzulässig. [3]Dies ist dem Empfänger der übermittelten Daten mitzuteilen.

(5) § 32 Abs. 1 bis 5 des Niedersächsischen Datenschutzgesetzes findet Anwendung.

(6) [1]Der Empfänger darf die übermittelten personenbezogenen Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verarbeiten, zu dem sie ihm übermittelt worden sind. [2]Eine Verarbeitung zu anderen Zwecken ist unter Beachtung des § 39 zulässig.

(7) Die Datenübermittlung zwischen Polizei und Verfassungsschutz erfolgt nach dem Niedersächsischen Verfassungsschutzgesetz.“

23. § 41 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„§ 41

Datenübermittlung im innerstaatlichen Bereich“.

b) Der bisherige Wortlaut wird Absatz 1 und wie folgt geändert:

In Satz 1 werden die Worte „Verwaltungs- und Polizeibehörden“ durch die Worte „Verwaltungsbehörden und die Polizei“ ersetzt.

c) Es werden die folgenden Absätze 2 und 3 angefügt:

„(2) Die Verwaltungsbehörden und die Polizei können personenbezogene Daten an andere öffentliche Stellen übermitteln, soweit dies

1. zur Erfüllung der Aufgaben der übermittelnden Stelle,
2. zur Abwehr einer Gefahr durch die empfangende Stelle oder
3. zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer Person

erforderlich ist.

(3) [1]Die Verwaltungsbehörden und die Polizei können personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit

1. dies zur Abwehr einer Gefahr erforderlich ist,
2. die Empfänger ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an der Geheimhaltung überwiegt, oder
3. dies im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und die Betroffenen in diesen Fällen der Übermittlung nicht widersprochen haben.

[2]In den Fällen des Satzes 1 Nr. 3 sind die Betroffenen über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise und rechtzeitig zu unterrichten. [3]Die übermittelnde Stelle hat die Empfänger zu verpflichten, die Daten nur für die Zwecke zu verarbeiten, zu denen sie ihnen übermittelt werden.“

24. Nach § 41 wird der folgende § 41 a eingefügt:

„§ 41 a

Datenübermittlung zum Zweck einer Zuverlässigkeitsüberprüfung

(1) [1]Die Polizei darf anlässlich von besonders gefährdeten Veranstaltungen personenbezogene Daten auf Ersuchen einer öffentlichen oder nicht öffentlichen Stelle übermitteln, soweit dies

1. für eine Zuverlässigkeitsüberprüfung erforderlich ist,
2. mit schriftlicher Zustimmung der betroffenen Person erfolgt und
3. im Hinblick auf den Anlass dieser Überprüfung, insbesondere den Zugang der betroffenen Person zu der Veranstaltung, sowie wegen der Art und des Umfangs der Erkenntnisse über sie und mit Rücksicht auf ein berechtigtes Sicherheitsinteresse des Datenempfängers angemessen ist.

[2]Die Rückmeldung an eine nicht öffentliche Stelle beschränkt sich auf die Auskunft zum Vorliegen von Zuverlässigkeitsbedenken.

(2) [1]Der Empfänger darf die Daten nur für den Zweck der Zuverlässigkeitsüberprüfung verarbeiten. [2]Die Polizei hat den Empfänger schriftlich zu verpflichten, diese Zweckbestimmung einzuhalten und eine Löschung der Daten spätestens nach Beendigung der Veranstaltung vorzunehmen. [3]Die betroffene Person ist durch die Polizei über den Inhalt der Übermittlung zu informieren, soweit dies nicht bereits auf andere Weise sichergestellt ist.“

25. § 42 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Es wird der folgende neue Satz 4 eingefügt:

„[4]Werden besondere Kategorien personenbezogener Daten übermittelt, ist die Unerlässlichkeit der Übermittlung zu dokumentieren.“

bb) Der bisherige Satz 4 wird Satz 5.

b) Absatz 4 wird gestrichen.

c) Der bisherige Absatz 5 wird Absatz 4.

26. § 43 erhält folgende Fassung:

„§ 43

Datenübermittlung im Bereich der
Europäischen Union und deren Mitgliedstaaten

Die §§ 41 und 42 gelten entsprechend für die Übermittlung von personenbezogenen Daten an

1. öffentliche und nichtöffentliche Stellen in Mitgliedstaaten der Europäischen Union,
2. zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten, die mit Aufgaben der Gefahrenabwehr sowie der Verhütung und Verfolgung von Straftaten befasst sind, und
3. Polizeibehörden oder sonstige für Gefahrenabwehr oder die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stellen von Schengen-assoziierten Staaten (§ 24 Nr. 16 des Niedersächsischen Datenschutzgesetzes).“

27. Nach § 43 wird der folgende § 43 a eingefügt:

„§ 43 a

Datenübermittlung der Polizei im internationalen Bereich

[1]Die Polizei kann unter Beachtung des § 49 des Niedersächsischen Datenschutzgesetzes personenbezogene Daten an andere als die in § 43 genannten Staaten oder an andere als die in § 43 genannten ausländischen öffentlichen Stellen und über- und zwischenstaatliche Stellen übermitteln, soweit dies

1. in einem Gesetz oder aufgrund eines Gesetzes, in einem Rechtsakt der Europäischen Union oder einem internationalen Vertrag geregelt ist, oder
2. zur Erfüllung polizeilicher Aufgaben oder zur Abwehr einer erheblichen Gefahr durch die empfangende Stelle erforderlich ist.

[2]Die §§ 46 bis 48 des Niedersächsischen Datenschutzgesetzes sind anzuwenden.“

28. § 44 wird wie folgt geändert:

    a) Die Überschrift erhält folgende Fassung:

    „§ 44

    Veröffentlichung von Daten“.

    b) Absatz 1 wird gestrichen.

    c) Der bisherige Absatz 2 wird einziger Absatz und darin erhält Satz 2 folgende Fassung:

    „[2]Die Warnung kann mit einer wertenden Angabe über die Person verbunden werden.“

29. Nach § 44 wird der folgende § 44 a eingefügt:

„§ 44 a

Übermittlungsverbote und Verweigerungsgründe

Die Datenübermittlung nach den §§ 43 und 43 a ist unzulässig,

1. wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung der Daten zu den in der Charta der Grundrechte der Europäischen Union enthaltenen Grundsätzen, insbesondere dadurch, dass durch die Nutzung der übermittelten Daten im Empfängerstaat Verletzungen von elementaren rechtsstaatlichen Grundsätzen oder Menschenrechtsverletzungen drohen, in Widerspruch stünde,
2. wenn hierdurch wesentliche Sicherheitsinteressen des Bundes oder eines Landes beeinträchtigt würden,
3. wenn die Übermittlung der Daten unverhältnismäßig wäre oder die Daten für die Zwecke, für die sie übermittelt werden sollen, nicht erforderlich sind, oder
4. wenn hierdurch der Erfolg laufender Ermittlungen oder Leib, Leben oder Freiheit einer Person gefährdet würde.“

30. Nach § 44 a wird die folgende Überschrift eingefügt:

„5. Abschnitt

Datenabgleich, Verzeichnis von Verarbeitungstätigkeiten“.

31. § 45 wird wie folgt geändert:

    a) In Absatz 1 Sätze 1 und 2 wird jeweils das Wort „Dateien“ durch das Wort „Informationssystemen“ ersetzt.

    b) In Absatz 2 Satz 1 werden die Worte „polizeilichen Dateien oder mit Dateien“ durch die Worte „polizeilichen Informationssystemen oder mit Informationssystemen“ und die Worte „dieser Dateien“ durch die Worte „dieser Informationssysteme“ ersetzt.

32. Nach § 45 wird der folgende neue § 45 a eingefügt:

„§ 45 a

Automatisierte Datenanalyse

(1) [1]Die Polizei kann personenbezogene Daten, die sie zur Erfüllung der ihr obliegenden Aufgaben weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat, mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und zum Zweck der Analyse weiterverarbeiten, sofern

1. 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 für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt, erforderlich ist,

2. Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von erheblicher Bedeutung begehen wird, und, wenn es sich bei dieser Straftat um eine Vorfeldstraftat handelt, die Verwirklichung der Straftat zu einer Gefahr für das geschützte Rechtsgut führen würde oder

3. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird,

und die automatisierte Datenanalyse zur Abwehr der Gefahr oder zur Verhütung der Straftat unerlässlich ist. [2]In die automatisierte Datenanalyse können rechtmäßig erhobene und gespeicherte Daten, insbesondere Vorgangsdaten, Falldaten, Daten aus den polizeilichen Auskunftssystemen, Verkehrsdaten, Telekommunikationsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch einbezogen werden. [3]Datensätze aus gezielten Abfragen in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen können ergänzend einbezogen werden, soweit dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. [4]Die in der Analyseplattform gespeicherten Verkehrsdaten sind nach Ablauf von zwei Jahren zu löschen, soweit die weitere Speicherung der Daten für die Fallbearbeitung nicht ausnahmsweise erforderlich ist. [5]Die Entscheidung, die Daten nicht zu löschen, ist zu begründen. [6]Soweit personenbezogene Daten gemäß Satz 1 Nr. 1 verarbeitet werden sollen, die durch den verdeckten Einsatz technischer Mittel in Wohnungen oder den verdeckten Eingriff in informationstechnische Systeme gewonnen wurden, ist dies nur zur Abwehr einer dringenden Gefahr zulässig; im Übrigen dürfen diese personenbezogenen Daten nicht in die automatisierte Datenanalyse einbezogen werden.

(2) [1]Die automatisierte Datenanalyse stellt auf der Grundlage vordefinierter Regeln Informationen bereit, mittels derer die Polizei eigene Bewertungen, Prognosen und Entscheidungen trifft. [2]Maschinelle Entscheidungen sind unzulässig. [3]Im Rahmen der Weiterverarbeitung nach Absatz 1 können insbesondere datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, Suchkriterien gewichtet, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden. [4]Die automatisierte Datenanalyse wird manuell ausgelöst und erfolgt anhand von Suchbegriffen, die sich aus einem konkreten Sachverhalt, bezogen auf einen Anlass im Sinne des Absatzes 1, ergeben. [5]Eine direkte Anbindung der Analyseplattform an Internetdienste ist unzulässig. [6]Die §§ 38, 39 und 39 a bleiben unberührt.

(3) [1]Bei dem Einsatz selbstlernender Systeme hat die Polizei sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. [2]Soweit wie technisch möglich, muss die Nachvollziehbarkeit des verwendeten Verfahrens sichergestellt werden. [3]Der Einsatz selbstlernender Systeme ist bei Maßnahmen nach Absatz 1 Satz 1 Nrn. 2 und 3 ausgeschlossen.

(4) [1]Das Fachministerium bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 Satz 1 nach Anhörung der oder des Landesbeauftragten für den Datenschutz durch eine Verwaltungsvorschrift, die zu veröffentlichen ist, das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und nähere Vorgaben zu Art und Umfang der verarbeiteten Daten. [2]In der Verwaltungsvorschrift nach Satz 1 bestimmt es insbesondere

1. die Anforderungen an die Qualifikation der handelnden Personen und das Rollen- und Rechtekonzept,

2. das Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten,

3. die Art der zu verarbeitenden Daten,

4. besondere Regelungen über die Verarbeitung von Daten, die durch Maßnahmen nach den §§ 33 a bis 37 a erhoben wurden, und

5. die Protokollierung, einschließlich einer individuellen Kennung der handelnden Personen.

[3]Das Rollen- und Rechtekonzept regelt die zweckabhängige Verteilung sachlich eingeschränkter Zugriffsrechte anhand von Aufgabenbereichen. [4]Das Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten regelt, welche personenbezogenen Daten in welcher Weise in die automatisierte Analyse einbezogen werden dürfen.

(5) [1]Die Einrichtung und wesentliche Änderung eines Systems zur automatisierten Datenanalyse erfolgen durch Anordnung der Behördenleitung. [2]Diese kann ihre Anordnungsbefugnis auf Dienststellenleiterinnen oder Dienststellenleiter sowie Beamtinnen oder Beamte der Laufbahngruppe 2 ab dem zweiten Einstiegsamt übertragen. [3]Die oder der Landesbeauftragte für den Datenschutz ist vor der Einrichtung oder wesentlichen Änderung eines Systems zur automatisierten Datenanalyse nach Satz 1 anzuhören; bei Gefahr im Verzuge ist die Anhörung nachzuholen. [4]Jeder Fall einer automatisierten Datenanalyse ist schriftlich zu begründen.“

33. § 46 erhält folgende Fassung:

„§ 46

Verzeichnis von Verarbeitungstätigkeiten
für die polizeiliche Datenverarbeitung

Das Verzeichnis von Verarbeitungstätigkeiten nach § 38 des Niedersächsischen Datenschutzgesetzes erlässt die Behördenleitung.“

34. Nach § 46 wird die folgende Überschrift eingefügt:

„6. Abschnitt

Benachrichtigungspflichten, Prüffristen, Berichtigung, Löschung und Einschränkung der Verarbeitung“.

35. Im 6. Abschnitt wird der folgende § 46 a eingefügt:

„§ 46 a

Benachrichtigungspflichten

(1) Über eine Maßnahme nach § 32 Abs. 2 und nach den §§ 33 a bis 37 a sind nach Beendigung der Maßnahme zu benachrichtigen im Falle

1. des § 32 Abs. 2 (verdeckte Anfertigung von Aufzeichnungen) die Person, gegen die sich die Maßnahme richtete, und die erheblich mitbetroffenen Personen,
2. des § 33 a (Überwachung der Telekommunikation) die Beteiligten der überwachten Telekommunikation,
3. des § 33 b (Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten, Unterbrechung der Telekommunikation) die Zielperson,
4. des § 33 c Abs. 1 Nr. 2 (Auskunftsverlangen zu Nutzungsdaten) die Nutzerin oder der Nutzer,
5. des § 33 c Abs. 2 Nr. 2 (Auskunftsverlangen zu besonderen Bestandsdaten) die von der Maßnahme betroffene Person,
6. des § 33 c Abs. 2 Nr. 3 (Auskunftsverlangen zu Verkehrsdaten) die Beteiligten der betroffenen Kommunikation,
7. des § 33 d (verdeckter Eingriff in informationstechnische Systeme) die Zielperson und die mitbetroffenen Personen,
8. des § 34 (längerfristige Observation) und des § 35 (Einsatz technischer Mittel außerhalb von Wohnungen) die Zielperson und die erheblich mitbetroffenen Personen,

9. des § 35 a (Einsatz technischer Mittel in Wohnungen)
   a) die Person, gegen die sich die Maßnahme richtete,
   b) sonstige überwachte Personen und
   c) Personen, die die überwachte Wohnung zurzeit der Durchführung der Maßnahme innehatten oder bewohnten,
10. des § 36 (Vertrauenspersonen) und des § 36 a (Verdeckte Ermittlerinnen und Ermittler)
   a) die Zielperson,
   b) die erheblich mitbetroffenen Personen und
   c) die Personen, deren nicht allgemein zugängliche Wohnung betreten wurde,
11. des § 37 (Polizeiliche Beobachtung) die Zielperson und die Personen, deren personenbezogene Daten gemäß § 37 Abs. 3 übermittelt wurden,
12. des § 37 a (Rasterfahndung), die betroffene Person, gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden.

(2) [1]Die Benachrichtigung nach Absatz 1 unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. [2]Zudem kann die Benachrichtigung einer in Absatz 1 Nr. 2, 6 oder 7 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen ist und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. [3]Nachforschungen zur Feststellung der Identität einer in Absatz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

(3) Die betroffene Person ist mit der Benachrichtigung auf die Rechtsgrundlage der Datenverarbeitung, die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer, gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, das Auskunftsrecht nach § 51 des Niedersächsischen Datenschutzgesetzes sowie auf das Recht der Beschwerde gegen eine richterliche Anordnung einschließlich der hierfür geltenden Frist hinzuweisen.

(4) [1]Die Benachrichtigung nach Absatz 1 wird zurückgestellt, solange

1. eine Gefährdung des Zwecks der Maßnahme nicht ausgeschlossen werden kann,
2. Zwecke der Verfolgung einer Straftat entgegenstehen,
3. durch das Bekanntwerden der Datenerhebung Leib, Leben, Freiheit oder ähnlich schutzwürdige Belange einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, gefährdet werden,
4. durch das Bekanntwerden der Datenerhebung der weitere Einsatz einer in § 36 oder § 36 a genannten Person gefährdet wird und deshalb die Interessen der betroffenen Person zurücktreten müssen.

[2]Soll die Benachrichtigung über eine Maßnahme, die richterlich anzuordnen war, nach Ablauf von einem Jahr weiter zurückgestellt werden, so entscheidet das Gericht, das die Maßnahme angeordnet oder bestätigt hat. [3]Die weitere Zurückstellung nach Satz 2 ist auf höchstens ein Jahr zu befristen; sie kann um jeweils höchstens ein weiteres Jahr verlängert werden. [4]Bei Maßnahmen nach den §§ 33 d und 35 a betragen die Fristen nach den Sätzen 2 und 3 jeweils sechs Monate. [5]In den Fällen des Satzes 1 Nrn. 3 bis 5 kann das Gericht eine längere Frist bestimmen, wenn davon auszugehen ist, dass die Voraussetzungen für die weitere Zurückstellung während der längeren Frist nicht entfallen werden; dies gilt nicht bei Maßnahmen nach den §§ 33 d und 35 a. [6]Lehnt das Gericht die weitere Zurückstellung ab oder entfällt zwischenzeitlich der Grund für die Zurückstellung oder die weitere Zurückstellung, so ist die Benachrichtigung

unverzüglich von der Polizei vorzunehmen. [7]Für das gerichtliche Verfahren gilt § 19 Abs. 4 entsprechend.

(5) [1]Die Zurückstellung der Benachrichtigung über eine Maßnahme, die nicht richterlich anzuordnen war, ist nach Ablauf von zwei Jahren unter Angabe des Grundes und der voraussichtlichen Dauer der oder dem Landesbeauftragten für den Datenschutz mitzuteilen. [2]Eine Mitteilung ist erneut erforderlich, wenn die angegebene Dauer der Zurückstellung überschritten wird.

(6) [1]Die Polizei kann mit Zustimmung des Gerichts, das die Maßnahme angeordnet oder bestätigt hat, endgültig von einer Benachrichtigung nach Absatz 1 absehen, wenn

1. die Voraussetzungen der Zurückstellung auch fünf Jahre nach Beendigung der Maßnahme noch nicht entfallen sind,
2. die Voraussetzungen der Zurückstellung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht entfallen werden und
3. die Voraussetzungen für eine Löschung der Daten vorliegen.

[2]Wurde die Maßnahme nicht von einem Gericht angeordnet oder bestätigt, ist die Zustimmung des Amtsgerichts einzuholen, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. [3]Für das gerichtliche Verfahren gilt § 19 Abs. 4 entsprechend.

(7) Eine an eine minderjährige Person gerichtete Benachrichtigung ist zugleich deren gesetzlichen Vertreterinnen und Vertretern zuzuleiten.“

36. § 47 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Satz 1 erhält folgende Fassung:

„[1]Für jede Person, über die personenbezogene Daten in einem Informationssystem gespeichert sind, sind Fristen festzulegen, zu denen spätestens zu prüfen ist, ob personenbezogene Daten zu berichtigen, zu löschen oder in ihrer Verarbeitung einzuschränken sind.“

bb) Es wird der folgende Satz 5 angefügt:

„[5]Die Beachtung der Aussonderungsprüffristen ist durch geeignete technische Maßnahmen zu gewährleisten.“

b) Es wird der folgende neue Absatz 2 eingefügt:

„(2) [1]In den Fällen des § 31 Abs. 2 Nrn. 2 bis 5 dürfen die Prüffristen

1. bei Erwachsenen fünf Jahre und
2. bei Minderjährigen zwei Jahre

nicht überschreiten.“

c) Der bisherige Absatz 2 wird Absatz 3.

d) Der bisherige Absatz 3 wird gestrichen.

37. Nach § 47 wird der folgende § 47 a eingefügt:

„§ 47 a

Berichtigung, Löschung und Einschränkung der Verarbeitung

(1) [1]Wird bei der nach § 47 vorzunehmenden Überprüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt, dass personenbezogene Daten unrichtig sind, sind diese zu berichtigen. [2]Wenn die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. [3]Sind Daten in nichtautomatisierten Dateien oder Akten zu berichtigen, reicht es aus, in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten unrichtig waren oder geworden sind.

(2) Gespeicherte personenbezogene Daten sind unverzüglich zu löschen, wenn

1. dies durch dieses Gesetz bestimmt ist,
2. ihre Speicherung unzulässig ist oder
3. bei der nach § 47 vorzunehmenden Überprüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass ihre Kenntnis für die speichernde Stelle für die Verarbeitungszwecke nicht mehr erforderlich ist.

(3) [1]Die Löschung unterbleibt, wenn

1. Grund zu der Annahme besteht, dass schutzwürdige Belange der betroffenen Person beeinträchtigt würden, insbesondere weil sie noch nicht nach § 46 a über die Datenerhebung benachrichtigt wurde und die Daten für die Erfolgsaussichten eines Rechtsbehelfs gegen die Maßnahme von Bedeutung sein können, oder
2. diese mit einem unverhältnismäßigen Aufwand verbunden ist.

[2]In diesen Fällen sind die Daten in der Verarbeitung einzuschränken.

(4) In ihrer Verarbeitung eingeschränkte Daten dürfen nur zu den in Absatz 3 Nr. 1 genannten Zwecken oder mit Einwilligung der betroffenen Person verarbeitet werden.

(5) Bei Informationssystemen ist die Einschränkung der Verarbeitung technisch sicherzustellen.“

38. Nach § 47 a wird die folgende Überschrift eingefügt:

„7. Abschnitt

Datenschutzkontrolle, Anwendung des Niedersächsischen Datenschutzgesetzes“.

39. § 48 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 werden nach der Angabe „§§ 33 a bis 37 a“ ein Komma und die Angabe „Datenverarbeitungen nach den §§ 32 b und 32 c“ eingefügt.

bb) In Satz 2 Nr. 1 werden nach dem Wort „Datenerhebung“ die Worte „oder Datenverarbeitung“ eingefügt.

b) In Absatz 2 werden nach dem Wort „erhoben“ die Angabe „oder nach den §§ 32 b, 32 c oder 45 a verarbeitet“ eingefügt.

40. § 49 erhält folgende Fassung:

„§ 49

Anwendung des Niedersächsischen Datenschutzgesetzes

(1) Für die Verarbeitung personenbezogener Daten durch die Polizei zu den in § 23 Abs. 1 Satz 1 des Niedersächsischen Datenschutzgesetzes genannten Zwecken sind neben den Bestimmungen dieses Gesetzes die §§ 24, 34 bis 45 und 50 bis 61 des Niedersächsischen Datenschutzgesetzes anwendbar.

(2) Im Übrigen sind für die Verarbeitung personenbezogener Daten durch die Verwaltungsbehörden und die Polizei neben den Bestimmungen dieses Gesetzes Artikel 1 bis 4 und 12 bis 99 der Datenschutz-Grundverordnung sowie die §§ 2, 7 bis 12, 14 bis 16, 18 bis 22 und 59 bis 61 des Niedersächsischen Datenschutzgesetzes anwendbar.“

41. Die bisherigen Teile „Vierter Teil“ bis „Elfter Teil“ werden „Fünfter Teil“ bis „Zwölfter Teil“.

42. Nach § 111 wird der folgende § 112 angefügt:

„§ 112

Übergangsbestimmung

Abweichend von § 38 a dürfen personenbezogene Daten auch ohne eine dort vorgesehene Kennzeichnung nach den am XX.XX.XXXX [Einsetzen: Tagesdatum des Inkrafttretens des Gesetzes] für die betreffenden Dateien und automatisierten Verfahren geltenden Errichtungsanordnungen weiterverarbeitet und insbesondere übermittelt werden.“

Artikel 2

Änderung des Niedersächsischen Verwaltungsvollstreckungsgesetzes

In § 70 Abs. 1 des Niedersächsischen Verwaltungsvollstreckungsgesetzes in der Fassung vom 14. November 2019 (Nds. GVBl. S. 316), zuletzt geändert durch Artikel 5 des Gesetzes vom 29. Januar 2025 (Nds. GVBl. 2025 Nr. 3), wird das Wort „Sechsten“ durch das Wort „Siebenten“ ersetzt.

Artikel 3

Einschränkung von Grundrechten

Aufgrund dieses Gesetzes können das Grundrecht auf Leben, körperliche Unversehrtheit und Freiheit der Person (Artikel 2 Abs. 2 Sätze 1 und 2 des Grundgesetzes), das Grundrecht auf Wahrung des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) und das Grundrecht auf Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) eingeschränkt werden.

Artikel 4

Evaluierung

[1]Die Landesregierung prüft drei Jahre nach Aufnahme des Wirkbetriebs unter wissenschaftlicher Begleitung die Wirksamkeit und die praktische Anwendung der Maßnahmen, die in Artikel 1 zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes in § 32 Abs. 4, §§ 32 b, 32 c und 45 a eingefügt wurden. [2]Die Landesregierung berichtet dem Landtag jeweils über das Ergebnis der Evaluierung.

Artikel 5

Neubekanntmachung

Das für Inneres zuständige Ministerium wird ermächtigt, das Niedersächsische Polizei- und Ordnungsbehördengesetz in der nunmehr geltenden Fassung mit neuem Datum bekannt zu machen und dabei Unstimmigkeiten des Wortlauts zu beseitigen.

Artikel 6

Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Anlass und Zielsetzung des Gesetzes

Seit der letzten umfassenden Novellierung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG) in der Fassung vom 19. Januar 2005 (Nds. GVBl. S. 9), zuletzt geändert durch Artikel 3 des Gesetzes zur Änderung des Verwaltungsvollstreckungsgesetzes und weiterer Gesetze vom 22. September 2022 (Nds. GVBl. S. 589), im Jahr 2019 hat sich umfangreicher Änderungsbedarf ergeben.

1. Die Anforderungen an die Sicherheitsbehörden in der Kriminalitäts- und Terrorismusbekämpfung haben sich in den vergangenen Jahren enorm verändert und verschärft. Angesichts dynamischer technischer Entwicklungen und neu entstandener hybrider Bedrohungsformen muss die Polizei in die Lage versetzt werden, diese Gefahren adäquat und konsequent zu bekämpfen. Daher ist es unerlässlich, entsprechende Rechtsgrundlagen zu schaffen, damit die Polizei auch zukünftig das notwendige Rüstzeug hat, ihren Aufgaben gerecht zu werden und die Sicherheit der Menschen zu gewährleisten.

   Mit der Novelle sollen deshalb neue Befugnisnormen in das NPOG aufgenommen sowie bereits bestehende Befugnisnormen erweitert oder klarstellend geregelt werden.

   Im Einzelnen:

   Die bestehenden Vorschriften zur elektronischen Aufenthaltsüberwachung („elektronische Fußfessel“) werden erweitert, um von häuslicher Gewalt Betroffene besser zu schützen (§ 17 c Abs. 1). Ergänzend wird eine Rechtsgrundlage geschaffen, um den Betroffenen - mit ihrer Zustimmung - ein technisches Mittel zur Verfügung zu stellen, welches etwaige Zuwiderhandlungen des Täters gegen Maßnahmen nach § 17 a oder gegen richterliche Anordnungen nach § 1 des Gesetzes zum zivilrechtlichen Schutz vor Gewalttaten und Nachstellungen (Gewaltschutzgesetz - GewSchG) anzeigt (sog. Spanisches Modell) (§ 17 c Abs. 2). Als weitere flankierende Maßnahme in diesem Kontext wird in § 17 a geregelt, dass die Polizei personenbezogene Daten von Täterinnen und Tätern auch ohne deren Einwilligung an geeignete Beratungsstellen übermitteln kann.

   Vor dem Hintergrund der anhaltend hohen Bedrohungslage durch Terrorismus, gewaltbereiten Extremismus und organisierte Kriminalität wird in § 32 Abs. 4 für die Polizei der Einsatz Intelligenter Videoüberwachung ermöglicht, mittels derer in Videoaufzeichnungen automatisiert bestimmte Gefahrensituationen oder Verhaltensmuster erkannt werden können, die auf die Begehung von Straftaten hindeuten oder auf bestimmte Muster von Objekten.

   Zum besseren Schutz von Einsatzkräften sowie von Bürgerinnen und Bürgern beispielsweise in Einsatzsituationen im Zusammenhang mit häuslicher Gewalt wird die bisher in § 32 Abs. 4 geregelte und bislang auf den öffentlichen Raum beschränkte Ermächtigung zum Einsatz von

mobilen Bild- und Tonaufzeichnungsgeräten erweitert und deren Einsatz unter Berücksichtigung der verfassungsrechtlichen Vorgaben künftig auch in Wohnungen zugelassen. Des Weiteren werden neue Regelungen zum offenen Anfertigen von Bild- und Tonaufzeichnungen im Zusammenhang mit der Androhung und Anwendung von unmittelbarem Zwang sowie auf Verlangen der von einer polizeilichen Maßnahme betroffenen Personen geschaffen. Zudem soll ein automatisiertes Auslösen der Aufzeichnung ermöglicht werden, sobald die Dienstwaffe aus der dafür vorgesehenen Tragevorrichtung entnommen wird.

Mit dem neuen § 32 b wird der Polizei unter Beachtung der strengen Vorgaben der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Verordnung über Künstliche Intelligenz - KI-Verordnung) der Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlichen Räumen zur Abwehr einer Gefahr für Leib oder Leben einer Person oder der Gefahr einer terroristischen Straftat sowie zur gezielten Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung und vermissten Personen ermöglicht, soweit die Suche auf diese Weise unbedingt erforderlich ist.

Im Hinblick auf stetig steigende und kaum mehr überschaubare Datenmengen in öffentlich zugänglichen Datenbanken wird mit dem neuen § 32 c eine spezifische Ermächtigung für die Polizei geschaffen, zur Identifizierung und Lokalisierung insbesondere von Störern und Tatverdächtigen einen nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet vorzunehmen. Aufgrund der Vielzahl potenzieller Eingriffe in grundrechtlich geschützte Bereiche soll ein solcher nachträglicher biometrischer Datenabgleich nur in engen, konkret vordefinierten Anwendungsfällen möglich sein, zudem ist der Einsatz nur als letztes Mittel zulässig (ultima-ratio-Grundsatz).

Mit dem neuen § 32 d wird eine klarstellende Rechtsgrundlage für den Einsatz von unbemannten Fahrzeugsystemen, insbesondere Drohnen, geschaffen. Mobil einsetzbare Foto-, Video- und Audiotechnik, u. a. auch mit Drohnen, stellt einen einsatztaktischen Mehrwert für die Polizei im Rahmen ihrer Aufgabenerfüllung dar.

Aufgrund aktueller technischer Entwicklungen von unbemannten Fahrzeugsystemen entstehen allerdings auch neue Gefahrenlagen. Um hierauf angemessen reagieren zu können, wird mit § 32 e eine neue Rechtsgrundlage zur Detektion und Abwehr von unbemannten Land-, Luft und Wasserfahrzeugen geschaffen.

Da die Polizei zur Erfüllung ihrer Aufgaben eine aufgrund der Digitalisierung stetig ansteigende Anzahl von Daten auswerten und miteinander verknüpfen muss, was aufgrund der Datenmengen sinnvoll nur noch über technische Anwendungen erfolgen kann, werden in einem neuen § 45 a unter Berücksichtigung der Vorgaben des Bundesverfassungsgerichts (Urteil vom 16. Februar 2023 - 1 BvR 1547/19) die Voraussetzungen für die Nutzung von Anwendungen zur automatisierten Datenanalyse geschaffen.

2. Des Weiteren enthält der Gesetzentwurf die Inhalte eines Entwurfs zur Änderung des NPOG (Drs. 18/8111), der in der 18. Legislaturperiode der Diskontinuität anheimgefallenen ist.

   Seit dem 25. Mai 2016 gilt die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ (Datenschutz-Grundverordnung, im Folgenden DS-GVO genannt) als unmittelbar anzuwendendes Recht. Die DS-GVO regelt das allgemeine und bereichsspezifische Datenschutzrecht jedoch nicht abschließend. So enthält sie sowohl an die Mitgliedstaaten adressierte Regelungsaufträge als auch Öffnungsklauseln und die Möglichkeit zur Normierung spezifischer Bestimmungen und zur Beschränkung ihrer Vorschriften. Insoweit haben der Bund und auch die Länder ihre allgemeinen und fachspezifischen Datenschutzvorschriften anzupassen.

   Die direkte Geltung der DS-GVO erfordert, dass der Bund und auch die Länder ihre allgemeinen und fachspezifischen Datenschutzvorschriften anpassen, um insbesondere widersprüchliche und unzureichende Regelungslagen oder Doppelungen zu vermeiden. Vor diesem Hintergrund wurde im Land Niedersachsen bereits das allgemeine Datenschutzrecht im Niedersächsischen

Datenschutzgesetz (NDSG) mit dem Gesetz zur Neuordnung des niedersächsischen Datenschutzrechts vom 24. Mai 2018 (Nds. GVBl. S. 66) angepasst. Unter Berücksichtigung des NDSG und der unmittelbar geltenden Vorschriften der DS-GVO bedarf es auch einer - bereichsspezifischen - Anpassung der datenschutzrechtlichen Bestimmungen im NPOG.

Neben der DS-GVO ist am 5. Mai 2016 auch die „Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“ (im Folgenden DS-RL genannt) in Kraft getreten. Sie war nach deren Artikel 63 in den Mitgliedstaaten verpflichtend umzusetzen. Dies ist in Niedersachsen mit dem o. a. Gesetz zur Neuordnung des niedersächsischen Datenschutzrechts weitgehend geschehen. Auf den Zweiten Teil des NDSG §§ 23 bis 58 wird hingewiesen. Auch im NPOG wurden Änderungen zur Umsetzung der DS-RL aufgenommen. Darüber hinaus existieren im NPOG bereits etliche Bestimmungen, die den Bestimmungen der DS-RL entsprechen, wie z. B. Unterrichtungspflichten gegenüber der betroffenen Person (§ 30 Abs. 4), die Unterscheidung von Kategorien betroffener Personen (insbesondere § 31 Abs. 2, 3, §§ 31 a bis 37 a, §§ 38, 39, 47), Vorschriften zur Zweckfestlegung, -bindung und -änderung (§§ 38 und 39 sowie §§ 40, 41, 44) und spezifische Regelungen, die den Umgang mit den besonderen Kategorien personenbezogener Daten betreffen (Schutz zeugnisverweigerungsberechtigter Personen, Kernbereichsschutz, §§ 31 a und 33). Diese Bestimmungen bedurften keines weiteren Umsetzungsakts.

Trotz der Anstrengungen zur Umsetzung der DS-RL bestehen noch Bereiche im NPOG, an denen Korrekturen und Nachschärfungen vorgenommen werden müssen, um die DS-RL in allen Einzelheiten umzusetzen. Dies betrifft insbesondere die Schaffung spezieller Regelungen für die Verarbeitung besonderer Kategorien von Daten und die Neufassung der Vorschriften über die Datenübermittlung ins Ausland, die an Mitgliedstaaten der EU unter den gleichen Voraussetzungen erfolgen darf wie die innerstaatliche Datenübermittlung.

Ein weiterer gewichtiger Teil des Gesetzentwurfs dient der Anpassung von Regelungen über die Datenverarbeitung an die im Bundeskriminalamtgesetz (BKAG) getroffenen Regelungen. Dies betrifft insbesondere den Grundsatz der hypothetischen Datenneuerhebung für die Weiterverarbeitung von Daten durch die Polizei sowie die Kennzeichnung von Daten in polizeilichen Informationssystemen. Dabei handelt es sich um Postulate aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 - 1 BvR 966/09 - zum BKAG, die mit der 2019 in Kraft getretenen Änderung des NPOG, die vor allem der Umsetzung dieses Urteils diente, noch nicht aufgegriffen worden waren.

Darüber hinaus wird die Übermittlung von Daten durch die Polizei im Rahmen von Zuverlässigkeitsüberprüfungen ausdrücklich geregelt.

Der bisherige Entwurf wurde zudem unter Berücksichtigung neuer Rechtsprechung sowie zwischenzeitlich erfolgter Gesetzesänderungen überarbeitet. Dies betrifft insbesondere die Formulierung von Eingriffsermächtigungen im Vorfeld der konkreten Gefahr und den Kernbereichsschutz beim Einsatz von Vertrauenspersonen und verdeckten Ermittlerinnen und Ermittlern nach einer Entscheidung des Bundesverfassungsgerichts vom 9. Dezember 2022 (1 BvR 1345/21).

II. Wesentliches Ergebnis der Gesetzesfolgenabschätzung

Mit den vorgeschlagenen gesetzlichen Änderungen wird den technischen Möglichkeiten und den Bedarfen der Polizei an zeitgemäßen Instrumenten zur Bewältigung der polizeilichen Aufgaben Rechnung getragen und die Polizei mit dem notwendigen Rüstzeug ausgestattet, um ihren Aufgaben auch künftig gerecht zu werden und die Sicherheit der Menschen zu gewährleisten. Zudem sollen zwingend notwendige Umsetzungen und Anpassungen an das europäische Datenschutzrecht und die Rechtsprechung des Bundesverfassungsgerichts vorgenommen werden.

Diese Ziele werden mit dem Änderungsgesetz erreicht. Eine Alternative zum Erreichen der Ziele besteht nicht. Durch die im Gesetz enthaltenen unterschiedlichen, teils neuen, teils neu strukturierten und systematisierten Vorschriften werden die für die Gefahrenabwehr zuständigen Behörden in die

Lage versetzt, ihre Aufgaben im Einklang mit europäischem Recht und der Rechtsprechung des Bundesverfassungsgerichts wahrzunehmen. Mit den vorgeschlagenen gesetzlichen Änderungen sind für die Kommunen keine neuen Aufgaben verbunden, durch die ein zusätzlicher Vollzugsaufwand entstehen würde. Konnexitätsrechtliche Folgen nach Artikel 57 Abs. 4 der Niedersächsischen Verfassung werden durch die vorgesehenen Regelungen nicht ausgelöst.

III. Auswirkungen auf die Umwelt, insbesondere auf das Klima und auf die Anpassung an die Folgen des Klimawandels, den ländlichen Raum und die Landesentwicklung

Keine.

IV. Auswirkungen auf die Verwirklichung der Gleichstellung von Männern und Frauen

Keine.

V. Auswirkungen auf Familien

Keine.

VI. Auswirkungen auf Menschen mit Behinderungen

Keine.

VII. Voraussichtliche Kosten und haushaltsmäßige Auswirkungen

Im Hinblick auf die neuen Methoden der Datenerhebung und -analyse, die elektronische Aufenthaltsüberwachung im Kontext Häusliche Gewalt in Form eines Zwei-Komponenten-Modells sowie den Einsatz von Bodycams in Wohnungen ist derzeit noch nicht abschließend geklärt, welche neuen Anwendungen bzw. technischen Mittel beschafft werden und in welchem Umfang die neuen Einsatzmittel in der Praxis eingesetzt werden. Deshalb sind insoweit zum jetzigen Zeitpunkt noch keine belastbaren Aussagen zu den voraussichtlichen Kosten möglich. Überdies ergeben sich aus den neu geschaffenen Befugnisnormen keine Verpflichtungen für die Polizei, bestimmte technische Mittel zu beschaffen. Vielmehr handelt es sich um Ermessensvorschriften, die für den polizeilichen Einsatzbereich näher genannte Optionen eröffnen. Aus dem Gesetzentwurf resultieren daher unmittelbar keine Kosten bzw. Kostenfolgen mit Auswirkung auf den Landeshaushalt.

Hinsichtlich der Kennzeichnung personenbezogener Daten sind umfangreiche IT-seitige Anpassungen der Fachverfahren vorzunehmen. Die diesbezüglich mit Artikel 1 neu eingefügten Regelungen beruhen auf den Vorgaben des Bundesverfassungsgerichtes aus dem Urteil zum BKAG vom 20. April 2016 und dienen deren Umsetzung. Die für die IT-seitige Anpassung aufzuwendenden Mittel können derzeit noch nicht konkret beziffert werden.

Soweit die aus dem Gesetzesentwurf zwangsläufig resultierenden Aufgabenänderungen bzw. -zuwächse (insbesondere die Kennzeichnung personenbezogener Daten) mit zusätzlichem Aufwand verbunden sind, wird dieser (vorbehaltlich etwaig anderslautender Entscheidungen des Haushaltsgesetzgebers) aus den vorhandenen Haushaltsmitteln des Einzelplans 03 erwirtschaftet. Sofern sich aus dem Gesetzentwurf darüber hinaus gegebenenfalls mittelfristig ein zusätzlicher Bedarf zulasten des Landeshaushalts ergeben sollte, steht dieser unter dem Vorbehalt entsprechender Beschlussfassungen des Haushaltsgesetzgebers. Ein Automatismus zur Bereitstellung zusätzlicher Haushaltsmittel zulasten des Gesamthaushalts besteht nicht.

VIII. Auswirkungen auf die Digitalisierung (Digitalcheck)

Durch die neuen polizeilichen Rechtsgrundlagen, insbesondere zur Datenerhebung und -analyse, werden für die Polizei umfassende Befugnisse für den Einsatz zeitgemäßer technischer Instrumente geschaffen, die den steigenden Anforderungen an die tägliche Polizeiarbeit gerecht werden. Diese neuen digitalen Instrumente stellen sicher, dass der Polizei auch zukünftig moderne Einsatzmittel für die Gefahrenabwehr zur Verfügung stehen und sie auch in Zukunft Bedrohungen effektiv begegnen kann. Insofern fördern die neuen Rechtsgrundlagen den weiter voranschreitenden Prozess der Digitalisierung und geben der Polizei die Möglichkeit, die eigene digitale Infrastruktur weiter auszubauen.

IX. Wesentliches Ergebnis der Verbandsbeteiligung

Im Rahmen der Verbandsanhörung gemäß § 31 GGO ist der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens (AGKSV), dem Deutschen Gewerkschaftsbund (DGB), dem dbb niedersachsen beamtenbund und tarifunion, der Gewerkschaft der Polizei (GdP), der Deutsche Polizeigewerkschaft (DPolG); dem Bund Deutscher Kriminalbeamter (BDK), dem Niedersächsische Richterbund (NRB) und dem Niedersächsischen Anwalts- und Notarverband (NANV) Gelegenheit zur Stellungnahme gegeben worden. Zugleich wurde der Landesbeauftragte für den Datenschutz (LfD) beteiligt.

Im Wesentlichen haben die Verbandsanhörung sowie die Beteiligung des Landesbeauftragten für den Datenschutz folgende Ergebnisse gebracht:

– Der LfD begrüßt, dass für bestimmte eingriffsintensive Maßnahmen wie etwa die Echtzeit-Fernidentifizierung im öffentlichen Raum (§ 32 b) oder den nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§ 32 c) im Gesetzentwurf spezifische Rechtgrundlagen geschaffen werden sollen. Gleiches gelte für die neuen Regelungen zu den Benachrichtigungspflichten in § 46 a sowie für die Schaffung von Rechtsgrundlagen beispielsweise für den Einsatz von sogenannten „stillen SMS“ (§ 33 b) und für die Datenübermittlung zum Zweck der Zuverlässigkeitsüberprüfung (§ 41 a). Der LfD begrüßt auch die in § 40 normierte detaillierte Dokumentationspflicht sowie grundsätzlich die in § 47 vorgenommene Abstufung bei den Prüffristen. Gleichzeitig kritisiert der LfD, dass der Gesetzentwurf nicht allen nach seinem Verständnis notwendigen und zwingend einzuhaltenden Vorgaben gerecht werde, und sieht bezüglich der einzelnen Rechtsgrundlagen verschiedentlich noch Änderungs- und Anpassungsbedarfe. Der LfD hat ferner weitere, über den vorgelegten Entwurf hinausgehende Änderungen des NPOG gefordert.

– Die GdP als Mitgliedsgewerkschaft des DGB begrüßt die Regelungen zu der Elektronischen Aufenthaltsüberwachung im Kontext Häusliche Gewalt in Form eines Zwei-Komponenten-Modells und zur Datenübermittlung an Täterberatungsstellen. Für die Aufgaben müssten ausreichend Mittel zur Verfügung gestellt werden. Auch die Regelung zur intelligenten Videoüberwachung wird begrüßt, hier weist die GdP jedoch zugleich auf rechtliche Bedenken hin. Das gleiche gilt für den Einsatz von Bodycams in Wohnungen und bei unmittelbarem Zwang. Der DGB schließt sich der Stellungnahme der GdP an.

– Die DPolG hat sich zusammen mit dem dbb niedersachsen geäußert. Der dbb niedersachsen befürwortet ebenfalls die Regelungen zur Elektronischen Aufenthaltsüberwachung bei häuslicher Gewalt und den Einsatz von Bodycams in Wohnungen, weist jedoch auch auf praktische und rechtliche Bedenken hin.

– Der NANV erkennt die Notwendigkeit einer Anpassung des NPOG aufgrund geänderter technischer Möglichkeiten und Risiken sowie zur Anpassung an einschlägige Rechtsprechung und an das Datenschutzrecht an. Gleichzeitig kritisiert der NANV an verschiedenen Stellen des Gesetzentwurfs das Fehlen von Richtervorbehalten und die Formulierung einzelner Eingriffsbefugnisse.

– Die AG KSV hat zu dem Gesetzentwurf keine Stellungnahme abgegeben. Sie hat jedoch einen Entwurf einer Rechtsgrundlage der Region Hannover für die Weiterverarbeitung personenbezogener Daten aus Gründen der Eigen- oder Fremdgefährdung übermittelt, um einen besseren Austausch zwischen den Behörden über Informationen zu Gefährdern zu gewährleisten. Für die Berücksichtigung des Vorschlags im Rahmen der Novellierung des NPOG wird jedoch keine Notwendigkeit gesehen.

Die eingegangenen Anregungen und Bedenken werden im Zusammenhang mit den einzelnen Vorschriften näher dargestellt.

B. Besonderer Teil

Zu Artikel 1:

Vorbemerkungen zu den Änderungen aufgrund von EU-Datenschutzvorschriften:

Die Anpassungen an die EU-Datenschutzvorschriften verbindet das Ziel, - soweit rechtlich zulässig und möglich - eine direkte Regelung der im Bereich des Gefahrenabwehrrechtes zu beachtenden datenschutzrechtlichen Bestimmungen im NPOG selbst vorzunehmen. Es sollen datenschutzrechtliche Regelungen im NPOG geschaffen werden, die sowohl der Umsetzung der DS-RL dienen als auch den Regelungen der unmittelbar geltenden DS-GVO entsprechen. Dies ist erforderlich, da der EU-Richtliniengeber den Gefahrenabwehrbereich nicht vollständig in den Anwendungsbereich der DS-RL einbezogen hat, sodass einige wenige Fallgestaltungen verbleiben, die dem Anwendungsbereich der DS-GVO zuzuordnen sind und die bei den Gesetzesänderungen mit zu betrachten und - soweit rechtlich zulässig - auch mit zu regeln sind.

Dazu wird insbesondere von den Klauseln in Artikel 6 Abs. 2 und 3 der DS-GVO zur Schaffung spezifischer Bestimmungen Gebrauch gemacht. Diese Regelung sieht vor, dass die Mitgliedstaaten spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der DS-GVO in Bezug auf die Verarbeitung für die Wahrnehmung einer Aufgabe in Ausübung öffentlicher Gewalt einführen können, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten.

Zudem wird auf Artikel 23 Abs. 1 DS-GVO hingewiesen, der bestimmt:

„Durch Rechtsvorschriften (…) der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

(…)

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit; (…)“.

Danach ermöglichen es die Vorgaben und Ziele der DS-GVO, im Bereich des NPOG ein weitgehend einheitliches Regelungssystem für den Datenschutz zu schaffen, das insbesondere dazu beiträgt, Vollzugsdefiziten aufgrund der Abgrenzungsschwierigkeiten zwischen Verordnung und Richtlinie entgegenzuwirken.

Damit transparent wird, welche Vorschrift im NPOG als spezifische Bestimmung welches Artikels der DS-GVO zu verstehen ist, wird dies bei der jeweiligen Vorschrift in der Begründung angegeben.

Insgesamt wird zur Abgrenzung des Anwendungsbereichs der Rechtsregime der DS-RL und der DS-GVO für den gefahrenabwehrrechtlichen Aufgabenbereich im Grundsatz von Folgendem ausgegangen:

Der Bereich der Gefahrenabwehr wird in Ansehung der praxisrelevanten Konstellationen nahezu ausschließlich beziehungsweise ganz überwiegend dem Anwendungsbereich der DS-RL und somit den angepassten Datenschutzbestimmungen des NPOG sowie ergänzend des zweiten Teils des NDSG zuzurechnen sein. Entsprechend Artikel 1 Abs. 1 der DS-RL enthält diese „Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“.

Die Erwägungsgründe 11 ff. zur DS-RL enthalten nähere Erläuterungen zur Auslegung der Definition. Selbst wenn beim Handeln zur Gefahrenabwehr nicht bereits von vorherein klar die Verhütung von Straftaten als Zweck oder Ergebnis feststeht, besteht nahezu immer zumindest die Möglichkeit, dass die Gefahrenlage zu einer Straftat führen kann, beziehungsweise dass dies nicht ausgeschlossen ist.

Zu Nummer 1 (§ 2):

Zu Buchstabe a:

In § 2 wird mit der neuen Nummer 15 der Begriff der Vorfeldstraftat in das NPOG eingeführt und definiert, wie er im Sinne dieses Gesetzes zu verstehen ist.

Mit dieser und den weiteren Änderungen in den §§ 34 und 37 werden Vorgaben aus dem Beschluss des Bundesverfassungsgerichts vom 9. Dezember 2022 (1 BvR 1345/21) zu Eingriffsschwellen beim Einsatz besonderer Mittel der Datenerhebung bei Vorfeldstraftatbeständen umgesetzt.

Ergänzend wird auf die Ausführungen zu § 34 Abs. 1 Satz 1 Nr. 2 Buchst. a verwiesen.

Zu Buchstabe b:

Es handelt sich um eine redaktionelle Folgeanpassung.

Zu Nummer 2 (Änderungen Dritter Teil)

Zu Buchstaben a und b (Überschriften):

Mit diesem Gesetzentwurf soll die Systematik des Gesetzes verbessert werden, um mehr Übersichtlichkeit zu erreichen. Dazu werden neue Überschriften eingefügt und bestehende Überschriften geändert oder ergänzt. Der „Dritte Teil“ enthält neben dem 1. Abschnitt „Allgemeine und besondere Befugnisse“ auch die „Befugnisse zur Datenverarbeitung“ im 2. Abschnitt. Dieser 2. Abschnitt soll aufgrund seiner Bedeutung ein eigenständiger Teil des Gesetzes werden und weitere Überschriften erhalten. Daher muss die Überschrift des dritten Teils geändert werden. Da im dritten Teil nur noch die allgemeinen und besonderen Befugnisse verbleiben, erhält dieser Teil die Überschrift „Allgemeine und besondere Befugnisse der Verwaltungsbehörden und der Polizei“. Eine Gliederung dieses Teils ist nach Herauslösung der „Befugnisse zur Datenverarbeitung“ nicht mehr erforderlich, sodass die Überschrift „1. Abschnitt Allgemeine und besondere Befugnisse“ gestrichen werden kann.

Zu Buchstabe c (§ 12):

Bei der Regelung zur Befragung in § 12 ist eine Anpassung der in Absatz 5 Satz 1 vorgesehenen Hinweis- und Unterrichtungspflichten erforderlich. Die im Zuge der Änderung des NDSG vom 16. Mai 2018 geschaffene Regelung zum Hinweis auf das Auskunftsrecht wird im Sinne einer redaktionellen Vereinheitlichung gestrichen. Grund hierfür ist, dass Informationspflichten bei der Befragung vorgesehen sind, die sich mit den geltenden Informationsverpflichtungen nach dem NDSG und der DS-GVO überschneiden. Um dies auszuräumen, wird dieser Teil des Absatzes 5 Satz 1 gestrichen.

Die Verpflichtung zum Hinweis auf eine gegebenenfalls bestehende Freiwilligkeit bei der Auskunft soll hingegen sowohl für die Verwaltungsbehörden als auch für die Polizei beibehalten werden, weil sie über die europarechtliche Informationspflicht hinausgeht.

Zu Buchstaben d und e (§§ 15, 15 a):

Zur Schaffung einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts wird in § 15 a zu Artikel 9 Abs. 2 Buchst. g DS-GVO eine spezifische Bestimmung im Sinne des Artikels 6 Abs. 2 und 3 jeweils in Verbindung mit Absatz 1 Buchst. e der DS-GVO geschaffen.

Molekulargenetische Untersuchungen nach § 15 a stellen eine Verarbeitung besonderer Kategorien von Daten im Sinne des Artikels 10 der DS-RL bzw. Artikel 9 der DS-GVO dar. Der Begriff der „Datenverarbeitung“ ist nach Artikel 3 Nr. 2 der DS-RL und Artikel 4 Nr. 2 der DS-GVO der Oberbegriff für alle Schritte des Umgangs mit personenbezogenen Daten. Er umfasst das Speichern, Verändern und Verwenden ebenso wie die Datenerhebung.

Nach Artikel 10 DS-RL ist eine Verarbeitung dieser besonderen Daten nur zulässig, wenn sie „unbedingt erforderlich“ ist. Eine Legaldefinition dieses Begriffs findet sich weder in Artikel 10 DS-RL noch

dem dazugehörigen Erwägungsgrund (EG) 37. Aus EG 37 der DS-RL lässt sich jedoch schließen, dass es keinerlei weniger eingriffsintensive und mit vertretbarem Aufwand durchführbare Alternativmaßnahmen zur Zweckerreichung geben darf. Diese Auslegung des Begriffs „unbedingt erforderlich“ ist gleichzusetzen mit der Bedeutung des im NPOG bereits verwendeten Begriffs „unerlässlich“. Insofern soll im Interesse eines einheitlichen Sprachgebrauchs der Begriff „unerlässlich“, wie auch schon in § 25 Abs. 3 NDSG, bei der Verarbeitung besonderer Kategorien von Daten Verwendung finden. Aus diesem Grund kann auch dem Vorschlag des LfD, zur Vermeidung von begrifflichen Ungenauigkeiten die Formulierung „unbedingt erforderlich“ zu verwenden, nicht gefolgt werden. Die Vorgabe aus der DS-RL wird mit der Änderung in § 15 a umgesetzt.

Die ebenfalls mit dem Begriff „unerlässlich“ inhaltsgleiche Formulierung „auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist“ in § 15 wird im Interesse eines einheitlichen Sprachgebrauchs ebenfalls durch den Begriff „unerlässlich“ ersetzt.

Zu Buchstabe f (§ 17 a):

Die Arbeit mit Täterinnen und Tätern ist ein wichtiger Baustein der vernetzten Intervention bei Häuslicher Gewalt, sowohl im Kontext des Opferschutzes als auch im Hinblick auf die Prävention von Gewalt in zukünftigen Beziehungen. Die Übermittlung von personenbezogenen Daten von Täterinnen bzw. Tätern an Stellen für Täterinnen- bzw. Täterarbeit durch die Polizei erfolgt bislang grundsätzlich mit Einverständnis der Betroffenen.

Es darf für Opfer innerhalb Niedersachsens indes nicht vom Zufall respektive dem Einverständnis der Täterin oder des Täters in die Datenübermittlung abhängen, inwiefern Maßnahmen zu ihrem Schutz ergriffen werden (können) oder ob im Rahmen ganzheitlicher Prävention, wie z. B. durch die Übermittlung des Angebots sozialer Trainingskurse/Gefährderansprachen durch die Stellen für Täterinnen- bzw. Täterarbeit an die Adressaten, weitere Gefahren für die Allgemeinheit von einer Person ausgehend abgewendet werden können.

Um ein einheitliches Vorgehen in Niedersachsen bei der Übermittlung von Daten an eine geeignete Stelle für Täterinnen- bzw. Täterarbeit sicherzustellen, werden die bislang in Absatz 1 Satz 4 bis 6 getroffenen Regelungen über die Unterrichtung sowie zur Datenübermittlung an dieser Stelle gestrichen und aus systematischen Gründen für die betroffene Person in einem neuen Absatz 4 sowie für die gefährdete Person in einem neuen Absatz 5 neu gefasst.

Zu Absatz 4:

Satz 1 entspricht inhaltlich dem bisherigen Absatz 1 Satz 4. Der neue Satz 2 regelt, dass die Polizei personenbezogene Daten der Täterin oder des Täters künftig auch ohne deren Einwilligung an geeignete Beratungsstellen (Stellen für Täterinnen- bzw. Täterarbeit in Niedersachsen) übermitteln kann, damit diese ein Beratungsangebot unterbreiten können. An die Erforderlichkeit zur Abwehr einer Gefahr wird die Datenübermittlung hier - anders als bei der nunmehr in Absatz 5 geregelten Übermittlung von Daten der gefährdeten Person - nicht geknüpft. Der mit der Datenübermittlung verbundene Eingriff in das Recht auf informationelle Selbstbestimmung der Person, von der die Gefahr ausgeht, ist immer schon dann gerechtfertigt, wenn zumindest die Möglichkeit besteht, dass die fachlich fundierte Kontaktaufnahme durch eine Beratungsstelle zur Reduzierung einer verbleibenden Gefährdung beitragen kann. Der LfD hat zu dieser Vorschrift empfohlen, anstatt des Begriffs der „Einwilligung“ den Begriff des „Einverständnisses“ zu verwenden. Aus Gründen der Einheitlichkeit ist jedoch der auch sonst im NPOG verwendete Begriff der „Einwilligung“ vorzugswürdig.

Der NANV hat gegen diese Regelung insbesondere unter dem Gesichtspunkt der Geeignetheit Bedenken geäußert und Regelungen zur Weiterverarbeitung und Löschung der übermittelten Daten gefordert. Die Kritik des NANV wird nicht geteilt. Einer gesetzlichen Pflicht zur Wahrnehmung des Beratungsangebotes bedarf es nicht als Voraussetzung für die Einführung der Übermittlungsvorschrift. Bei nicht mitwirkungswilligen Personen besteht bei einer Kontaktaufnahme durch eine Beratungsstelle die Möglichkeit, dass die Bereitschaft zur Annahme von Angeboten erst geweckt wird.

Für die Weiterverarbeitung der Daten durch die Beratungsstellen bieten die Regelungen der DSGVO i. V. m. dem NDSG einen ausreichenden Rahmen. Der Zweck der Datenübermittlung wird in Satz 2 hinreichend bestimmt. Die Löschung der Daten richtet sich nach dem Grundsatz der Zweckbindung und ist dann erforderlich, sobald der Zweck, für den sie erhoben wurden, nicht mehr besteht. Insofern

besteht abseits der allgemeinen Grundsätze der Datenverarbeitung kein weiteres Regelungserfordernis.

Zu Absatz 5:

Der neue Absatz 5 entspricht inhaltlich dem bisherigen Absatz 1 Satz 5 und 6.

Zu Buchstabe g (§ 17 c):

Zu Doppelbuchstabe aa:

Der Anstieg der Fallzahlen der häuslichen Gewalt in Niedersachsen verdeutlicht, dass es einer landesrechtlichen präventivpolizeilichen Regelung für die Anordnung einer elektronischen Aufenthaltsüberwachung („elektronische Fußfessel“) im Kontext Häusliche Gewalt bedarf. Zugleich handelt es sich um eine Ausweitung der möglichen polizeilichen Maßnahmen im Bereich der häuslichen Gewalt, wonach bislang insbesondere Maßnahmen nach § 17 a (Wegweisung und Aufenthaltsverbot bei häuslicher Gewalt) in Betracht gekommen sind.

Regelungsstandort ist § 17 c NPOG, der bereits die Anordnungsgrundlagen für die Kontrolle des Aufenthalts von Gefährdern des Terrorismus und der organisierten Gewaltkriminalität vorsieht (siehe Absatz 1 Nrn. 1 und 2). § 17 c NPOG soll nunmehr um die Möglichkeit ergänzt werden, auch im Bereich der häuslichen Gewalt den Einsatz einer elektronischen Aufenthaltsüberwachung anordnen zu können.

Nach Absatz 1 Satz 2 kommt die Anordnung einer elektronischen Aufenthaltsüberwachung in Betracht, wenn gegen die betroffene Person eine Maßnahme nach § 17 a getroffen wurde oder eine richterliche Anordnung nach § 1 des Gesetzes zum zivilrechtlichen Schutz vor Gewalttaten und Nachstellungen ergangen ist und die Überwachung sowie die Erhebung, Speicherung, Veränderung und Nutzung der Daten zur Abwehr einer Gefahr für Leib, Leben, Freiheit oder die sexuelle Selbstbestimmung der gefährdeten Person erforderlich ist. Dies kann z. B. der Fall sein, wenn in Fällen häuslicher Gewalt die Anordnungen nach § 17 a NPOG nicht zum Erfolg geführt haben bzw. von vornherein einer dauerhaften Überwachung bedürfen.

Hierdurch soll das Eindringen einer Person in einen räumlichen Schutzbereich des Opfers oder die Tatsache, dass diese Person sich dem Opfer annähert, sofort und so rechtzeitig durch die Polizei festgestellt werden können, dass Maßnahmen zum Schutz des Opfers eingeleitet werden können. Es ist Aufgabe des Staates und seiner Einrichtungen, Präventivmaßnahmen zu ergreifen, um einen Menschen zu schützen. Wurde Gewalt ausgeübt oder in massiver Weise angedroht, bedarf es einer entsprechenden polizeilichen Befugnisnorm.

Gerade in Fällen häuslicher Gewalt stellt die elektronische Aufenthaltsüberwachung eine geeignete Maßnahme zum Schutz von bedeutenden Rechtsgütern wie Leben, Gesundheit, Freiheit oder sexuelle Selbstbestimmung dar. Es handelt sich bei der Maßnahme der elektronischen Aufenthaltsüberwachung jedoch auch um eine besonders eingriffsintensive Maßnahme der Datenverarbeitung, die notwendigerweise offen erfolgt.

Wie bereits bei den bisherigen Anordnungsgründen bedarf auch diese Maßnahme grundsätzlich einer richterlichen Anordnung (siehe § 17 c Abs. 3); lediglich unter den Voraussetzungen des § 17 c Abs. 4 kann eine Anordnung ohne vorherige rechtliche Anordnung ergehen.

An der Regelung in Absatz 1 Satz 2 beanstandet der LfD, dass die gewählte Eingriffsschwelle zu niedrig gewählt sei, und fordert eine Angleichung an § 17 a NPOG (Wegweisung und Aufenthaltsverbot bei häuslicher Gewalt), welcher eine gegenwärtige Gefahr für Leib, Leben, Freiheit oder die sexuelle Selbstbestimmung als Eingriffsschwelle vorsieht. Eine solche Angleichung ist jedoch nicht erforderlich. So dient die elektronische Aufenthaltsüberwachung der Überwachung u. a. von Maßnahmen nach § 17 a NPOG. Demnach handelt es sich bei den Maßnahmen der Aufenthaltsüberwachung über eine nachfolgende Maßnahme zu der Anordnung nach § 17a NPOG, sodass aufgrund der Verweisung in diesen Fällen ohnehin eine gegenwärtige Gefahr als Eingriffsvoraussetzung vorliegen muss. Der Auffassung des LfD, es handele sich bei der eAÜ nach § 17 c Abs. 1 Satz 2 im Vergleich zu § 17 a unter Umständen um eingriffsintensivere Maßnahmen, ist ebenfalls zu widersprechen. Wegweisungen sowie Aufenthaltsverbote stellen vielmehr andersartige Eingriffe dar, die im Einzelfall deutlich schwerwiegendere Grundrechtseingriffe nach sich ziehen können.

Die Verpflichtung zum Mitführen eines technischen Mittels zur Kontaktaufnahme, insbesondere eines Mobiltelefons, soll zukünftig gemäß Absatz 1 Satz 3 in allen Fällen einer elektronischen Aufenthaltsüberwachung zum Zweck der Gefahrenabwehr gelten. Demnach können dem Betroffenen im Zuge eines zeitnahen Erstkontakts mögliche Verstöße gegen Anordnungen und deren Konsequenzen aufgezeigt werden. Zugleich kann darüber hinaus dem Betroffenen auch technische Unterstützung gewährt werden.

Zu Doppelbuchstabe bb:

Nach § 17 c Abs. 2 Satz 1 kann der gefährdeten Person mit deren Zustimmung ein technisches Mittel zur Verfügung gestellt werden, das etwaige Zuwiderhandlungen des Täters gegen Maßnahmen nach § 17 a NPOG oder gegen richterliche Anordnungen nach § 1 GewSchG anzeigt.

Hierbei handelt es sich um ein Zwei-Komponenten-Modell, welches bereits in anderen europäischen und nicht europäischen Ländern zur Anwendung kommt. Wesentliche Voraussetzung für die Durchführung einer solchen Maßnahme ist, dass die gefährdete Person der Maßnahme ausdrücklich zustimmt.

Diese Maßnahme hat besondere Relevanz bezüglich der Abstandsgebote insbesondere bei Maßnahmen nach § 17 a NPOG oder dem GewSchG. Es wird ein Alarm ausgelöst und die gefährdete Person informiert, insbesondere, wenn die Distanz zwischen Täter und gefährdeter Person eine festgelegte Entfernung unterschreitet. Ziel dieser Regelung ist, neben der Polizei auch die gefährdete Person frühzeitig über Zuwiderhandlungen des Täters zu informieren und das Opfer so in die Lage zu versetzen, ergänzend gegebenenfalls eigene Schutzmaßnahmen zu ergreifen.

Darüber hinaus ist es nach Absatz 2 Satz 2 auch möglich, dass das technische Gerät, welches die gefährdete Person bei sich führt, Verstöße des Gefährders gegen die Verpflichtung nach Absatz 1 Satz 2, wonach das elektronische Überwachungsgerät stets in betriebsbereiten Zustand bei sich zu führen ist, anzeigt. Im Falle eines - auch ohne Zutun des Gefährders eingetretenen - Ausfalls des Sendersignals kann eine frühzeitige, automatisierte Benachrichtigung der gefährdeten Person ermöglicht werden. Die Einrichtung einer entsprechenden Funktion des technischen Gerätes ist aufgrund der Ausgestaltung der Regelung als Ermessensvorschrift für die zuständige Behörde nicht verpflichtend.

Der LfD regt zudem an, die Regelungen zum Zwei-Komponenten-Modell bezüglich der Anforderung an die Informiertheit der Entscheidung sowie die Möglichkeit des Widerrufs zu ergänzen. Dem ist jedoch entgegenzuhalten, dass die betroffene gefährdete Person künftig alleine aufgrund der technischen Lösung vorab umfangreich über die folgende Maßnahme sowie die damit einhergehenden Verfahren zu informieren ist. Im Rahmen dieses Informationsgesprächs wird die betroffene Person ebenso informiert, dass jederzeit ein Widerruf der Zustimmung erfolgen kann und mithin die Maßnahme in diesem Falle unverzüglich beendet wird. Eine gesetzliche Regelung hierzu ist nicht erforderlich.

Zu Doppelbuchstabe cc:

Es handelt sich um eine redaktionelle Folgeanpassung.

Zu Doppelbuchstabe dd:

Zu Dreifachbuchstabe aaa:

Zu Vierfachbuchstabe aaaa:

Hierbei handelt es sich um eine Folgeanpassung zur Ausweitung der Anordnungsmöglichkeit der elektronischen Aufenthaltsüberwachung auf die Fälle häuslicher Gewalt, dass die dort gewonnenen Daten auch zur Feststellung von Verstößen gegen eine Wegweisung oder Aufenthaltsverbot nach § 17 a sowie zur Feststellung von Verstößen gegen eine Anordnung nach dem Gesetz zum zivilrechtlichen Schutz vor Gewalttaten und Nachstellungen verarbeitet werden dürfen.

Zu Vierfachbuchstabe bbbb:

Es handelt sich um eine redaktionelle Folgeanpassung.

Zu Dreifachbuchstabe bbb:

Absatz 2 Satz 5 enthält die Vorgabe, dass die Verarbeitung der Daten in gewissen Fällen (u. a. zur Feststellung von Verstößen gegen eine Aufenthaltsvorgabe oder ein Kontaktverbot nach § 17 b) automatisiert zu erfolgen hat. Dies soll nunmehr auch für die ergänzten Anwendungsfälle (siehe Nummern 2 und 3) erfolgen.

Zu Dreifachbuchstabe ccc:

Satz 12 regelt die Verarbeitung der Daten des einer gefährdeten Person zur Verfügung gestellten Mittels, wenn das Zwei-Komponenten-Modell zur Anwendung kommt. Der LfD hat in seiner Stellungnahme eine Beschränkung der Verarbeitung dieser Daten gefordert. Daher werden die Nutzung der Aufenthaltsdaten zu anderen Zwecken als dem Schutz dieser Person sowie die Erstellung von Bewegungsbildern ausdrücklich ausgeschlossen.

Zu Doppelbuchstabe ee:

Absatz 4 enthält einen Richtervorbehalt für die Anordnung der elektronischen Aufenthaltsüberwachung. Der NANV hat angeregt, den Inhalt der gerichtlichen Anordnung auch auf die Art und Weise der Überwachung, den Umfang und die Speicherdauer der Bewegungsbilder und die Einzelheiten der Überlassung des Ortungsgerätes und seine technischen Möglichkeiten auszudehnen. Bereits im Antrag der Polizei an das Amtsgericht sind jedoch gemäß § 17c Abs. 3 S. 2 Nr. 2 Art, Umfang und Dauer der Maßnahme anzugeben, sodass das zuständige Amtsgericht bereits Kenntnis über diese Umstände hat und diese in die Entscheidung mit einfließen lassen kann.

Zu Dreifachbuchstabe aaa:

Hierbei handelt es sich um eine Folgeanpassung zur Ausweitung der Anordnungsmöglichkeit der elektronischen Aufenthaltsüberwachung auf die Fälle häuslicher Gewalt, dass die Angabe, ob die betroffene Person einer Wegweisung oder einem Aufenthaltsverbot nach § 17 a oder einer Anordnung nach dem Gesetz zum zivilrechtlichen Schutz vor Gewalttaten und Nachstellungen unterliegt, auch im Antrag der Polizei zu erwähnen ist.

Zu Dreifachbuchstabe bbb:

Es handelt sich um eine redaktionelle Folgeanpassung.

Zu Doppelbuchstabe ff:

Es handelt sich um eine redaktionelle Folgeanpassung.

Zu Buchstabe h:

Die Befugnisse zur Datenverarbeitung, die bisher ein Abschnitt des dritten Teils des Gesetzes sind, werden aufgrund der Bedeutung dieser Vorschriften zu einem eigenständigen vierten Teil. Gleichzeitig wird dieser Teil durch die Einfügung von Unterabschnitten weiter systematisiert. Die §§ 30 bis 31 a werden zu einem ersten Abschnitt mit der Überschrift „Datenerhebung“.

Zu Nummer 3 (Überschriften):

Auf die Begründung zu Nummer 2 Buchst. h wird verwiesen.

Zu Nummer 4 (§ 30):

Zu Buchstabe a:

Mit der Änderung wird ausdrücklich klargestellt, dass nicht nur bei dritten Personen, sondern bei Vorliegen der Voraussetzungen auch bei Behörden oder sonstigen öffentlichen Stellen Daten erhoben werden dürfen.

Zu Buchstabe b:

Die Verweisung auf den ursprünglich in § 32 Abs. 5 geregelten Einsatz von automatisierten Kennzeichenlesesystemen wird an den neuen Standort der Vorschrift angepasst.

Zu Buchstabe c:

In Absatz 3 wird der dort verwendete Begriff der „Datei“ durch den neuen europarechtlichen Begriff des „Dateisystems“ angepasst, Artikel 3 Nr. 6 DS-RL und Artikel 4 Nr. 6 DS-GVO.

Zu Buchstabe d:

Die Absätze 4 bis 7, in denen die Benachrichtigung geregelt ist, werden an dieser Stelle gestrichen. Die Benachrichtigung erhält aufgrund ihrer Bedeutung mit § 46 a (neu) eine eigenständige Rechtsgrundlage und wird grundlegend überarbeitet.

Zu Nummer 5 (§ 31):

Zu Buchstabe a:

Bei der Einfügung des Wortes „kann“ statt des Wortes „darf“ handelt es sich um eine redaktionelle Angleichung an die in diesem Gesetz üblicherweise verwendeten Begrifflichkeiten.

Mit der Einfügung des Begriffs der verschiedenen Kategorien betroffener Personen wird ausdrücklich klargestellt, dass mit dieser bereits bestehenden Regelung Artikel 6 DS-RL im NPOG umgesetzt wird. Gleichzeitig wird im Interesse einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts zu Artikel 5 Abs. 1 Buchst. a, b und e DS-GVO eine spezifische Bestimmung im Sinne des Artikels 6 Abs. 2 und 3 jeweils in Verbindung mit Absatz 1 Buchst. e DS-GVO geschaffen.

Eine Änderung der bestehenden Kategorisierung in den Nummern 1 bis 5 ist nicht erforderlich. Die in Artikel 6 DS-RL aufgenommenen beispielhaften Kategorien finden sich bereits in der aktuellen Fassung des § 31 Abs. 2 Nrn. 1 bis 5.

Zu Buchstabe b:

Mit dem neu eingefügten Absatz 5 wird für die Verwaltungsbehörden und die Polizei sowohl im Anwendungsbereich der DS-GVO als auch der DS-RL geregelt, unter welchen Voraussetzungen die Erhebung von besonderen Kategorien personenbezogener Daten erlaubt ist. Im Anwendungsbereich der DS-GVO dient die Regelung der Schaffung einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts und enthält zu Artikel 6 Abs. 1 Buchst. e und Artikel 9 Abs. 2 Buchst. g DS-GVO spezifische Bestimmungen im Sinne des Artikels 6 Abs. 2 und 3 jeweils in Verbindung mit Absatz 1 Buchst. e der DS-GVO. Im Verhältnis zu § 25 Abs. 3 NDSG, der eine allgemeine Norm zur Verarbeitung besonderer Kategorien personenbezogener Daten enthält, ist der neue § 31 Abs. 5 die fachspezifische abschließende Norm, sodass ein Rückgriff auf § 25 Abs. 3 NDSG nicht in Betracht kommt.

Der Begriff der „besonderen Kategorien personenbezogener Daten“ ist in § 24 Nr. 13 NDSG definiert. Wie sich aus § 49 (neu) ergibt, soll diese Definition auch für Maßnahmen nach dem NPOG einschlägig sein.

In Absatz 5 wird eine weitere Schwelle eingezogen, wodurch die Verarbeitung nur zulässig ist, wenn sie „unerlässlich“ ist. Auf die Ausführungen zu § 15 und § 15 a wird verwiesen.

Der LfD hat angemerkt, dass Artikel 10 der DS-RL für die Verarbeitung besonderer Kategorien von Daten besondere Schutzvorkehrungen für die Freiheiten und Rechte der betroffenen Personen verlange. Diese sind indes nicht in § 31 zu regeln, der sich ausschließlich mit den Voraussetzungen für die Datenerhebung befasst, sondern sind Gegenstand der Regelungen über die Weiterverarbeitung von Daten sowie über technischen und organisatorische Sicherungen nach dem NDSG.

Zu Nummer 6 (Überschrift):

Nach § 31 a wird ein neuer 2. Abschnitt mit der Überschrift „Besondere Befugnisse und Maßnahmen der Datenerhebung“ eingeführt, an den sich die besonderen eingriffsintensiven und teilweise verdeckten Befugnisse und Maßnahmen anschließen.

Zu Nummer 7 (§ 32 Abs. 4):

In § 32 Abs. 4 wird eine neue Rechtsgrundlage für bestimmte Arten der intelligenten Videoüberwachung geschaffen. Der bisherige Absatz 4 wird in einen neuen § 32 a verschoben.

Aufgrund der anhaltend hohen Bedrohungslage durch Terrorismus, gewaltbereiten Extremismus und organisierte Kriminalität bedarf es neuer gesetzlicher Grundlagen für den Einsatz moderner technischer Einsatzmittel. In dem neuen Absatz 4 soll eine spezielle Rechtsgrundlage für den Einsatz „intelligenter Videoüberwachung“ geschaffen werden. Durch die intelligente Videoüberwachung in der vorliegend geregelten Form soll unter Einsatz der erforderlichen technischen Mittel die Erkennung

von Mustern bezogen auf Gegenstände und Personen ermöglicht werden. Auf Grundlage dieser Regelung können die gemäß den Absätzen 1 bis 3 angefertigten Bildaufzeichnungen automatisch ausgewertet werden.

Aufgrund der Verweisung auf die Absätze 1 bis 3 ist der Einsatz der intelligenten Videoüberwachung nur an Orten möglich, an denen auch eine konventionelle Videoüberwachung unter den genannten Voraussetzungen zulässig ist. Durch die vorliegende Regelung wird keine Ermächtigung für den Einsatz von Gesichtserkennungssoftware, insbesondere auch nicht in Form der Echtzeit-Fernidentifizierung, eingeführt.

Die automatisierte Auswertung des Bildmaterials erfolgt durch das Erkennen typischer Verhaltensmuster, die auf die Begehung von Straftaten hindeuten. Die Rechtsgrundlage ermöglicht aber auch das Erkennen bestimmter Muster von Objekten (beispielsweise alleinstehender Koffer). Ein wesentliches Merkmal der Auswertungstechnik ist ein hinterlegter Algorithmus, der die einzelnen Videosequenzen quasi in Echtzeit miteinander vergleicht und auffällige Verhaltens- bzw. Objektmuster erkennen bzw. kenntlich machen kann. Im Hinblick auf das Erkennen von Mustern bezüglich Personen darf es sich jedoch nur um solche Verhaltensmuster handeln, die auf die Begehung einer Straftat oder den Eintritt eines Unglücksfalls im Sinne von § 323 c Abs. 1 StGB hindeuten.

Gegenüber der konventionellen Videoüberwachung stellt die automatisierte Auswertung einen zusätzlichen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Dieser Eingriff ist jedoch verfassungsrechtlich gerechtfertigt. Die Verhütung von Straftaten stellt dabei ein legitimes Ziel der Maßnahme dar. Die automatisierte Auswertung des Bildmaterials ist ein geeignetes Mittel, um dieses Ziel zu erreichen. Sie ist auch zur Zielerreichung erforderlich. Die konventionelle Videoüberwachung stellt kein im unmittelbaren Vergleich zur intelligenten Videoüberwachung gleich geeignetes, milderes Mittel zur Zielerreichung dar. Zwar können durch die konventionelle Videoüberwachung ähnliche Ergebnisse erreicht werden. Die intelligente Videoüberwachung ist jedoch deutlich effektiver, da typische menschliche Ermüdungserscheinungen bei dauerhafter Überwachungstätigkeit durch intelligente Videoüberwachung minimiert werden. Um Ermüdungserscheinungen zu minimieren, ist erforderlich, dass das vorhandene Personal in möglichst kurzen Zeiträumen ausgetauscht wird. Durch den Einsatz der neuen Technik wird das vorhandene Personal hingegen dadurch entlastet, dass dieses nur noch in bestimmten „Alarmfällen“ tätig werden muss. In diesen Fällen wird die finale Entscheidung, ob ein Einschreiten erforderlich ist, unter Berücksichtigung der Systemmeldung nach wie vor von einem Menschen getroffen. Somit findet keine automatisierte Entscheidungsfindung im Einzelfall im Sinne von Artikel 11 Abs. 1 DS-RL statt. Um die gleichen Ergebnisse wie eine intelligente Videoüberwachungstechnik zu erreichen, wäre ein im Vergleich deutlich höherer Personaleinsatz mit kurzen Rotationszeiten erforderlich.

Die Rechtsgrundlage für den Einsatz der intelligenten Videoüberwachung ist auch angemessen. Durch den Einsatz der personenbezogenen Mustererkennung werden zwar auch Nichtstörer betroffen. Es ist jedoch zu beachten, dass die Maßnahme bereits durch die Beschränkung auf Bildaufzeichnungen nach Absatz 1 bis 3 umfassend inhaltlich eingeschränkt wird. Aufgrund dieser Verweisung ist der Einsatz nicht anlasslos und nur unter Einhaltung der vorgegebenen zeitlichen und örtlichen Beschränkungen möglich. Die Voraussetzungen für die konventionelle Videoüberwachung sind daher auch bei dem Einsatz der intelligenten Videoüberwachung einzuhalten.

Der Einsatz der intelligenten Videoüberwachung lässt in der vorliegend geregelten Form gegenüber der konventionellen Videoüberwachung keine erhöhte Eingriffsintensität erkennen. Die automatisierte Erkennung und Auswertung erfolgen gerade nicht auf Grundlage personenbezogener Merkmale, die für die Identifikation einzelner Personen genutzt werden, sondern aufgrund von Aktivitäten, Handlungen und körperlichen Reaktionen, die auf Gefahrensituationen hindeuten. Von den Personen, die sich im Aufnahmebereich der eingesetzten Kameras aufhalten, werden grundsätzlich nicht mehr Daten erfasst als im Falle der konventionellen Videoüberwachung. Es bedarf daher keiner weitergehenden Beschränkung der Eingriffsbefugnisse für die intelligente Videoüberwachung, wie sie vom LfD gefordert wird. Eine weitere Einschränkung der intelligenten Videoüberwachung etwa durch eine genauere Begrenzung der zu erfassenden Verhaltensmuster in Satz 2, wie sie die GdP und der NANV im Rahmen der Verbandsanhörung gefordert haben, ist ebenfalls nicht erforderlich.

Gemäß Satz 3 ist die automatisierte Erkennung und Auswertung der Bildaufzeichnungen nach Absatz 1 und 3 kenntlich zu machen. Im Rahmen von verdeckten Maßnahmen nach Absatz 2 ist dies nicht möglich, angesichts der höheren Eingriffsschwelle des Absatzes 2 aber auch gerechtfertigt. Eine Parallelregelung findet sich auch für die konventionelle Videoüberwachung in Absatz 3 Satz 2. Da es sich bei der automatisierten Erkennung und Auswertung um einen zusätzlichen Eingriff in das

Recht auf informationelle Selbstbestimmung handelt, ist auch auf diese Maßnahme gesondert hinzuweisen. Für den Bürger muss deutlich erkennbar sein, an welchen Orten er von der konventionellen bzw. von der intelligenten Videoüberwachung betroffen ist. Wie auch die bei der herkömmlichen Videoüberwachung angefertigten Aufnahmen werden die Auswertungsergebnisse gemäß Satz 4 nach spätestens sechs Wochen gelöscht, sodass es sich dabei um die Höchstspeicherfrist handelt. Satz 5 bestimmt die Dokumentation der Auswertungsergebnisse sowie deren Löschung.

Zu Nummer 8 (§§ 32 a bis 32 b):

Zu § 32 a:

Mit dem neuen § 32 a wird eine eigene Vorschrift für den Einsatz technischer Mittel, insbesondere am Körper getragener Bild- und Tonaufzeichnungsgeräte wie z. B. Bodycams, geschaffen und die Regelung um weitere Einsatzsituationen sowie die Möglichkeit des Einsatzes in Wohnungen erweitert.

Zu Absatz 1:

§ 32 Abs. 4 Satz 1 wird neuer § 32 a Abs. 1 Satz 1.

In den Sätzen 2 und 3 werden neue Einsatzszenarien geregelt, die insbesondere in Fällen relevant werden, in denen Einsatzkräfte Bodycams mit sich führen. Nach Satz 2 Nr. 1 sollen Bild- und Tonaufzeichnungen - insbesondere mittels Bodycam - gefertigt werden, wenn durch eine Polizeivollzugsbeamtin oder einen Polizeivollzugsbeamten unmittelbarer Zwang angedroht oder angewendet wird (Satz 2), da das Gefahren- und Eskalationspotenzial in einer solchen Situation besonders ausgeprägt ist. In Ausnahmefällen kann von einer Aufzeichnung abgesehen werden, wenn die konkreten Umstände des Einzelfalls dies nicht zulassen, z. B. wenn ein plötzlicher, unvorhersehbarer gewaltsamer Angriff auf die Beamtin oder den Beamten eine unmittelbare abwehrende Reaktion zur Eigensicherung erfordert und keinen zeitlichen Spielraum dafür bietet, die Bodycam zu aktivieren. Eine Ausgestaltung der Vorgabe in Absatz 1 Satz 2 als Ermessensvorschrift, wie vom LfD vorgeschlagen, ist hingegen nicht zielführend. Von der Bild- und Tonaufzeichnung in den dort geregelten Anwendungsbereichen ist nur im Ausnahmefall abzusehen. Zudem liegt ein möglichst umfassender Einsatz der Bodycam auch im Interesse der jeweils betroffenen Personen, da deren Nutzung der nachträglichen Aufklärung eines gegebenenfalls unübersichtlichen Einsatzgeschehens dienlich sein kann. Insofern sollte dann ein umfassender Einsatz der Bodycams forciert werden, wenn diese auch von den Einsatzkräften mit sich geführt werden.

Auch einfache Kontrollsituationen können schnell in eine lebensbedrohliche bis tödliche Gefahr umschlagen. Um Polizeivollzugsbeamtinnen und -beamte in Gefahrensituationen, die den Einsatz von Waffen beim unmittelbaren Zwang erfordern, zu entlasten und einen Zeitverzug zwischen manueller Auslösung der Kamera und Entnahme der Dienstpistole aus dem Holster zu vermeiden, soll ein automatisiertes Auslösen der Aufzeichnung ermöglicht werden, sobald die Pistole aus dem Holster gezogen wird (Satz 3). Dies kann z. B. in Form einer Holster-Signal-Nachrüstung erfolgen, die das Ziehen der Waffe nicht beeinflusst. Durch den Wegfall der manuellen Auslösung können Ablenkung und Zeitverlust in kritischen Einsatzsituationen vermieden werden, die eingesetzten Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten können sich vollständig auf die Abwehr der konkreten Gefahr konzentrieren.

Eine technisch automatisierte Auslösung ermöglicht zudem in derartigen Situationen den Kamera-Einsatz losgelöst von subjektiven Einschätzungen der Handelnden und damit ein größtmögliches Maß an Objektivität. Kommt es zum Einsatz der Schusswaffe, wird der Kamera-Einsatz auch immer verhältnismäßig sein.

Nach Satz 2 Nr. 2 sollen Bild- und Tonaufzeichnungen auch auf Verlangen der betroffenen Person ausgelöst werden. Den von polizeilichen Maßnahmen betroffenen Personen wird so die Möglichkeit eingeräumt, selbst eine Nachprüfbarkeit des weiteren polizeilichen Handelns herbeizuführen. Da Bild- und Tonaufzeichnungen nicht nur in das Recht auf informationelle Selbstbestimmung der das Verlangen äußernden betroffenen Person eingreifen, sondern auch Dritte sowie die Einsatzkräfte betroffen werden, beschränkt Satz 2 Nr. 2 das Recht, Bild- und Tonaufnahmen zu verlangen, auf polizeiliche Maßnahmen, die durch die Anwendung von unmittelbarem Zwang durchgesetzt werden können, in denen es also zur Anwendung von physischer Gewalt kommen kann. Dadurch wird eine Vergleichbarkeit der Einsatzsituationen mit den in Satz 1 und Satz 2 Nr. 1 geregelten Fälle gewährleistet.

Eine Pflicht zum Mitführen von Bild- und Tonaufzeichnungsgeräten sowie technischen Lösungen zum automatisierten Auslösen derselben wird durch Satz 2 und 3 nicht begründet. Die Rechtmäßigkeit der Anfertigung oder des Absehens von der Anfertigung von Bild- und Tonaufzeichnungen nach Satz 1 und 2 hat keine Auswirkungen auf die Rechtmäßigkeit der polizeilichen Maßnahmen, auf die sich die Aufzeichnung bezieht.

Zu Absatz 2:

§ 32 Abs. 4 Satz 2 bis 8 wird neuer § 32 a Abs. 2 Satz 1 bis 7.

Zu Absatz 3:

Der Einsatz von körpernah getragenen Aufnahmegeräten (Bodycams) hat sich seit ihrer Einführung durch Pilotprojekt im Jahre 2016 bewährt. Eine Regelung für den Einsatz von Bodycams in der Polizei wurde im Jahr 2019 in § 32 Abs. 4 geschaffen. Bodycams schützen sowohl Einsatzkräfte als auch Dritte gleichermaßen vor Gewalt und unzutreffenden Anschuldigungen. Der Einsatz der mobilen Bild- und Tonaufzeichnungsgeräte soll daher unter Gewährleistung der grundgesetzlichen Vorgaben künftig auch in Wohnungen zur Vermeidung besonders schwerer Straftaten ermöglicht werden. Der Einsatz der mobilen Bild- und Tonaufzeichnungsgeräte wie z. B. der Bodycam in Wohnungen ist aus polizeilicher Sicht auch notwendig, da gerade dort spezielle Gefahrensituationen vorherrschen können und es vermehrt zu Eskalationen kommen kann. Um die deeskalierenden Potenziale von mobilen Bild- und Tonaufzeichnungsgeräten zu nutzen, wird deren Einsatz in Wohnungen und im öffentlichen Raum zum Schutz von Polizeibeamtinnen und Polizeibeamten oder Dritten gegen eine dringende Gefahr für Leib und Leben erlaubt. Mit aufgenommen werden auch Regelungen zum Schutz des Kernbereichs der privaten Lebensgestaltung.

Beim Einsatz von mobilen Bild- und Tonaufzeichnungsgeräten in Wohnungen gilt es einerseits einem besonderen Bedürfnis der polizeilichen Praxis, andererseits aber auch dem insoweit gültigen Maßstab des Artikels 13 Abs. 7 GG beim Betreten von Wohnungen Rechnung zu tragen. Die Einsatzszenarien zwischen öffentlich zugänglichen Orten und Wohnungen, wozu auch Arbeits-, Betriebs- und Geschäftsräume gehören, sind bei grundsätzlich vergleichbaren Szenarien oftmals fließend. Häufig entwickeln sich Einsätze im Umfeld von Gaststätten, Einkaufszentren oder Diskotheken, die sich dann im weiteren Verlauf in diese hinein verlagern. Umgekehrt entstehen entsprechende Situationen auch in solchen Räumlichkeiten, die dann ihre Fortsetzung im öffentlichen Raum finden. Auch in Wohnräumen können mobile Bild- und Tonaufzeichnungsgeräte einen wichtigen Beitrag zum Schutz der Einsatzkräfte oder Dritter leisten. Gerade Einsatzsituationen im Zusammenhang mit häuslicher Gewalt bergen erfahrungsgemäß ein erhöhtes Gefahrenpotenzial für die eingesetzten Kräfte in sich. Die vorgefundene Aggression kann urplötzlich und ohne Vorwarnung umschwenken und sich gegen die eingesetzten Kräfte richten. Bei dem Einsatz von mobilen Bild- und Tonaufzeichnungsgeräten in Wohnungen handelt es sich dabei weder um eine verdeckte Maßnahme noch um die Überwachung von Wohnraum. Denn anders als beim verdeckten Einsatz von technischen Überwachungsmitteln in Wohnungen nach Artikel 13 Abs. 4 oder 5 GG durchbricht die offene Aufzeichnung in Gegenwart der Polizei den speziell geschützten Bereich nicht, sondern dokumentiert lediglich das Geschehen in dem durch die Polizeipräsenz bereits durchbrochenen Rahmen. Bei der Dokumentation des Geschehens handelt es sich zudem lediglich um eine Begleiterscheinung des Einsatzes, wobei der primäre Zweck der mobilen Bild- und Tonaufzeichnungsgeräte in der präventiven Deeskalation liegt. Schranke für diesen Eingriff in Artikel 13 GG ist deshalb allein Artikel 13 Abs. 7 GG, der - anders als von GdP und NANV vertreten - den Einsatz technischer Mittel nicht ausschließt. Wie die Formulierung „im Übrigen“ in Artikel 13 Abs. 7 GG zeigt, geht es um solche Beeinträchtigungen des Schutzbereichs, die weder eine Durchsuchung i. S. des Absatzes 2 noch den Einsatz technischer Mittel i. S. der Absätze 3, 4 und 5 darstellen. Dies ist grundsätzlich jedes körperliche Eindringen, Betreten, Besichtigen oder Verweilen staatlicher Organe in den bzw. im geschützten Bereich. Nach Artikel 13 Abs. 7, 3. Variante GG dürfen Eingriffe und Beschränkungen u. a. aufgrund eines Gesetzes zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung vorgenommen werden. Der Begriff der öffentlichen Sicherheit umfasst neben der Unverletzlichkeit der Rechtsordnung die subjektiven Rechte und Rechtsgüter des Einzelnen und damit auch die durch § 32 a Abs. 3 zu schützenden Rechtsgüter Leib und Leben. Ziel der Maßnahme darf nicht die Überwachung der Wohnung, sondern nur die Abwehr einer dringenden Gefahr für Leib oder Leben einer Person sein. Die verdeckte Wohnraumüberwachung richtet sich hingegen nach § 35 a NPOG. Weitere Voraussetzung nach Artikel 13 Abs. 7 GG ist, dass der Eingriff zur Verhütung einer „dringenden“ Gefahr erfolgt. Der Begriff der dringenden Gefahr bezieht sich sowohl auf das Ausmaß des drohenden Schadens als auch auf die Wahrscheinlichkeit des Schadenseintritts. Das Ausmaß des drohenden Schadens knüpft an die Hochrangigkeit des gefährdeten Rechtsguts an. Ob eine hinreichende

Wahrscheinlichkeit für den Schadenseintritt gegeben ist, entscheiden die handelnden Kräfte anhand der ihnen bekannten Umstände im Einzelfall. Gleichwohl ist der Schutz der Wohnung ausdrücklich zu betonen. Satz 1 setzt die Anforderungen des Artikels 13 Abs. 7 GG für die Fertigung von Bild- und Tonaufzeichnungen zum Schutz von Einsatzkräften oder Dritten um. Eines Richtervorbehalts bedarf es im Anwendungsbereich des Artikels 13 Abs. 7 GG nicht. Ein Einsatz der Bodycams in Wohnungen ist daher - entgegen der Auffassung des LfD, der GdP und des NANV - unter den Voraussetzungen des Artikel 13 Abs. 7 GG möglich.

Auch in Wohnungen kommt nach Satz 2 Absatz 1 Sätze 2 und 3 zur Anwendung, sodass auch hier Bild- und Tonaufzeichnungen bei Androhung und Anwendung unmittelbaren Zwanges - einschließlich der Möglichkeit einer automatisierten Auslösung bei Schusswaffengebrauch - sowie auf Verlangen der betroffenen Person gefertigt werden sollen. Durch den zweiten Halbsatz des Satzes 2 ist sichergestellt, dass eine betroffene Person den Einsatz nicht verlangen kann, wenn sie sich offenkundig selbst in Bezug auf die betroffene Örtlichkeit nicht auf das Grundrecht aus Artikel 13 des Grundgesetzes berufen kann oder wenn eine andere berechtigte Person die Aufzeichnung nicht akzeptiert.

Der LfD hat im Rahmen der Verbandsbeteiligung erneut Kritik am sogenannten „Pre-Recording“ geäußert, welches auch beim Einsatz von Bodycams in Wohnungen gemäß Absatz 3 Satz 2 und Absatz 2 Sätze 3 und 4 zur Anwendung kommt. Der LfD gab zu bedenken, dass durch die bis zu 30 Sekunden andauernde Aufnahme der Bodycam im Bereitschaftsbetrieb der geschützte Kernbereich privater Lebensgestaltung (Intimsphäre) insbesondere auch von unbeteiligten Dritten betroffen sein könnte und durch die Regelung die gefahrenabwehrrechtliche Zweckbestimmung letztlich nicht erreichbar sei. In vielen Fällen kann jedoch aufgrund der jeweiligen Einsatzsituation ein manuelles Einschalten erst zu einem Zeitpunkt erfolgen, in welchem bereits wichtige Ereignisse nicht aufgezeichnet werden. Zudem wird das Eingriffsgewicht auch dadurch deutlich gemindert, dass aufgrund der Regelung in Absatz 2 Satz 4 die Aufnahme bereits nach 30 Sekunden automatisch gelöscht wird, sofern nicht in dieser Zeitspanne Aufzeichnungen nach Absatz 1 beginnen.

Darüber hinaus ist auch der Vorschlag des LfD, die in Absatz 3 Satz 2 in Verbindung mit Absatz 2 Satz 2 für den Einsatz von Bodycams erforderliche Kenntlichmachung auch auf den Bereich des Pre-Recordings auszudehnen, abzulehnen. Dies ist in Anbetracht des geringen Eingriffsgewichts nicht erforderlich und auch nicht praktikabel. Hier würden eher Missverständnisse und Unsicherheit gefördert, weil für die betroffenen Personen der Bedeutungsgehalt unterschiedlicher Kennzeichnungen für die echte, zu speichernde Aufzeichnung und für das nach 30 Sekunden gelöschte Pre-Recording nicht ersichtlich wäre.

Durch die Regelungen in den Sätzen 3 bis 7 wird der Schutz des Kernbereichs privater Lebensgestaltung gewährleistet. Von den offenen Bild- und Tonaufzeichnungen, die durch bereits in die Wohnung eingedrungene Einsatzkräfte gefertigt werden, wird der Kernbereich privater Lebensgestaltung nur ausnahmsweise betroffen sein. Ist dies aufgrund der Art der Räume und der Eigenart der vorgefundenen Situation doch der Fall, sind die Aufzeichnungen nach Satz 3 zu unterbrechen. Satz 4 regelt besondere Dokumentationspflichten für den Fall, dass eine eigentlich erforderliche Unterbrechung wegen einer Gefährdung von Leib oder Leben der eingesetzten Kräfte unterbleibt. Das weitere Verfahren regeln die Sätze 5 bis 7.

Bei Aufzeichnungen mit körpernah getragenen Aufnahmegeräten innerhalb der Wohnung ist nach Satz 8 die Verwertung zum Zweck der Gefahrenabwehr oder zur Überprüfung der Rechtmäßigkeit des aufgezeichneten polizeilichen Handelns künftig nur dann zulässig, wenn die Rechtmäßigkeit Bild- und Tonaufnahmen richterlich festgestellt wurde. Nicht die Maßnahme selbst unterliegt dem Richtervorbehalt, sondern nur die anschließende Verwertung der dort gefertigten Aufzeichnungen zu präventiven oder Kontrollzwecken. Für Zwecke der Strafverfolgung bestehen keine Beschränkungen. Satz 9 regelt das gerichtliche Verfahren.

Einer gesetzlichen Regelung zur Kennzeichnung der durch den Einsatz von Bodycams in Wohnungen erstellten Aufzeichnungen, wie vom LfD vorgeschlagen wurde, bedarf es nicht. Eine entsprechende Vorgabe kann gegebenenfalls auch in Form einer untergesetzlichen Regelung erfolgen.

Zu § 32 b:

In dem neuen § 32 b wird für die Polizei die Möglichkeit des Einsatzes der biometrischen Echtzeit-Fernidentifizierung geschaffen. In der Vorschrift sind die konkreten Voraussetzungen festgelegt, die einen rechtmäßigen Einsatz ermöglichen und insbesondere die verfassungsrechtlichen und europarechtlichen Vorgaben umfassend berücksichtigen. Die Echtzeit-Fernidentifizierung stellt für die

Polizei in Anbetracht stetig wachsender Datenmengen und komplexer werdender Sach- und Einsatzlagen ein zusätzliches Erkenntnismittel dar, um die zunehmend begrenzten menschlichen Erkenntnismöglichkeiten im digitalen Zeitalter ausgleichen zu können. Dabei ist jedoch stets die Entscheidung eines Menschen (sogenannter human in the loop) für weitere polizeiliche Maßnahmen maßgeblich. Im Rahmen einer Folgeabschätzung müssen auch die durch den Einsatz der Echtzeit-Fernidentifizierung berührten Grundrechte ausreichend berücksichtigt werden.

Auf Grundlage des bereits bestehenden § 32 ist die konventionelle Videoüberwachung an den in der Regelung näher benannten Orten auf Grundlage des bestehenden Rechtsrahmens möglich. Eine vollständige und ausreichend schnelle Auswertung des aufgenommenen Videomaterials ist jedoch aufgrund des personellen und zeitlichen Aufwandes und vor dem Hintergrund großer zu sichtender Datenmengen nicht möglich. Diese Problematik lässt sich durch den Einsatz von moderner Bildanalysesoftware auf Basis von KI entschärfen. Moderne Einsatzmittel, wie die biometrische Echtzeit-Fernidentifizierung, ermöglichen eine effektive Kontrolle von Brennpunktbereichen und eine frühzeitige Erkennung von Gefahren. Es ist daher zu erwarten, dass durch den Einsatz der biometrischen Echtzeit-Fernidentifizierung im Vergleich zur konventionellen Videoüberwachung die Begehung von Straftaten effektiver verhindert werden kann.

Die Regelung der biometrischen Echtzeit-Fernidentifizierung ist maßgeblich durch die bereits unmittelbar geltenden Vorgaben der KI-Verordnung (VO (EU) 2024/1689) determiniert. Diese sieht insbesondere in Artikel 5 Abs. 1 Satz 1 Buchst. h, Satz 2, Abs. 2 bis 7 KI-VO konkrete Regelungen zum Einsatz der biometrischen Echtzeit-Fernidentifizierung vor, die unmittelbar zur Anwendung kommen und als höherrangiges Recht einer nationalen Rechtsgrundlage vorgehen. Diese Regelungen sind daher auch zwingend beim Einsatz der biometrischen Echtzeit-Fernidentifizierung zu beachten. Welchen Inhalt eine nationale Ermächtigung für den Einsatz der biometrischen Echtzeit-Fernidentifizierung aufweisen muss, wird durch Artikel 5 Abs. 5 KI-VO näher bestimmt.

Welche KI-Anwendungen als biometrische Echtzeit-Fernidentifizierungssysteme der Vorschrift unterfallen ergibt sich unmittelbar aus der KI-VO. Gemäß Artikel 3 Nr. 42 KI-VO ist ein biometrisches Echtzeit-Fernidentifizierungssystem ein biometrisches Fernidentifizierungssystem, bei dem die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen und das zur Vermeidung einer Umgehung der Vorschriften nicht nur die sofortige Identifizierung, sondern auch eine Identifizierung mit begrenzten kurzen Verzögerungen umfasst. Ein biometrisches Fernidentifizierungssystem wiederum ist gemäß Artikel 3 Nr. 41 KI-VO ein KI-System, das dem Zweck dient, natürliche Personen ohne ihre aktive Einbeziehung und in der Regel aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren. Ein KI-System ist gemäß Artikel 3 KI-VO ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.

Der Einsatz der biometrischen Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zum Zwecke der Gefahrenabwehr ist nur in den in Artikel 5 Abs. 1 S. 1 Buchst. h) Ziffer i) und ii) KI-VO genannten Fallgruppen möglich. Nach dieser Regelung ist eine Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken erlaubt, wenn und insoweit dies im Hinblick auf eines der in Artikel 5 Abs. 1 Satz 1 Buchst. h KI-VO genannten Ziele unbedingt erforderlich ist. Die dort formulierten Fallgruppen werden in § 32 b aufgegriffen und entsprechend der Systematik des NPOG in nationales (Landes-)Recht übertragen.

Der LfD geht davon aus, dass Maßnahmen der Echtzeit-Fernidentifizierung im Rahmen einer Videoüberwachung Informationspflichten nach Artikel 13 der DS-RL auslösen, und leitet daraus angesichts der Unmöglichkeit einer individuellen Information sämtlicher betroffener Personen eine Kennzeichnungspflicht ab. Artikel 13 der DS-RL enthält jedoch keine Kennzeichnungspflichten für Maßnahmen mit einem großen Kreis an nicht gezielt betroffenen Personen, sondern regelt allgemeine und individuelle Informationspflichten gegenüber Einzelpersonen, die von spezifischen Maßnahmen der Datenverarbeitung betroffen sind. Eine Kennzeichnung von Maßnahmen der Echtzeit-Fernidentifizierung würde den Zielen der Maßnahme zuwiderlaufen und könnte dazu führen, dass sich gesuchte Personen gezielt aus den von den Kameras erfassten Bereichen fernhalten.

Maßnahmen der biometrischen Echtzeit-Fernidentifizierung unterliegen jedoch der Dokumentationspflicht nach § 48 Abs. 1. Dies gewährleistet ein möglichst hohes Maß an Transparenz, eine nachträgliche Überprüfung und eine effektive Selbstkontrolle.

Zu Absatz 1:

In Absatz 1 sind die Eingriffsschwellen geregelt, durch welche die materiellen Voraussetzungen für den Einsatz der biometrischen Echtzeit-Fernidentifizierung festgelegt werden. Die Eingriffsschwellen ergeben sich maßgeblich aus den Vorgaben in Artikel 5 Abs. 1 Satz 1 Buchst. h Ziffern i und ii KI-VO. In der Vorschrift sind die konkreten Tatbestandsvoraussetzungen enthalten, unter denen eine biometrische Echtzeit-Fernidentifizierung möglich ist.

Satz 1 ist dabei Ausfluss der in Artikel 5 Abs. 1 Satz 1 Buchst. h Ziffer ii KI-VO geregelten Fallgruppen. Die biometrische Echtzeit-Fernidentifizierung ist danach möglich zum „Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr eines Terroranschlags“.

Nach der in Landesrecht umgesetzten Vorschrift in Satz 1 Nr. 1 und 2 kann die Polizei zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person oder zur Abwehr einer Gefahr einer terroristischen Straftat bei Maßnahmen nach § 32 Abs. 1 bis 3 die biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zur gezielten Suche nach im Datenbestand der polizeilichen Auskunfts- und Fahndungssysteme gespeicherten Personen, die diese Gefahr verursachen, durchführen, soweit dies zur Abwehr dieser Gefahr unerlässlich ist. Ein Einsatz bei Vorliegen rein abstrakter oder weit in der Zukunft liegender Gefahren ist hingegen nicht möglich - etwa die allgemeine Gefahr islamistischer Anschläge auf Veranstaltungen wie Weihnachts- oder Ostermärkten. Eine andere Bewertung kann sich allerdings bei Vorliegen außergewöhnlich konkreter Terrorwarnungen ergeben, oder wenn aufgrund der Häufigkeit schwerer Straftaten eine hinreichend erhebliche Dauergefahr anzunehmen ist (*Wendehorst* in: Martini/ders., KI-VO, 1. Auflage 2024, Artikel 5 Rn. 155).

Eine gegenwärtige Gefahr ist in § 2 Nr. 2 definiert als eine Gefahr, bei der die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder bei der diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht. Im Gegensatz zur konkreten Gefahr wird bei dieser Gefahrenschwelle eine „geringere zeitliche Entfernung zwischen Maßnahmenzeitpunkt und schädigendem Ereignis verlangt“ (*Ullrich* in: Möstl/Weiner, BeckOK NPOG, 30. Edition, Stand: 01.04.2024, § 2 Rn. 74). Die terroristischen Straftaten sind in § 2 Nr. 15 definiert.

Der Einsatz der Maßnahme ist auch nach Satz 2 zur gezielten Suche nach im Datenbestand der polizeilichen Auskunfts- und Fahndungssysteme gespeicherten bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung und vermissten Personen zulässig. Bei dieser Regelung handelt es sich um die landesrechtliche Umsetzung des in Artikel 5 Abs. 1 S. 1 Buchst. h) Ziffer i) KI-VO definierten Anwendungsfalls.

Der Einsatz der biometrischen Echtzeit-Fernidentifizierung ist in Absatz 1 örtlich auf öffentlich zugängliche Räume beschränkt. Gemäß Artikel 3 Nr. 44 KI-VO bezeichnet ein öffentlich zugänglicher Raum einen einer unbestimmten Anzahl natürlicher Personen zugänglichen physischen Ort in privatem oder öffentlichem Eigentum, unabhängig davon, ob bestimmte Bedingungen für den Zugang gelten, und unabhängig von möglichen Kapazitätsbeschränkungen.

Das Einsatzmittel kann zudem nur im Zusammenhang mit Maßnahmen nach § 32 Abs. 1 bis 3 zur Anwendung kommen. Insofern sind auch die Voraussetzungen für eine der in § 32 Abs. 1 bis Abs. 3 geregelten Maßnahmen zu beachten.

Die biometrische Echtzeit-Fernidentifizierung kann zudem nur dann zum Einsatz kommen, soweit dieser auch zur Gefahrenabwehr unerlässlich ist.

Weiterhin sind bei dem Einsatz der biometrischen Echtzeit-Fernidentifizierung auch die Vorgaben in Artikel 5 Abs. 2 KI-VO einzuhalten. Vor Verwendung des Einsatzmittels ist insbesondere auch eine Folgenabschätzung im Hinblick auf betroffene Grundrechte vorzunehmen.

Der Einsatz der biometrischen Echtzeit-Fernidentifizierung ist allein zur gezielten Suche nach den in Absatz 1 genannten Personen zulässig und ist daher auf diesen Personenkreis konkret beschränkt. Der personelle Anwendungsbereich der Maßnahme wird durch den Wortlaut der Vorschrift daher

hinreichend bestimmt. Die gezielte Suche nach Dritten, die unter Umständen mit einem zu untersuchenden Sachverhalt in Zusammenhang stehen, aber nicht dem in Absatz 1 genannten Personenkreis unterfallen, wie dies etwa bei Zeuginnen und Zeugen oder Hinweisgeberinnen oder Hinweisgebern der Fall sein kann, ist von der Ermächtigung nicht abgedeckt und daher nicht zulässig. Aus diesem Grund sind auch entsprechende Bedenken des LfD, der personelle Anwendungsbereich der Norm sei uferlos, zurückzuweisen.

Zu Absatz 2:

Maßnahmen nach Absatz 1 bedürfen der Anordnung durch das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. Satz 1 stellt diese Maßnahmen unter einen Richtervorbehalt, der die in Artikel 5 Abs. 3 Unterabs. 1 KI-VO vorgegebenen Maßgaben berücksichtigt. Die Formulierung des Richtervorbehalts orientiert sich zudem an eingriffsintensiven Einsatzmitteln wie der Datenerhebung durch Überwachung der Telekommunikation in § 33 a Abs. 5. Im Rahmen seiner inhaltlichen Entscheidung hat das Amtsgericht insbesondere die in Artikel 5 Abs. 3 Unterabs. 2 KI-VO aufgeführten Voraussetzungen einzuhalten und bei seiner Prüfung zu berücksichtigen. Diese Voraussetzungen der KI-VO gelten unmittelbar und bedürfen keines weiteren Umsetzungsaktes.

Der Antrag der Polizei muss die in Satz 2 genannten Angaben beinhalten.

In Satz 3 und 4 werden die Inhalte der in Satz 2 Nr. 4 geforderten Begründung näher spezifiziert. Aus der Begründung müssen sich die wesentlichen Abwägungsgesichtspunkte für die Anwendung der Maßnahme ergeben. In diesem Kontext sind insbesondere einzelfallbezogen die bestimmten Tatsachen, die das Vorliegen der Voraussetzungen nach Absatz 1 begründen, und die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme in der Begründung darzustellen.

Satz 5 statuiert das Schriftformerfordernis für die Anordnung. Die Anordnung muss mindestens die in Satz 2 Nr. 1 und 2 bezeichneten Angaben sowie die wesentlichen Gründe enthalten. In Satz 7 wird auf die für die Entscheidung geltenden Maßgaben nach Artikel 5 Abs. 3 UAbs. 2 der KI-Verordnung (EU) 2024/1689 verwiesen. Zwar ist die Wiederholung aller oder einzelner Verordnungsbestimmungen im mitgliedstaatlichen Recht grundsätzlich verboten (sogenanntes Dopplungsverbot, vgl. EuGH, Urt. v. 07.02.1972 - C-39/72 -, juris Rn. 16 f., und Urt. v. 28.03.1985 - 272/83 -, juris Rn. 10 f.). Eine Ausnahme gilt jedoch dann, wenn die Wiederholung bestimmter Punkte für die Verständlichkeit erforderlich ist (vgl. EuGH, Urt. v. 28.03.1985 - 272/83 -, juris Rn. 26 f.). Da Satz 5 und 6 Anforderungen für die richterliche Anordnung enthalten, erscheint es geboten, in diesem Zusammenhang auch Artikel 5 Abs. 3 UAbs. 2 der Verordnung (EU) 2024/1689 in Bezug zu nehmen. Für das gerichtliche Verfahren gilt § 19 Abs. 4 entsprechend.

Der durch den LfD in seiner Stellungnahme geäußerten Kritik, es bleibe unklar, welche räumliche Reichweite und zeitliche Dauer die Anordnung der biometrischen Echtzeit-Fernidentifizierung durch das Amtsgericht habe, ist zu widersprechen. Eine räumliche Beschränkung der Anordnung besteht bereits durch die Bezugnahme auf Maßnahmen nach den § 32 Abs. 1 bis 3. Der Einsatz der biometrischen Echtzeit-Fernidentifizierung ist nur innerhalb der in der Vorschrift konkret genannten Örtlichkeiten möglich. Mithin ist ein Einsatz nur innerhalb der räumlichen Grenzen der konventionellen Videoüberwachung möglich. Eine räumliche Eingrenzung innerhalb des § 32 b ist daher nicht erforderlich. Die Dauer der Anordnung wird bereits durch Absatz 1 begrenzt, da der Einsatz der biometrischen Echtzeit-Fernidentifizierung nur so lange zulässig ist, wie die dort geregelten Voraussetzungen vorliegen und insbesondere die jeweils einschlägigen Gefahren- oder Verdachtslagen auch tatsächlich vorliegen.

Absatz 3:

Gemäß Satz 1 kann die Anordnung nach Absatz 2 Satz 1 bei Gefahr im Verzug auch durch die Polizei getroffen werden. Da § 33 a Abs. 6 Satz 3 bis 8 umfassende Regelungen für das konkrete Verfahren bei Vorliegen von Gefahr im Verzug trifft, kann die Vorschrift grundsätzlich für entsprechend anwendbar erklärt werden. Da in Artikel 5 Abs. 3 Unterabs. 1 Sätze 2 und 3 KI-VO jedoch teilweise abweichende Regelungen enthalten sind, sind die Vorgaben nur auf Grundlage modifizierender Maßgaben anzuwenden: Eine nachträgliche richterliche Bestätigung der Anordnung für die Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken ist in diesen Fällen spätestens innerhalb von 24 Stunden zu beantragen. Wenn die Anordnung gemäß § 33 a Abs. 6 Satz 6 außer Kraft tritt, ist die Verwendung der biometrischen Echtzeit-Fernidentifizierung mit sofortiger Wirkung einzustellen und alle Daten sowie die Ergebnisse und Ausgaben dieser Verwendung sind unverzüglich zu löschen.

Zu Absatz 4:

Nach Satz 1 besteht für die Einrichtung und wesentliche Änderung eines biometrischen Echtzeit-Fernidentifizierungssystems (Artikel 3 Nr. 42 KI-Verordnung) ein Behördenleitervorbehalt. In Satz 2 wird der Behördenleitung die Möglichkeit zur Delegation der Anordnungsbefugnis eingeräumt. Zusätzlich ist die oder der Landesbeauftragte für den Datenschutz vor der Einrichtung und wesentlichen Änderung eines Systems nach Satz 1 anzuhören. Bei Gefahr im Verzug kann auf eine Anhörung verzichtet werden. Die Anhörung ist jedoch im Anschluss an die Gefahrenlage unverzüglich nachzuholen.

Zu § 32 c:

Vor dem Hintergrund stetig steigender und kaum mehr überschaubarer Datenmengen in öffentlich zugänglichen Datenbanken bedarf es moderner technologischer Einsatzmittel, um die großen Datenbestände effektiv analysieren und nach relevanten Daten filtern zu können. Die alleinige manuelle Sichtung von öffentlichem Bild- und Stimmmaterial stellt dabei eine nicht mehr zeitgemäße polizeiliche Ermittlungsarbeit dar. Vielmehr bedarf es moderner technischer Instrumente zur effektiven Gefahrenabwehr. Der biometrische Datenabgleich stellt ein sinnvolles und zeitgemäßes Hilfsmittel für die Polizei dar. Der nachträgliche Abgleich biometrischer Daten von Gesichtern und Stimmen mit öffentlich zugänglichen Daten aus dem Internet zielt auf die Identifizierung und Lokalisierung insbesondere von Störern und Tatverdächtigen.

Unter einem biometrischen Abgleich im Sinne dieser Vorschrift ist die technisch gestützte Überprüfung der Übereinstimmung von biometrischen Signaturen mit dem Ergebnis einer Übereinstimmungsbewertung zu verstehen. Öffentlich zugänglich sind alle Daten, die von jedermann verwendet werden können. Als Beispiel sind Daten aus sozialen Medien zu nennen, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten.

Zwar ist es bereits nach bestehender Rechtslage möglich, öffentlich zugängliche Daten im Rahmen der allgemeinen polizeilichen Ermittlungsbefugnisse zu erheben. Vorliegend ergibt sich jedoch der spezialgesetzliche Regelungsbedarf daraus, dass der biometrische Datenabgleich mittels einer automatisierten Verarbeitung erfolgen soll. Aufgrund der besonderen Grundrechtsrelevanz automatisierter Datenverarbeitungsvorgänge ist für deren Einsatz auch eine entsprechende Rechtsgrundlage zu schaffen.

Sofern der Datenabgleich mittels eines KI-Systems im Sinne des Artikel 3 Nr. 1 KI-VO erfolgt, sind auch die Vorschriften der KI-Verordnung zu beachten. Gemäß Artikel 3 Nr. 34 KI-VO handelt es sich bei biometrischen Daten um *„mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, wie etwa Gesichtsbilder oder daktyloskopische Daten“*. Für den Vorgang des Datenabgleichs ist Artikel 5 Abs. 1 lit. e KI-VO zu beachten. Diese Vorschrift untersagt „*das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern*“ (sogenanntes Scraping). Nicht verboten ist hingegen im Umkehrschluss etwa die gezielte KI-gestützte Suche nach Gesichtsbildern von Einzelpersonen oder einer Personengruppe, z. B. einem konkreten Tatverdächtigen oder einer Gruppe von Opfern einer Straftat (Leitlinien der Kommission, C(2025) 884 final, Rn. 228 f.; *Raue* in: BeckOK KI-Recht, KI-VO, Stand: 01.08.2025, Artikel 5 Rn. 88). Bei dem Einsatz des nachträglichen biometrischen Datenabgleichs ist daher zu gewährleisten, dass kein ungezieltes Auslesen öffentlicher Datenbestände im Internet und stets eine anlassbezogene Nutzung der Recherche-Anwendung erfolgt. Auch der LfD hat in seiner Stellungnahme auf das Verbot des Webscraping hingewiesen.

Zu Absatz 1:

Aus Satz 1 ergibt sich, dass ein Abgleich mit biometrischen Daten im Allgemeinen möglich ist. Beispielhaft werden biometrische Daten zu Gesichtern und Stimmen genannt. Der biometrische Datenabgleich beschränkt sich dabei auf Daten, die die Polizei zur Erfüllung der ihr obliegenden Aufgaben weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat. Die zur Verfügung stehenden Referenzdaten werden daher auf bereits erhobene polizeiliche Daten sowie auf solche Daten, für welche die Polizei eine Abrufberechtigung verfügt, beschränkt.

Voraussetzung für einen biometrischen Datenabgleich auf Grundlage des Satzes 1 ist das Vorliegen einer konkreten Gefahr gemäß § 2 Nr. 1 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

Erhaltung im öffentlichen Interesse liegt. Ein Datenabgleich ist hiernach nur möglich, wenn die positiv benannten Rechtsgüter betroffen sind. Darüber hinaus muss der Einsatz des biometrischen Datenabgleichs zum Zweck der Identifizierung oder Ermittlung des Aufenthaltsorts der betroffenen Person erforderlich sein. Durch die Regelung wird sichergestellt, dass gleich geeignete, aber mildere Maßnahmen vor dem Einsatz des biometrischen Abgleichs vorrangig anzuwenden sind.

In Satz 1 Nr. 2 wird explizit der ultima-ratio-Gedanke des biometrischen Datenabgleichs betont. Im Zuge des Datenabgleichs werden sehr große Datenbestände und in besonders hohem Maße auch biometrische Daten zu Gesichtern und Stimmen von unbeteiligten Dritten abgeglichen. Darüber hinaus kann nach derzeitigem Stand der Technik nicht ausgeschlossen werden, dass es auch zu Fehlidentifizierungen kommt. Insofern ist der Datenabgleich als eingriffsintensive Maßnahme zu bewerten, die dementsprechend auch erst dann zur Anwendung kommt, wenn bereits bestehende, konventionelle Ermittlungsinstrumente keinen Erfolg versprechen.

Satz 2 legt straftatenbezogene Eingriffsschwellen fest. In Satz 2 Nr. 1 ist geregelt, dass Maßnahmen nach Satz 1 auch zulässig sind, wenn Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von erheblicher Bedeutung begehen wird und, wenn es sich bei dieser Straftat um eine Vorfeldstraftat handelt, die Verwirklichung der Straftat zu einer Gefahr für das geschützte Rechtsgut führen würde und der nachträgliche biometrische Abgleich zur Verhütung der Straftat unerlässlich ist. Auch im Rahmen dieser Eingriffsschwellen kommt der Einsatz des biometrischen Datenabgleichs erst als ultima-ratio in Betracht. Der Anwendungsbereich der Vorschrift ist auf Straftaten von erheblicher Bedeutung gemäß § 2 Nr. 14 beschränkt. Zum Begriff der Vorfeldstraftat wird auf die Ausführungen zu § 2 Nr. 14 a verwiesen.

Gemäß Satz 2 Nr. 2 ist ein biometrischer Datenabgleich zudem auch dann zulässig, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird und der nachträgliche biometrische Abgleich zur Verhütung der Straftat unerlässlich ist. Diese Vorschrift stellt auf das individuelle Verhalten einer Person ab. Der Begriff der terroristischen Straftat ist in § 2 Nr. 15 legal definiert. Ein biometrischer Datenabgleich ist hiernach möglich, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird (BVerfG, Urt. v. 20.04.2016, Az.: 1 BvR 966/09, 1 BvR 1140/09, Rn. 112).

Durch die Regelung in Satz 3 wird festgelegt, dass ein Abgleich der biometrischen Daten mit im Internet öffentlich zugänglichen Echtzeit-Bildübertragungen ausgeschlossen ist, sodass eine Echtzeit-Fernidentifizierung auf Basis dieser Rechtsgrundlage nicht möglich ist. Die Echtzeit-Fernidentifizierung stellt ein aliud zu dem vorliegend geregelten biometrischen Datenabgleich dar und bedarf daher einer gesonderten Rechtsgrundlage.

Das Verbot in Satz 3 umfasst zum einen Live-Streams, etwa von Veranstaltungen, in denen auch das Publikum erfasst wird, oder das Live-Video einer Webcam an einem öffentlichen Ort. Zum anderen erfasst die Vorschrift explizit auch Echtzeit-Lichtbild-Dateien. Darunter fallen etwa Bilder von Webcams, die in zeitlich kurzer Abfolge einzelne Lichtbilder ins Internet hochladen.

Satz 4 schließt einen biometrischen Datenabgleich von Gesichtern und Stimmen, die aus einer Wohnraumüberwachung oder einer Online-Durchsuchung gewonnen wurden, aus. Da diese Eingriffsmaßnahmen besonders eingriffsintensiv sind, wird die Verwendung dieser Daten im Rahmen des biometrischen Datenabgleichs ausgeschlossen.

Zu Absatz 2:

Die Vorschrift in Absatz 2 begrenzt den personellen Anwendungsbereich des biometrischen Datenabgleichs. Danach darf der nachträgliche biometrische Datenabgleich nur gegen die gemäß § 6 oder § 7 Verantwortlichen, die in § 8 Abs. 1 bezeichneten Personen sowie Personen im Sinne von Absatz 1 Satz 2 durchgeführt werden.

Zu Absatz 3:

Die Durchführung des nachträglichen biometrischen Datenabgleichs steht gemäß Satz 1 in jedem Einzelfall unter einem Behördenleitervorbehalt. Nach der Vorschrift dürfen Maßnahmen nach Absatz 1 Sätze 1 und 2 nur durch die Behördenleitung angeordnet werden. Die Behördenleitung hat die Möglichkeit, ihre Anordnungsbefugnis auf die Dienststellenleiterinnen und Dienststellenleiter sowie Beamtinnen und Beamte der Laufbahngruppe 2 ab dem zweiten Einstiegsamt zu übertragen. Gemäß

Satz 3 steht die Anordnung unter einem Schriftformerfordernis. Sofern die Voraussetzungen der Anordnung nachträglich wegfallen, ist der Datenabgleich unverzüglich zu beenden.

Zu Absatz 4:

Darüber hinaus besteht nach Satz 1 auch für die Einrichtung und wesentliche Änderung eines Systems zum automatisierten nachträglichen biometrischen Abgleich ein Behördenleitervorbehalt. In Satz 2 wird der Behördenleitung, wie bereits in Absatz 3, ebenfalls die Möglichkeit zur Delegation der Anordnungsbefugnis eingeräumt. Zusätzlich ist die oder der Landesbeauftragte für den Datenschutz vor der Einrichtung und wesentlichen Änderung eines Systems nach Satz 1 anzuhören. Bei Gefahr im Verzug kann auf eine Anhörung verzichtet werden. Die Anhörung ist jedoch im Anschluss an die Gefahrenlage unverzüglich nachzuholen.

Zu Absatz 5:

Satz 1 statuiert eine Begründungspflicht für jeden Einsatz des nachträglichen biometrischen Datenabgleichs. Durch die Vorgabe soll insbesondere eine effektive Kontrolle durch externe Stellen, wie etwa durch den Landesbeauftragten für den Datenschutz, gewährleistet werden.

In Satz 2 und 3 werden die Mindestinhalte der Begründung vorgegeben. Gemäß Satz 2 sind die Voraussetzungen für die Maßnahme und die wesentlichen Abwägungsgesichtspunkte darzulegen. In Satz 3 wird der Inhalt der Begründung weiter konkretisiert.

Absatz 6:

Satz 1 enthält spezifische Vorgaben für die Löschung nicht mehr benötigter Daten. Danach sind die im Rahmen des nachträglichen biometrischen Datenabgleichs erhobenen Daten nach Durchführung des Abgleichs unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen.

Satz 2 bestimmt weiterhin, dass die Weiterverarbeitung der beim Abgleich erhobenen Daten zu anderen Zwecken unzulässig ist. Durch diese Beschränkung wird eine Nutzung der Daten zu anderen Zwecken verwehrt und die Eingriffstiefe der Maßnahme begrenzt.

Zu § 32 d:

Mobil einsetzbare Foto-, Video- und Audiotechnik, u. a. auch in Kombination mit unbemannten Luftfahrtsystemen (ULS), stellt einen einsatztaktischen Mehrwert für die Polizei im Rahmen ihrer Aufgabenerfüllung dar. Mit § 32 d wird eine klarstellende Rechtsgrundlage für den Einsatz dieser Geräte geschaffen, was die Zulässigkeit von z. B. ULS bei bestimmten Maßnahmen der Datenerhebung nach den §§ 32, 33 a, 33 b, 33 d, 35 und 35 a oder der Abwehr von unbemannten Fahrzeugsystemen nach § 32 e angeht.

Zu Absatz 1:

Der Einsatz von unbemannten mobilen Fahrzeugsystemen als Plattform für z. B. Bildübertragungs-, Bildaufzeichnungs-, Tonübertragungs- und Tonaufzeichnungsgeräte darf nur bei den in Absatz 1 genannten Maßnahmen und nur unter den für diese Maßnahmen geltenden Voraussetzungen erfolgen. Das bedeutet, dass keine Ausweitung der jeweils einschlägigen Befugnisnormen erfolgt. Gestatten die Eingriffsnormen z. B. keine Datenerhebung aus Wohnungen, so darf dies auch nicht im Anwendungsbereich des § 32 d erfolgen. Es handelt sich daher um eine klarstellende Norm. Aus dieser Akzessorietät folgt auch, dass die einzelnen Tatbestandsvoraussetzungen der §§ 32, 32 e, 33 a, 33 b, 33 d, 35 und 35 a auch für den Einsatz unbemannter Fahrzeugsysteme vorliegen müssen.

Zu Absatz 2:

Absatz 2 hebt klarstellend hervor, dass Bild- und Tonübertragungen oder -aufzeichnungen nach § 32, bei denen nach Absatz 1 ebenfalls der Einsatz von unbemannten Fahrzeugsystemen (z. B. ULS) zugelassen wird, auch im Fall eines Einsatzes von unbemannten mobilen Sensorträgern ihren Charakter als offene Maßnahmen grundsätzlich bewahren müssen. Aus diesem Grund wird mit Satz 2 ausdrücklich und abermals klarstellend auf die Pflicht zur Kenntlichmachung der Maßnahme durch z. B. Durchsagen, Beschilderungen oder gut sichtbare Hinweise besonders hingewiesen. Der Einsatz von konventionellen Luftfahrzeugen, die für die Bevölkerung etwa durch lautere Fluggeräusche und/oder größere Abmessungen auffälliger und ihr letztlich auch vertrauter sind, wie z. B. Hubschrauber, wird von der Vorschrift nicht erfasst. § 32 Abs. 2 bleibt aus systematischen Gründen unberührt.

Zu Absatz 3:

Absatz 3 stellt klar, dass richterliche Anordnungen für Maßnahmen nach Absatz 1 auch den Einsatz von unbemannten Fahrzeugsystemen für Bild- und Tonübertragungen- oder -aufzeichnungen umfassen müssen.

Zu § 32 e:

Mit § 32 e wird auf die aktuellen technischen Entwicklungen und die damit einhergehenden neuen Gefahrenlagen durch z. B. ULS reagiert und eine neue Rechtsgrundlage für die Detektion und Abwehr von Land-, Luft-, und Wasser- und Unterwasserfahrzeugen, die nicht durch eine an Bord befindliche Person gesteuert werden (z. B. ferngesteuerte oder autonome Geräte), und zur Ermittlung des Steuergerätes geschaffen.

Geregelt wird damit insbesondere die Abwehr von ULS mit geeigneten technischen Mitteln, wobei sich der Einsatz der technischen Mittel auch auf die Unterbrechung und Übernahme der Steuerungsverbindung beziehen kann.

Zum Einsatz gegen ferngesteuerte und autonome Geräte kommen in der polizeilichen Praxis moderne Techniken wie z. B. Laser, elektromagnetische Impulse, Jamming, GPS-Störung und die Nutzung von Detektionstechnik (Überwachung des elektromagnetischen Wellenspektrums) sowie physische Mittel der Einwirkung auf die Systeme.

Gemäß Satz 2 wird auch die Möglichkeit geregelt, technische Mittel zur Erkennung einer Gefahr, die von unbemannten Fahrzeugsystemen ausgeht, einzusetzen. Durch diese Maßnahme kann etwa Herkunft und Steuerung unbemannten Fahrzeugsysteme geklärt werden. Diese möglichen Anwendungsfälle werden beispielhaft durch die Regelung aufgegriffen.

Ferner ist auch zu beachten, dass durch die eingesetzten technischen Mittel zum Zwecke der Erkennung einer Gefahr nach Satz 1 unbeteiligte Dritte unbeabsichtigt, etwa durch den Einsatz von Kamerasystemen, erfasst werden können. Ein Einsatz muss aus praktischen Erwägungen auch dann möglich sein, wenn Dritte unvermeidbar von der Maßnahme betroffen sind. Gemäß Satz 3 dürfen Maßnahmen nach den Sätzen 1 und 2 daher auch durchgeführt werden, wenn Dritte von einer Datenverarbeitung unvermeidbar betroffen werden.

Zu Nummer 9 (bisheriger § 32 a):

Der bisherige § 32 a erhält einen neuen Regelungsstandort und wird nunmehr inhaltsgleich zu § 32 f.

Zu Nummer 10 (§ 33):

Mit den Änderungen sollen Vorgaben des Bundesverfassungsgerichts aus dem Beschluss vom 9. Dezember 2022 (1 BvR 1345/21) umgesetzt werden. Mit der Entscheidung hat das Bundesverfassungsgericht Konkretisierungen hinsichtlich der Einschränkungen zur Erhebung kernbereichsrelevanter Daten im Bereich des Einsatzes von Vertrauenspersonen sowie von verdeckten Ermittlerinnen und verdeckten Ermittlern festgelegt, die der Gesetzgeber umzusetzen hat.

Zu Buchstabe a:

Mit der Ergänzung in Satz 1 wird Absatz 2 um eine Regelung ergänzt, die den Erfordernissen aus der Rechtsprechung des Bundesverfassungsgerichts 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 ff.). Das Bundesverfassungsgericht hat entschieden, 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 des 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 Ermittlerinnen und verdeckten Ermittlern 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 Unterbrechungsverbot verfassungsrechtlich gerechtfertigt sein. Das gälte jedenfalls, wenn ansonsten Leib oder Leben der Vertrauenspersonen oder der verdeckten Ermittlerin oder des verdeckten Ermittlers in Gefahr gerieten.

Verfassungsrechtlich anzuerkennen sei aber - so das Bundesverfassungsgericht ausdrücklich - auch das in der Praxis bedeutsame ermittlungstechnische Bedürfnis, den weiteren Einsatz von Vertrauenspersonen und verdeckt Ermittelnden zu sichern (BVerfG, a. a. O., Rn. 115). Neben der Gefährdung von Leib oder Leben der eingesetzten 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.

Zu Buchstabe b:

Zu Doppelbuchstabe aa:

Unterbleibt in den Fällen der §§ 36 und 36 a eine Unterbrechung der Datenerhebung aufgrund einer Gefährdung nach Absatz 2 Satz 1, setzt die Verfassungsmäßigkeit der Ausnahme von Unterbrechungsgebot zudem voraus, dass weitere Schutzvorkehrungen auf der Auswertungs- und Verwertungsebene bestehen. Ausdrücklich geregelt wird daher 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 unterbliebene 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).

Nach dem neuen Satz 3 in Absatz 5 sind auch die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und die Umstände des Fortsetzens der Maßnahme zu dokumentieren, wenn ein Abbruch aufgrund einer Gefährdung nach Absatz 2 Satz 1 unterbleibt.

Zu Doppelbuchstabe bb:

Es handelt sich um notwendige Folgeänderungen, die durch die Einfügung des neuen Satz 3 veranlasst sind.

Zu Buchstabe c:

Absatz 6 setzt die Vorgaben des Bundesverfassungsgerichts zu spezifischen Prüfpflichten der Vertrauenspersonen und deren polizeilicher Führungspersonen sowie von verdeckten Ermittlerinnen und verdeckten Ermittlern hinsichtlich gewonnener Informationen auf kernbereichsrelevante Erkenntnisse um und legt den eingesetzten Personen und in den Fällen des § 36 auch den polizeilichen Führungspersonen 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 weitergegeben werden. In Zweifelsfällen entscheidet die oder der behördliche Datenschutzbeauftragte über die Verwendbarkeit und Löschung der Daten.

Zu Nummer 11 (§ 33 b):

§ 33 b, in dem bisher aufgrund der einschränkenden Formulierung ausschließlich der Einsatz des sogenannten IMSI-Catchers geregelt war, wird nunmehr technikoffen formuliert. Zudem soll für den Einsatz einer sogenannten Stillen SMS eine eigenständige Rechtsgrundlage geschaffen werden. „Stille SMS“ (stealth ping) sind spezielle Kurzmitteilungen, die zur Ortung von Mobiltelefonen benutzt werden. Sie werden vom Empfänger nicht bemerkt, bewirken aber eine Rückmeldung des Geräts bei der Funkzelle, in die es eingebucht ist. Dadurch wird beim Provider ein Verkehrsdatensatz erzeugt, der nach § 33 c Abs. 2 i. V. m. § 96 Abs. 1 Satz 1 Nr. 1 Telekommunikationsgesetz erhoben werden kann.

Eine eigenständige Rechtgrundlage ist erforderlich, nachdem der Bundesgerichtshof mit Beschluss vom 8. Februar 2018 - 3 StR 400/17 entschieden hat, dass Rechtsgrundlage für das Versenden von „Stillen SMS“ nicht § 100 a Strafprozessordnung (Telekommunikationsüberwachung) sein kann, sondern § 100 i Abs. 1 Nr. 2 Strafprozessordnung (Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten). Die parallele Vorschrift im NPOG wäre § 33 b, die aber ausschließlich für den Einsatz des IMSI-Catchers konzipiert ist. Um auch weiterhin das Mittel der „Stillen SMS“ nutzen zu können, bedarf § 33 b einer Anpassung.

Zu Buchstabe a:

Damit die Änderungen sich auch in der Überschrift widerspiegeln, wird statt „Geräte- und Standortermittlung“ die Formulierung „Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten“ in die Überschrift eingefügt. Damit wird der Regelungsgegenstand besser erkennbar.

Zu Buchstabe b:

In Absatz 1 bleiben die Voraussetzungen für den Einsatz dieser Mittel unverändert. Die Beschränkung auf den Einsatz des IMSI-Catchers wird gestrichen und der Absatz so formuliert, dass auch das Versenden einer „Stillen SMS“ auf die Regelung gestützt werden kann.

Zu Buchstabe c:

Die bisherigen Regelungen aus Absatz 1 Sätze 2 und 3 zur Betroffenheit von Dritten und zur Verwendung der Daten, werden in einen neuen Absatz 2 überführt und sprachlich angepasst.

Zu Buchstaben d und e:

Es handelt sich um notwendige Folgeänderungen, die durch die Einfügung eines neuen Absatzes 2 veranlasst sind.

Zu Buchstabe f:

In dem neuen Absatz 5 ist eine Ausnahme vom Richtervorbehalt vorgesehen. Die „Stille SMS“ ist bei der Suche nach akut suizidgefährdeten Personen von besonderer Bedeutung. Durch die Standortbestimmung des mitgeführten und eingeschalteten Mobiltelefons besteht die Möglichkeit, eine gefährdete Person rechtzeitig aufzufinden. Für eine solche Suche ist, insbesondere in den Fällen eines angekündigten Suizids, größte Eile geboten. Das vorherige Einholen einer richterlichen Anordnung würde in der Regel einen möglichen Erfolg der Maßnahme gefährden. Dies spricht dafür, in diesen Fällen eine Anordnung durch die Polizei zu ermöglichen. Gleichzeitig ist auch der mit der Maßnahme verbundene Grundrechtseingriff in solchen Fällen deutlich geringer als in anderen Fällen, sodass ein Verzicht auf die verfahrenssichernde Maßnahme der richterlichen Anordnung, wie er auch in § 33 c Abs. 5 vorgesehen ist, zulässig ist.

Zu Nummer 12 (§ 33 c):

Die bisherigen Verweisungen auf das TKG und das TMG bedürfen der Anpassung, da durch das Telekommunikationsmodernisierungsgesetz vom 23. Juni 2021 (BGBl. I 1858) sowie das Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz - TDDDG -) vom 23. Juni 2021 (BGBl. I 1982), Titel „TTDSG“, geänd. m.W.v. 14. Mai 2024 durch Gesetz vom 6. Mai 2024 (BGBl. 2024 I Nr. 149), zahlreiche Änderungen erfolgten.

Durch die zusätzliche Aufnahme des TDDDG wird dem Umstand Rechnung getragen, dass die in § 33 c enthaltenen Definitionen nicht mehr nur ausschließlich im TKG, sondern teilweise auch im TDDDG zu finden sind.

Zu Buchstabe a:

Das TMG ist am 14. Mai 2024 außer Kraft getreten. Die bisherigen Verweisungen auf das TMG in Absatz 1 werden daher entsprechend angepasst.

Zu Doppelbuchstabe aa:

Die bisherige Verweisung auf das Telemediengesetz (TMG) ist überholt. Die Vorschrift ist am 14. Mai 2024 außer Kraft getreten und durch das Digitale-Dienste-Gesetz (DDG) ersetzt worden.

Zu Doppelbuchstabe bb:

Die bisher in § 14 TMG (a. F.) enthaltene Definition zu Bestandsdaten ist durch die Definition in § 2 Abs. 2 Nr. 2 im TDDDG ersetzt worden.

Zu Doppelbuchstabe cc:

Die bisher in § 15 TMG (a.F.) enthaltene Definition zu Nutzungsdaten ist durch die Definition in § 2 Abs. 2 Nr. 3 im TDDDG ersetzt worden. Das TKG enthält keine entsprechende Definition.

Zu Buchstabe b:

Zu Doppelbuchstaben aa, bb und cc:

Die Anpassungen in Absatz 2 sind redaktionell und resultieren aus der Änderung des TKG.

Zu Buchstabe c:

Der Begriff „Teilnehmer“ ist seit der Änderung des TKG in § 3 TKG nicht mehr enthalten. Dies macht eine Anpassung der Begriffe „Teilnehmerin“ und „Teilnehmer“ erforderlich. Stattdessen werden nunmehr die Begriffe „Nutzerin“ bzw. „Nutzer“ verwendet. Die weiteren Anpassungen sind redaktionell.

Zu Nummer 13 (§ 34):

In § 34 Abs. 1 Satz 1 Nr. 2 wird geregelt, dass eine Datenerhebung durch längerfristige Observation bei Vorfeldstraftaten nur zulässig ist, wenn eine konkretisierte Gefahr der Begehung dieser Straftat vorliegt und die Verwirklichung der Straftat zu einer konkreten Gefahr für das geschützte Rechtsgut führen würde.

Mit dieser und den weiteren Änderungen in den §§ 2 und 37 werden Vorgaben aus dem Beschluss des Bundesverfassungsgerichts vom 9. Dezember 2022 (1 BvR 1345/21) zu Eingriffsschwellen beim Einsatz besonderer Mittel der Datenerhebung bei Vorfeldstraftatbeständen umgesetzt. Gegenstand des Beschlusses war eine Verfassungsbeschwerde, die sich gegen Regelungen im Sicherheits- und Ordnungsgesetz des Landes Mecklenburg-Vorpommern zu heimlichen Überwachungsmaßnahmen richtete. Das Bundesverfassungsgericht hat mehrere Vorschriften teilweise für nichtig und teilweise für mit dem Grundgesetz unvereinbar erklärt, u. a., weil sie den Anforderungen der Verhältnismäßigkeit im engeren Sinne nicht genügen. Die Eingriffsschwelle bei Eingriffen, die wie die besonderen Mittel der verdeckten Datenerhebung tief in die Privatsphäre eindringen und ein besonders schweres Eingriffsgewicht erlangen können, genügt den Anforderungen an die Verhältnismäßigkeit im engeren Sinne hiernach nur, wenn sie entweder an eine konkrete oder an eine wenigstens konkretisierte Gefahr für ein hinreichend gewichtiges Rechtsgut geknüpft ist (BVerfG, a. a. O., Rn. 88 ff.), was jedoch bei der Verwirklichung von Vorfeldstraftatbeständen nicht notwendigerweise der Fall ist.

Das Bundesverfassungsgericht (a. a. O., Rn. 92), führt hierzu dementsprechend wie folgt aus:

„Hingegen wird dem Gewicht eines Eingriffs durch heimliche polizeirechtliche Überwachungsmaßnahmen nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weiter in das Vorfeld einer in ihren Konturen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird. Eine Anknüpfung der Eingriffsschwelle an das Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn zu diesem Zeitpunkt nur relativ diffuse Anhaltspunkte für mögliche Rechtsgutsgefahren bestehen. Die Bedeutung einzelner Beobachtungen ist dann häufig vieldeutig. Die Geschehnisse können harmlos bleiben, aber auch den Beginn eines Vorgangs bilden, der in eine konkrete Gefahr oder gar eine Verletzung der tatbestandlich geschützten Rechtsgüter mündet. Solche Offenheit genügt für die Durchführung von eingriffsintensiven heimlichen Überwachungsmaßnahmen nicht (vgl. BVerfGE 141, 220 Rn. 113 mwN = NVwZ 2016, 839). Daher entspricht es nicht ohne Weiteres verfassungsrechtlichen Anforderungen, wenn die Ermächtigung zur Erhebung personenbezogener Daten zur Gefahrenabwehr als Eingriffsschwelle an die Gefahr der Begehung solcher Straftaten anknüpft, bei denen die Strafbarkeitsschwelle durch die Einbeziehung von Vorbereitungshandlungen in das Vorfeld von Gefahren verlagert wird. Zwar kann auch mit der Verwirklichung eines Vorfeldstraftatbestandes eine konkretisierte oder konkrete Gefahr für die jeweils geschützten Rechtsgüter einhergehen. Sicher ist dies jedoch nicht; allein aus der Gefahr der Verwirklichung eines Vorfeldstraftatbestandes ergeben sich nicht notwendigerweise bereits solche Gefahren für das Rechtsgut. Gerade auf eine Gefahr für das Rechtsgut kommt es aber an (vgl. BVerfGE 100, 313 (395) = NJW 2000, 55 = NVwZ 2000, 185 Ls.; BVerfGE 125, 260 (329 f.) = NJW 2010, 833 = NVwZ 2010, 770 Ls.; BVerfGE 141, 220 Rn. 112 f. = NVwZ 2016, 839; BVerfGE 154, 152 Rn. 221 = NVwZ 2020, 1412 = NVwZ-Beil. 2020, 10; BVerfG NVwZ-Beil. 2022, 70 Rn. 376). Zwar ist dem Gesetzgeber verfassungsrechtlich nicht verwehrt, zur Bestimmung der Eingriffsvoraussetzungen auch an die Gefahr der Begehung von Vorfeldstraftatbeständen in dem hier gemeinten Sinn (dazu Rn. 50) anzuknüpfen. Er muss 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 (vgl. BVerfG NVwZ-RR 2023, 1 Rn. 134 = NVwZ 2023, 66 Ls. - BVerfSchG - Übermittlungsbefugnisse).“

Die geltende Eingriffsschwelle in § 34 Abs. 1 Satz 1 Nr. 2 bezieht sich auf die Gefahr der Begehung einer Straftat von erheblicher Bedeutung und nicht auf das von dem Straftatbestand geschützte

Rechtsgut. Dies wäre unproblematisch, wenn mit der Gefahr der Tatbestandsbegehung zwangsläufig auch schon eine konkrete oder konkretisierte Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen würde. Das ist jedoch nicht der Fall, weil zu den Straftaten von erheblicher Bedeutung im Sinne des § 2 Nr. 14 auch Vorfeldtaten wie die §§ 87, 88, 89 a, 89 c, 98, 99, 129, 129 a Abs. 3 StGB gehören, die Gründungs-, Beteiligungs- und Unterstützungshandlungen bei terroristischen Vereinigungen unter Strafe stellen, bei denen - so das Bundesverfassungsgericht - mit der Tatbestandsverwirklichung nicht zwangsläufig eine konkrete oder wenigstens konkretisierte Gefahr für das geschützte Rechtsgut einhergeht. Knüpft der Gesetzgeber an die Begehung solcher Straftaten an, muss er zusätzlich fordern, dass damit bereits eine konkrete oder konkretisierte Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt (BVerfG, a. a. O, Rn. 92).

Dem soll durch die vorgesehene Änderung Rechnung getragen werden, indem nunmehr in § 34 Abs. 1 Satz 1 Nr. 2 geregelt wird, dass bei Vorfeldstraftaten zusätzlich zur konkretisierten Gefahr der Begehung dieser Straftat eine konkrete Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen muss, sofern der Straftatbestand verwirklicht wird.

Ergänzend wird auf die Ausführungen zu den §§ 2 und 37 verwiesen.

Zu Nummer 14 (§ 37):

Zu Buchstaben a und b:

In § 37 Abs. 1 wird geregelt, dass eine Ausschreibung zur polizeilichen Beobachtung bei Vorfeldstraftaten nur zulässig ist, wenn eine konkretisierte Gefahr der Begehung dieser Straftat vorliegt und die Verwirklichung der Straftat zu einer konkreten Gefahr für das geschützte Rechtsgut führen würde.

Mit dieser und den weiteren Änderungen in den §§ 2 und 34 NPOG werden Vorgaben aus dem Beschluss des Bundesverfassungsgerichts vom 9. Dezember 2022 (1 BvR 1345/21) zu Eingriffsschwellen beim Einsatz besonderer Mittel der Datenerhebung bei Vorfeldstraftatbeständen umgesetzt.

Ergänzend wird auf die Ausführungen zu § 34 Abs. 1 Satz 1 Nr. 2 Buchst. a) und b) verwiesen.

Zu Nummer 15 (Gliederung):

Nach § 37 b wird ein 3. Abschnitt eingefügt mit der Überschrift „Weiterverarbeitung personenbezogener Daten“. Damit wird ein neuer Begriff eingeführt. Der Begriff der „Datenverarbeitung“ ist nach Artikel 3 Nr. 2 der DS-RL und Artikel 4 Nr. 2 DS-GVO der Oberbegriff für alle Schritte des Umgangs mit personenbezogenen Daten. Er erfasst das Speichern, Verändern und Verwenden ebenso wie die Datenerhebung. Damit alle Datenverarbeitungsschritte, die nicht Datenübermittlung sind und zeitlich nach der Datenerhebung liegen, in §§ 38 und 39 (neu) erfasst werden, wird, wie auch in Polizeigesetzen anderer Länder (vgl. § 23 Polizeigesetz des Landes Nordrhein-Westfalen) und des Bundes (vgl. § 21 BKAG), der Begriff der „Weiterverarbeitung“ eingeführt. Dieser umfasst die bisherigen Begriffe der Speicherung, Veränderung und Nutzung.

Zu Nummer 16 (§ 38):

In der Überschrift des § 38 wird der Begriff der „Weiterverarbeitung“ eingeführt. Zur Begründung wird auf die Ausführungen zu Nummer 26 verwiesen.

§ 38 bleibt zusammen mit § 39 die zentrale Vorschrift zur Weiterverarbeitung personenbezogener Daten. Er erhält eine neue Struktur. Insbesondere werden in der neuen Fassung die grundlegenden Ausführungen des Bundesverfassungsgerichts in seinem Urteil vom 20. April 2016 - 1 BvR 966/09 zur Zweckbindung, insbesondere für besonders eingriffsintensive Maßnahmen im NPOG, umgesetzt.

Zu Absatz 1:

Die Fassung des neuen Absatzes 1 ist weitgehend dem § 12 BKAG entnommen und an den Anwendungsbereich des NPOG angepasst. Die vom Bundesverfassungsgericht entwickelten Kriterien zur Abgrenzung von der Zweckänderung werden wie auch in § 12 BKAG im Wortlaut übernommen.

Die erforderliche Regelungsbefugnis hierfür ergibt sich nach der DS-GVO aus Folgendem:

Der Grundsatz der Zweckbindung wird in Artikel 5 Abs. 1 Buchst. b DS-GVO zwar benannt, es fehlen aber weitere Konkretisierungen. Artikel 6 Abs. 2 und 3 DS-GVO ermöglicht es, bei der Wahrnehmung von Aufgaben in Ausübung öffentlicher Gewalt spezifischere Bestimmungen zu erlassen, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten und Rechtsgrundlagen zur Anpassung der

Anwendung der in der DS-GVO enthaltenen Vorschriften zu schaffen. U. a. sind Bestimmungen darüber möglich, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen und wie lange sie gespeichert werden dürfen. Danach sind spezifische Regelungen zur Zweckbindung zulässig.

§ 3 Satz 1 Nr. 2 NDSG ist Rechtsgrundlage für die Zulässigkeit der Datenverarbeitung auf der Grundlage des Artikels 6 Abs. 1 Buchst. e DS-GVO (in Ausübung öffentlicher Gewalt). Im NDSG fehlt aber eine grundlegende Regelung zur Zweckbindung. In § 6 Abs. 1 BDSG werden allerdings nur spezielle Bereiche geregelt.

Hiernach bedarf es einer Sonderregelung im NPOG.

Der neue 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 Straftaten durch die Verwaltungsbehörden und die Polizei nicht den in § 39 geregelten Anforderungen an eine Zweckänderung unterliegt. Das Bundesverfassungsgericht führt hierzu in seinem Urteil (BVerfG, a. a. O., Rn. 278, 281, 282) aus:

„*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 zugrunde liegenden 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*.“

Satz 1 regelt daher die Weiterverarbeitung nicht nur im Rahmen der im Einzelfall für die Datenerhebung maßgeblichen Gefahren- oder Verdachtslage, sondern auch, soweit die zuständige Behörde im Rahmen der Erfüllung derselben Aufgabe zur Bewältigung anderer Gefahren- oder Verdachtslagen handelt. Voraussetzung ist dann nur, dass es um den Schutz derselben Rechtsgüter oder Rechte oder um die Verhütung derselben Straftaten geht, wobei sich die Identität von Rechtsgütern, Rechten oder Straftaten nicht auf den ursprünglichen Erhebungsanlass bezieht, sondern auf die Schutzzwecke der Datenerhebungsnorm. Die Weiterverarbeitung kann also dem Schutz derjenigen Rechtsgüter oder Rechte oder der Verhütung derjenigen Straftaten dienen, um deren Schutz oder Verhütung es in der Rechtsgrundlage geht, auf die die Datenerhebung gestützt wurde. Nicht erforderlich ist hingegen, dass - wie nach § 39 Abs. 1 - auch eine bestimmte Verdachtslage gegeben ist; Daten können nach Satz 1 auch als bloßer Spurenansatz verwendet werden.

Die Sätze 2 und 3 regeln die entsprechende Anwendung von Satz 1 für personenbezogene Daten, denen keine Erhebung vorausgegangen ist. Die Zweckbestimmung ist bei der Speicherung festzulegen. Dies entspricht der bisherigen Rechtslage in § 38 Abs. 1.

Die erforderliche Regelungsbefugnis hierfür ergibt sich nach der DS-GVO aus Folgendem:

Siehe zunächst die entsprechenden Ausführungen zu Satz 1. Um die Rechtmäßigkeit der Verarbeitung in den Fällen zu gewährleisten, in denen die Daten nicht erhoben wurden, sind derartige

Vorschriften erforderlich. Nur so kann festgestellt werden, ob der Zweckbindungsgrundsatz eingehalten wird und eine Zweckänderung zulässig ist.

Das NDSG enthält keine Entsprechung.

Hiernach bedarf es einer Sonderregelung im NPOG.

Die Sätze 4 und 5 tragen den besonderen Anforderungen des Bundesverfassungsgerichts an die Zweckbindung für Daten, die aus einem verdeckten Eingriff in informationstechnische Systeme (§ 33 d) oder aus dem Einsatz technischer Mittel in Wohnungen (§ 35 a) stammen, Rechnung. Aufgrund 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. Das Bundesverfassungsgericht führt hierzu aus (BVerfG a. a. O, Rn. 283):

„Weiter reicht die Zweckbindung *allerdings für Daten aus Wohnraumüberwachungen und Onlinedurchsuchungen: Hier ist jede weitere Nutzung der Daten nur dann zweckentsprechend, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechenden dringenden Gefahr (vgl. BVerfGE 109, 279, 377, 379) oder im Einzelfall drohenden Gefahr (vgl. BVerfGE 120, 274, 326, 328 f.) erforderlich ist. Das außerordentliche Eingriffsgewicht solcher Datenerhebungen spiegelt sich hier auch in einer besonders engen Bindung jeder weiteren Nutzung der gewonnenen Daten an die Voraussetzungen und damit Zwecke der Datenerhebung. Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden oder im Einzelfall drohenden Gefahr kommt hier nicht in Betracht.“*

Für die Verarbeitung von personenbezogenen Daten, die aus Maßnahmen nach §§ 33 d erlangt wurden, sieht Satz 4 daher vor, dass die Weiterverarbeitung im jeweiligen Einzelfall zur Abwehr einer dringenden Gefahr nach § 33 d Abs. 1 Nr. 1 oder zur Verhütung einer in § 33 d Abs. 1 Nrn. 2 und 3 genannten Straftat unerlässlich ist.

Dem folgend, setzt auch die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in Wohnungen erlangt wurden, gemäß Satz 5 voraus, dass diese Weiterverarbeitung im jeweiligen Einzelfall zur Abwehr einer dringenden Gefahr nach § 35 a Abs. 1 Nr. 1 oder 2 unerlässlich ist.

Zur Regelungsbefugnis siehe die entsprechenden Ausführungen zu den Sätzen 2 und 3.

Zu Absatz 2:

Mit Absatz 2 wird für die Verwaltungsbehörden und die Polizei sowohl im Anwendungsbereich der DS-GVO als auch der DS-RL geregelt, unter welchen Voraussetzungen die Verarbeitung von besonderen Kategorien personenbezogener Daten erlaubt ist. Im Anwendungsbereich der DS-GVO dient die Regelung der Schaffung einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts und enthält zu Artikel 6 Abs. 1 Buchst. e und Artikel 9 Abs. 2 Buchst. g DS-GVO spezifische Bestimmungen im Sinne des Artikels 6 Abs. 2 und 3 jeweils in Verbindung mit Absatz 1 Buchst. e der DS-GVO.

Nach Artikel 9 Abs. 2 Buchst. g DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten ausnahmsweise zulässig, wenn die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts des 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 Grundrecht und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.

In § 17 NDSG sind allgemeine Befugnisse zur Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 Abs. 1 DS-GVO enthalten. Nach § 17 Abs.1 Nr. 5 NDSG dürfen solche Daten zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung verarbeitet werden.

Der Begriff der „besonderen Kategorien personenbezogener Daten“ ist in § 24 Nr. 13 NDSG definiert. Wie sich aus § 49 (neu) ergibt, soll diese Definition auch für Maßnahmen nach dem NPOG einschlägig sein.

Zu Satz 1:

Ebenso wie bei der Datenerhebung in § 31 Abs. 5 (neu) wird auch für die Weiterverarbeitung von besonderen Kategorien personenbezogener Daten mit Satz 1 eine § 31 Abs. 5 (neu) entsprechende Vorschrift eingefügt. Zur Begründung wird auf die Ausführungen zu § 31 verwiesen.

Zu Sätzen 2 bis 5:

Die nach Artikel 10 der DS-RL erforderlichen „Garantien für die Rechte und Freiheiten der betroffenen Person“ werden durch die Sätze 2 bis 5 und die §§ 38 ff. (neu) gewährleistet. Mit den Sätzen 2 bis 5 wird, neben der Sensibilisierung der Zugriffsberechtigten, eine Beschränkung des Zugangs zu diesen Daten geregelt. Darüber hinaus soll durch geeignete technische und organisatorische Maßnahmen sichergestellt werden, dass eine nachträgliche Überprüfung des Abrufs und der Verarbeitung dieser Daten möglich ist. In den §§ 38 ff. (neu) sind die materiellen Eingriffsschwellen vorgesehen, die dem deutschen Verfassungsrecht entsprechen und etwa im Fall der Zweckbindungs- und Zweckänderungsnormen teilweise sogar einen engeren Rahmen setzen als die, die der europäische Gesetzgeber vorgibt. Die Anforderungen an die Protokollierung bei automatisierter Datenverarbeitung nach § 35 Abs. 2 NDSG bleiben unberührt.

Die bisherige Regelung zur Kennzeichnung in Absatz 2 wird hier gestrichen und künftig in einem neuen § 38 a geregelt und umfassend verändert. Die bisherigen Regelungen in den Absätzen 3 und 4 werden hier gestrichen und in einen neuen § 39 a, der künftig die Weiterverarbeitung personenbezogener Daten zu besonderen Zwecken regeln soll, überführt.

Zu Nummer 17 (§ 38 a):

Der vom Bundesverfassungsgericht in der Entscheidung vom 20. April 2016 - 1 BvR 966/09 - entwickelte Grundsatz der hypothetischen Datenneuerhebung lässt sich in den polizeilichen Informationssystemen nur umsetzen, wenn die darin gespeicherten personenbezogenen Daten mit den notwendigen Zusatzinformationen versehen sind, mithin gekennzeichnet sind. Hierzu wird in Anlehnung an die Vorschrift des § 14 BKAG die Regelung des § 38 a (neu) in das NPOG aufgenommen.

Zu Absatz 1:

Satz 1 sieht vor, dass personenbezogene Daten bei der Speicherung in polizeilichen Informationssystemen, zu denen Systeme gehören sollen, die dem polizeilichen Informationsaustausch und der Auskunft dienen und nicht etwa der Vorgangsverwaltung, zu kennzeichnen sind. Diese Kennzeichnungspflicht erfolgt 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), dabei handelt es sich z. B. um die in § 31 Abs. 2 genannten Personen, durch die Angabe der Rechtsgüter oder sonstigen Rechte, deren Schutz die Erhebung dient oder der Straftaten, deren Verfolgung oder Verhütung die Erhebung dient (Nummer 3) und durch die Angabe der Stelle, die sie erhoben hat (Nummer 4). Die Kennzeichnungspflicht schafft die Voraussetzung für eine umfassende Anwendung des Grundsatzes der hypothetischen Datenneuerhebung.

Nach Satz 2 kann die Kennzeichnung auch durch eine Angabe der Rechtsgrundlage der der Erhebung zugrunde liegenden Mittel ergänzt werden.

Der LfD hat empfohlen, die Kennzeichnung um den Zweck der Datenverarbeitung zu ergänzen, um sicherzustellen, dass Änderungen des Zwecks der Datenverarbeitung erkannt werden, und zusätzlich die Rechtsgrundlage der Datenverarbeitung zu benennen. Die in Absatz 1 vorgesehenen Parameter, die auch den Regelungen § 14 BKAG entsprechen, sind jedoch für die Einordnung einer Datenverarbeitung ausreichend. Eine Weiterverarbeitung durch die Behörde, die die Daten erhoben hat, ist nach § 38 an die Wahrnehmung derselben Aufgabe geknüpft, die sich bereits aus den in Satz 1 vorgesehenen Angaben erschließt. Jede nicht derselben Aufgabe zuzuordnende oder durch eine andere Behörde erfolgende Weiterverarbeitung unterliegt den Vorschriften des § 39.

Zu Absatz 2:

Zur Vermeidung einer Weiterverarbeitung von Daten, die nicht den Vorgaben der hypothetischen Datenneuerhebung entspricht, bestimmt Absatz 2, dass personenbezogene Daten, die nicht den Anforderungen des Absatzes 1 entsprechend gekennzeichnet sind, solange nicht weiterverarbeitet werden dürfen, bis eine entsprechende Kennzeichnung erfolgt ist.

Zu Absatz 3:

Damit gewährleistet ist, dass der Grundsatz der hypothetischen Datenneuerhebung auch bei der Weiterverarbeitung von Daten bei anderen Stellen beachtet werden kann, regelt Absatz 3, dass die nach Absatz 1 vorzunehmende Kennzeichnung im Falle der Übermittlung der Daten durch die empfangende Stelle aufrechtzuerhalten ist.

Zu Nummer 18 (§ 39):

§ 39 erhält wie § 38 eine neue Struktur und wird grundlegend überarbeitet, um die Vorgaben des Bundesverfassungsgerichts an die zweckändernde Verarbeitung von personenbezogenen Daten umzusetzen. Der Grundsatz der hypothetischen Datenneuerhebung wird für die Polizei als allgemeiner Grundsatz in das NPOG eingeführt.

Gleichzeitig werden im Interesse einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts in § 39 (neu) zu Artikel 6 Abs. 1 Buchst. e und Abs. 4 DS-GVO spezifische Bestimmungen im Sinne des Artikels 6 Abs. 2 und 3 jeweils in Verbindung mit Absatz 1 Buchst. e der DS-GVO geschaffen.

Hierbei wird von dem in Artikel 6 Abs. 4 DS-GVO eröffneten Regelungsspielraum Gebrauch gemacht, wonach Ergänzungen der DS-GVO zulässig und erforderlich sind. Danach dürfen die Mitgliedstaaten in Fällen, in denen der Zweck der Weiterverarbeitung nicht mit dem Zweck, für den die Daten erhoben wurden, vereinbar ist, nationale Regelungen erlassen, soweit die nationale Regelung eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Abs. 1 DS-GVO genannten Ziele darstellt.

§ 6 Abs. 2 NDSG enthält die zur Anwendung der DS-GVO erforderlichen Ergänzungen im allgemeinen Recht im Hinblick auf den Grundsatz der Zweckbindung (Artikel 5 Abs. 1 Buchst. b DS-GVO). In verschiedenen Bereichen sind die Vorschriften mit dem NPOG vergleichbar. Allerdings fehlt die Möglichkeit einer Zweckänderung zur Verhütung von Straftaten. Die Zulässigkeit der Zweckänderung zur Abwehr einer konkreten Gefahr für die öffentliche Sicherheit und Ordnung ist zu eng.

Es bedarf daher einer Sondervorschrift im NPOG.

Zu Absatz 1:

Absatz 1 regelt für die Verwaltungsbehörden, dass sie personenbezogene Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten können, wenn die Daten zur Erfüllung eines anderen Zwecks der Gefahrenabwehr erforderlich sind und sie auch zu diesem Zweck mit der Maßnahme hätten erhoben werden dürfen, mit der sie erhoben worden sind. Dies entspricht der bisherigen Vorschrift zur Zweckänderung.

Die hypothetische Datenneuerhebung ist ausschließlich für den Bereich der Polizei von Interesse. Geschaffen vom Bundesverfassungsgericht für besonders schwerwiegende verdeckte Grundrechtseingriffe der Polizei, soll sie auch für alle anderen polizeilichen Eingriffe Anwendung finden. Darauf stützt sich die Neustrukturierung des polizeilichen Informationswesens. Für die Verwaltungsbehörden bestehen solche zwingenden Gründe nicht. Insofern wird auch kein Grund gesehen, diese komplexe zweckändernde Datenweiterverarbeitungsvorschrift auch für die Verwaltungsbehörden vorzusehen. Hier ist vielmehr, auch im Hinblick auf die Vorgaben der DS-GVO und der DS-RL, die bestehende Vorschrift zur Zweckänderung ausreichend.

Zu Absatz 2:

In Absatz 2 wird für die Polizei der Grundsatz der hypothetischen Datenneuerhebung in das NPOG eingeführt. Das Bundesverfassungsgericht (BVerfG a. a. O. Rn. 288 bis 290) hat zum Grundsatz der hypothetischen Datenneuerhebung 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 könnte (vgl. BVerfGE 100, 313, 389 f.; 109, 279, 377; 110, 33, 73; 120, 351,369; 130, 1, 34). 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."

In Absatz 2 werden diese verfassungsrechtlichen Anforderungen umgesetzt. Die Vorschrift regelt die zweckändernde Weiterverarbeitung und erfasst - im Unterschied zu § 38 Abs. 1 Satz 1 - die Weiterverarbeitung zur Erfüllung einer anderen Aufgabe als derjenigen, zu deren Erfüllung die Daten erhoben wurden, oder (im Rahmen derselben Aufgabe) zum Schutz anderer Rechtsgüter oder Rechte oder zur Verhütung anderer Straftaten als derjenigen, die für die Datenerhebung maßgebend waren. Nummer 1 regelt die Anforderungen an die Zwecke der Datenverarbeitung, d. h. an das Gewicht der zu schützenden Rechtsgüter oder Rechte oder der zu verhütenden Straftaten und verlangt, dass es um mindestens vergleichbar gewichtige Rechtsgüter oder Rechte oder um vergleichbar schwerwiegende Straftaten gehen muss. Die Formulierung „vergleichbar schwerwiegend" bezieht sich nicht auf die im Einzelfall bei der Datenerhebung verfolgten Zwecke, sondern auf die Zwecke, die nach der Rechtsgrundlage für die Datenerhebung maßgeblich sein können. Wenn etwa bei einer Telekommunikationsüberwachung, die zur Abwehr einer Lebensgefahr erfolgt, Zufallserkenntnisse zu einem anderen Lebenssachverhalt mit Anhaltspunkten für eine Freiheitsgefahr anfallen, kann auch diese andere Gefahr mit diesem Spurenansatz weiter erforscht werden. Die Abwehr der Freiheitsgefahr erscheint zwar gegenüber der Abwehr der Lebensgefahr auf den ersten Blick nicht gleichgewichtig, sie ist jedoch im Hinblick auf die Erhebungsschwelle vergleichbar gewichtig, denn die Telekommunikationsüberwachung ist nach § 33 a Abs. 1 zur Abwehr einer dringenden Gefahr zulässig, deren Schutzgut auch die Freiheit der Person sein kann. Insbesondere bei offenen Maßnahmen ist eine solche Betrachtungsweise unumgänglich, da hier aufgrund der regelmäßig niedrigen Erhebungsschwellen kein Grund besteht, die Verwendung von etwa zum Schutz eines bedeutsamen bzw. hochwertigen Rechtsguts (z. B. 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 Satz 1 weiterverarbeitet werden können.

Nummer 2 enthält die Anforderungen an die Verdachtslage und verlangt, dass sich im Einzelfall konkrete Ermittlungsansätze zur Verhütung solcher Straftaten oder zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für solche Rechtsgüter oder sonstigen Rechte erkennen lassen, zu deren Schutz die entsprechende Datenerhebung verfassungsrechtlich zulässig wäre. Die in Absatz 2 Nr. 2 Buchst. b verwendete Formulierung „in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter" erfordert, dass sich etwa eine Gefahr für mindestens vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte, zu deren Schutz die ursprüngliche Datenerhebung vorgenommen wurde, nicht nur abstrakt, sondern vielmehr als eine in ersten Umrissen absehbare und konkretisierte Möglichkeit eines Schadenseintrittes für ein solches Rechtsgut oder sonstiges Recht darstellt.

Die Regelungen im bisherigen Absatz 2 zur Dokumentation und Vorgangsverwaltung werden an dieser Stelle herausgelöst und einer eigenständigen neuen Regelung in § 39 b zugeführt.

Zu Absatz 3:

In den neuen Absatz 3 werden die bisher in § 39 Abs. 1 Satz 1 Nrn. 2 und 3 bestehenden zweckändernden Regelungen übernommen. Hierbei wurde in Nummer 1 die zweckändernde Nutzung zur Behebung einer Beweisnot zur Wahrung der Verhältnismäßigkeit (vgl. Artikel 4 Abs. 2 Buchst. b DS-RL) unter den Vorbehalt gestellt, dass nicht überwiegende Interessen der betroffenen Person entgegenstehen, und in Nummer 2 die Verweisung auf die Einwilligung nach § 33 NDSG redaktionell an § 31 Abs. 4 angepasst.

Zur Regelungsbefugnis nach der DS-GVO bezogen auf Satz 1 Nr. 1 siehe die Ausführungen vor Absatz 1. Das NDSG enthält keine Entsprechung. Hiernach bedarf es einer Sonderregelung im NPOG.

Mit Satz 1 Nr. 2 wird Artikel 6 Abs. 1 Buchst. a DS-GVO aufgegriffen und nach Artikel 6 Abs. 2 DS-GVO eine spezifische Voraussetzung für die Einwilligung zur Gewährleistung der Rechtmäßigkeit

geschaffen. Die Wiederholung der in der DS-GVO enthaltenen Vorschrift ist zur Verständlichkeit dieser Norm erforderlich. Da das NDSG keine Entsprechung enthält, bedarf es auch hier einer Sonderregelung im NPOG.

§ 39 Abs. 1 Satz 2 wird ebenfalls übernommen und statt einer Sperrung der Daten der Begriff der „Einschränkung der Verarbeitung“ eingeführt, um die Vorschrift an die Begrifflichkeiten aus dem europäischen Datenschutzrecht anzupassen. Ergänzend wird klargestellt, dass die Verarbeitung der personenbezogenen Daten in den Fällen des Satzes 1 Nr. 2 auf die Weiterverarbeitung zu beschränken ist, zu der die betroffene Person die Einwilligung erteilt hat.

Die Regelungsbefugnis nach der DS-GVO folgt hierfür aus Artikel 6 Abs. 2 DS-GVO, wonach spezifische Bestimmungen zulässig sind, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten. Das NDSG enthält keine Entsprechung. Hiernach bedarf es einer Sonderregelung im NPOG.

Zu Absatz 4:

Der neue Absatz 4 sieht vor, dass die strengen Vorgaben der Zweckbindung und der Grundsatz der hypothetischen Datenneuerhebung nicht gelten, wenn die vorhandenen zur Identifizierung dienenden Daten einer Person (Grunddaten) zu Identifizierungszwecken aufgrund spezialgesetzlicher Befugnisnormen verwendet werden sollen. 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. Aufgrund der in doppelter Weise eng begrenzten Datenverwendung ist das Eingriffsgewicht dieser Maßnahme folglich mit der Rechtsprechung des Bundesverfassungsgerichts zu vereinbaren. Der LfD lehnt die Regelung ab und legt dem eine sehr weitgehende Auslegung des neuen Absatzes 4 zugrunde, die im Wortlaut und der Systematik der Regelung allerdings keine Grundlage hat. Absatz 4 ermächtigt lediglich zur Verwendung von dort spezifisch geregelten Daten zum Zwecke der Identifizierung, auch ohne dass die Voraussetzungen des hypothetischen Ersatzeingriffs in Absatz 1, der hypothetischen Datenneuerhebung in Absatz 2 oder die speziellen Befugnisse zur Weiterverarbeitung in Absatz 3 vorliegen müssen. Alle weiteren in den §§ 39 ff geregelten Beschränkungen sind zu beachten.

Die erforderliche Regelungsbefugnis nach der DS-GVO ergibt sich aus Artikel 6 Abs. 3 DS-GVO, der es ermöglicht, Rechtsgrundlagen zur Anpassung der Anwendung der in der DS-GVO enthaltenen Vorschriften zu schaffen. U. a. sind Bestimmungen darüber möglich, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen und wie lange sie gespeichert werden dürfen. Danach sind spezifische Regelungen zur Art der zu verarbeitenden Daten zulässig.

Da das NDSG keine Entsprechung enthält, bedarf es auch hier einer Sonderregelung im NPOG.

Zu Absatz 5:

Absatz 5 trägt den besonderen Anforderungen des Bundesverfassungsgerichts (BVerfG a. a. O. Rn. 291) an die zweckändernde Nutzung von Daten, die aus einem verdeckten Eingriff in informationstechnische Systeme oder aus einem Einsatz technischer Mittel in Wohnungen stammen, Rechnung. Ihre Verwendung zu einem geänderten Zweck ist im Falle des Vorliegens einer Gefahr nur möglich, wenn eine im einzelnen Fall bestehende Gefahr im Sinne der Vorschriften vorliegt.

Auf den bisherigen Absatz 5 kann verzichtet werden. Angesichts des datenschutzrechtlichen Niveaus, das durch die neuen Regelungen weiter optimiert wird, bedarf es keiner zusätzlichen Vorschrift für die Weiterverarbeitung von Daten von unvermeidbar betroffenen Dritten. Eine solche Regelung ist in anderen Polizeigesetzen der Länder demnach auch nicht vorhanden und wurde auch vom Bundesverfassungsgericht in der grundlegenden Entscheidung zum BKAG nicht gefordert.

Zu Absatz 6:

Im neuen Absatz 6 wird auch für die zweckändernde Weiterverarbeitung eine Sonderregelung nach dem Vorbild des § 31 Abs. 5 (neu) und des § 38 Abs. 2 (neu) eingefügt. Zur Begründung wird auf die Ausführungen zu § 31 verwiesen.

Der bisherige Absatz 6 wird zu Absatz 8 (neu).

Zu Absatz 7:

In Absatz 7 werden die Regelungen aus § 39 Abs. 3 Sätze 1, 2, 4 und 5 zur Weiterverarbeitung von Daten aus der Verfolgung von Straftaten im Wesentlichen unverändert übernommen. Sprachlich werden die Regelungen an die Begrifflichkeiten des europäischen Datenschutzrechts angepasst. Auf den bisherigen Satz 3, der als Voraussetzung für die Verarbeitung dieser Daten fordert, dass die Daten zu dem geänderten Zweck auch nach dem NPOG mit dem Mittel oder der Methode hätten erhoben werden dürfen, mit denen sie nach der Strafprozessordnung erhoben worden sind, kann verzichtet werden. In Satz 1 wird bereits klargestellt, dass sich die Weiterverarbeitung dieser Daten nach den Absätzen 2, 3 und 4 richtet.

Absatz 7 kann darüber hinaus als Umsetzung von Artikel 6 DS-RL verstanden werden, weil in dieser Vorschrift verschiedene Kategorien von Personen gebildet werden und dies Auswirkungen auf die Datenverarbeitung hat.

Die bisherige Regelung in Absatz 7 zur Weiterverarbeitung zu besonderen Zwecken wird an dieser Stelle herausgelöst und einer eigenständigen Regelung in einem neuen § 39 a zugeführt.

Zu Absatz 8:

Absatz 8 Satz 1 entspricht inhaltlich unverändert dem bisherigen Absatz 6. Die Voraussetzungen aus dem bisherigen Absatz 6 werden durch den Hinweis auf die Absätze 2, 4 und 5 in Satz 2 aufgenommen.

Der neue Satz 2 untersagt, dass Erkenntnisse aus optischen Wohnraumüberwachungen zu Strafverfolgungszwecken verwendet werden dürfen, und dient damit der Umsetzung der besonderen Vorgaben des Bundesverfassungsgerichts zum Verbot der Verwendung von personenbezogenen Daten aus der optischen Wohnraumüberwachung für die Strafverfolgung (BVerfG a. a. O. Rn. 317). Diese Regelung ist notwendig, um Artikel 13 Abs. 3 GG gerecht zu werden, der für die Strafverfolgung nur den Einsatz der akustischen Wohnraumüberwachung vorsieht und nach Auffassung des Bundesverfassungsgerichts durch eine Übermittlung von Daten aus einer präventiv angeordneten optischen Wohnraumüberwachung nicht unterlaufen werden darf.

Die erforderliche Regelungsbefugnis nach der DS-GVO ergibt sich hierfür aus Folgendem:

Mit Absatz 8 wird von dem in Artikel 6 Abs. 4 Fall 2 DS-GVO eröffneten Regelungsspielraum Gebrauch gemacht. Danach dürfen die Mitgliedstaaten in Fällen, in denen der Zweck der Weiterverarbeitung nicht mit dem Zweck, für den die Daten erhoben wurden, vereinbar ist, nationale Regelungen erlassen, soweit die nationale Regelung eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Abs. 1 DS-GVO genannten Ziele darstellt.

In § 6 Abs. 2 Nr. 2 NDSG wird geregelt, dass eine zweckändernde Datenverarbeitung auch zur Verfolgung von Straftaten zulässig ist.

Zu Absatz 9:

In Absatz 9 wird inhaltlich unverändert die Regelung im bisherigen § 39 Abs. 1 Satz 3 aufgenommen.

Die Regelungsbefugnis für diese Regelung ergibt sich aus Artikel 6 Abs. 2 und 3 DS-GVO. Danach dürfen im mitgliedstaatlichen Recht die Zwecke der Verarbeitung festgelegt werden. Ergänzend wird auf die diesbezüglichen Ausführungen zu § 38 Abs. 1 verwiesen.

§ 6 Abs. 1 Nr. 1 NDSG entspricht dem Regelungsgehalt des Absatzes 9.

Zu Absatz 10:

Absatz 10 entspricht inhaltlich unverändert § 39 Abs. 4.

Zu Nummer 19 (§ 39 a):

Mit den neuen §§ 39 a und 39 b werden die bisher in verschiedenen Vorschriften enthaltenen Regelungen zur Weiterverarbeitung personenbezogener Daten zu besonderen Zwecken in zwei zentralen Vorschriften zusammengeführt. Damit wird die Übersichtlichkeit, Klarheit und rechtssichere Anwendung des Gesetzes erhöht.

Zu Absatz 1:

Die bisher in § 39 Abs. 7 enthaltene Regelung zur Weiterverarbeitung zu wissenschaftlichen Forschungszwecken wird in Absatz 1 aufgenommen und um historische Forschungszwecke ergänzt. § 39 a Abs. 1 trifft hierfür mit Ausnahme des Ausschlusses der Verarbeitung von Daten aus einem

verdeckten Einsatz technischer Mittel in Wohnungen oder einem verdeckten Eingriff in informationstechnische Systeme in Satz 2 keine eigenen Regelungen und verweist auf § 25 Abs. 5 NDSG, der für den Anwendungsbereich der DS-RL fast vollständig auf die für den Anwendungsbereich der DS-GVO geltenden Regelungen des § 13 NDSG verweist.

Nach § 39 a Abs. 1 Satz 1 i. V. m. §§ 25 Abs. 5, 13 Abs. 1 Satz 1 NDSG kann die Polizei Daten nicht nur selbst zu Forschungszwecken weiterverarbeiten, sondern auch an Dritte übermitteln. Der LfD hat kritisiert, dass eine solche Übermittlung erfolgen kann, ohne dass die Daten zuvor von der Polizei anonymisiert werden müssen. Tatsächlich verpflichtet § 13 Abs. 2 NDSG die Forschungseinrichtung und nicht die datenhaltende Stelle zur Anonymisierung von Daten, sobald dies nach dem Forschungszweck möglich ist. § 13 Abs. 2 Satz 2 und 3 NDSG sieht aber auch vor, dass bis zur Anonymisierung Merkmale, mit denen ein Personenbezug hergestellt werden kann, getrennt zu speichern sind und mit den Einzelangaben nur zusammengeführt werden dürfen, soweit der Forschungszweck dies erfordert. Damit ist ein weitgehender Schutz der personenbezogenen Daten auch im Rahmen der Forschungstätigkeit gewährleistet.

Eine einschränkende Regelung enthält Absatz 1 Satz 2, soweit Daten aus einem verdeckten Einsatz technischer Mittel in Wohnungen oder einem verdeckten Eingriff in informationstechnische Systeme erlangt wurden. Diese Daten sollen wegen des damit verbundenen tiefen Grundrechtseingriffs und der möglichen Sensibilität der Daten weder für wissenschaftliche noch für historische Forschungszwecke weiterverarbeitet werden dürfen.

Zu Absatz 2:

In Absatz 2 wird die bisherige Regelung zur Weiterverarbeitung von Daten zu statistischen Zwecken aus § 38 Abs. 4 übernommen und sprachlich an Absatz 1 Satz 1 sowie Absatz 3 Satz 1 angeglichen.

Zu Absatz 3:

Der neue Absatz 3 enthält die bisher in § 39 Abs. 7 enthaltene Regelung zur Weiterverarbeitung personenbezogener Daten zu Zwecken der Ausbildung, Fortbildung und Prüfung. Inhaltlich bleibt die Vorschrift unverändert. Die vorgenommenen Änderungen sind redaktioneller Art und betreffen die neue Systematik und die Begrifflichkeiten aus dem europäischen Datenschutzrecht.

Die erforderliche Regelungsbefugnis nach der DS-GVO ergibt sich hierfür aus Folgendem:

Die Vorschrift in Satz 1 wird auf die zur Anwendung der DS-GVO erforderlichen Ergänzungen im allgemeinen Recht im Hinblick auf den Grundsatz der Zweckbindung (Artikel 5 Abs. 1 Buchst. b DS-GVO) gestützt. Ergänzend wird auf die Ausführungen zu § 38 Abs. 1 verwiesen. In § 6 Abs. 1 Nr. 2 NDSG wird eine dem Absatz 3 vergleichbare Regelung getroffen.

Die Vorschriften in Satz 2 bis 4 werden auf Artikel 6 Abs. 2 DS-GVO gestützt, der spezifischere Bestimmungen zulässt, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten. Das NDSG enthält keine Entsprechung. Hiernach bedarf es einer Sonderregelung im NPOG.

Zu Absatz 4:

Der neue Absatz 4 enthält inhaltlich unverändert die bisherige Regelung aus § 38 Abs. 3 zur Aufnahme von fernmündlichen Hilfeersuchen und Mitteilungen durch die Polizei und die Verwaltungsbehörden, soweit sie Aufgaben der Hilfs- und Rettungsdienste wahrnehmen. Die bisherige Regelung wird durch eine Regelung für die Verarbeitung besonderer Kategorien personenbezogener Daten ergänzt. Der Verweis auf § 31 Abs. 5 stellt sicher, dass die dort formulierten besonderen Anforderungen an die Verarbeitung dieser Daten auch hier zur Anwendung kommen.

Die Regelung wird auf Artikel 6 Abs. 3 DS-GVO gestützt. Danach dürfen im mitgliedstaatlichen Recht die Zwecke der Verarbeitung festgelegt werden. Ergänzend wird auf die Ausführungen zu § 38 Abs. 1 verwiesen. Da das NDSG keine Entsprechung enthält, bedarf es auch hier einer Sonderregelung im NPOG.

Die bisherige Regelung zur Löschung von Daten in § 39 a wird aus systematischen Gründen nach den Datenübermittlungsvorschriften in einem neuen 6. Abschnitt mit der Überschrift „Benachrichtigungspflichten, Prüffristen, Berichtigung, Löschung und Einschränkung der Verarbeitung“ verortet.

Zu Nummer 20 (§ 39 b):

In dem neuen § 39 b wird die bisherige Regelung des § 39 Abs. 2 einer eigenständigen Rechtsgrundlage zugeführt. Inhaltlich bleibt die Vorschrift nahezu unverändert. Die Vorschrift wird redaktionell an

die Begrifflichkeiten aus dem europäischen Datenschutzrecht angepasst. Aus dem Blickwinkel der europarechtlichen Zulässigkeit dieser Norm ergibt sich die Befugnis zu dieser Regelung aus Artikel 6 Abs. 4 Fall 2 DS-GVO, weil die zur Vorgangsverwaltung und etwa zu Datensicherungs- oder Datenkontrollzwecken erhobenen Daten nicht unter den Anwendungsbereich der DS-RL fallen, sondern im Anwendungsbereich der DS-GVO liegen. Nach Artikel 6 Abs. 4 DS-GVO dürfen die Mitgliedstaaten in Fällen, in denen der Zweck der Weiterverarbeitung nicht mit dem Zweck, für den die Daten erhoben wurden, vereinbar ist, nationale Regelungen erlassen, soweit die nationale Regelung eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Abs. 1 DS-GVO genannten Ziele darstellt. Die Ziele von Artikel 23 Abs. 1 Buchst. a bis d DS-GVO haben die nationale und öffentliche Sicherheit sowie die Landesverteidigung als auch die Verhütung von Straftaten und die Abwehr von damit zusammenhängenden Straftaten im Blick. Gerade diese Zielsetzungen sind mit § 39 b Abs. 2 Nrn. 1 und 2 (neu) angesprochen.

Im Hinblick auf den Regelungsinhalt des Absatzes 1 enthält das NDSG zwar in § 6 Abs. 4 eine Regelung, nicht jedoch zur Vorgangsverwaltung und zur zeitlich befristeten Dokumentation. Soweit es Absatz 2 betrifft, regelt § 6 Abs. 4 NDSG lediglich ein Zweckänderungsverbot. Es bedarf daher jeweils einer Sonderregelung im NPOG.

Zu Nummer 21 (Überschrift):

Der neuen Systematik des Gesetzes folgend wird an dieser Stelle ein neuer 4. Abschnitt mit der Überschrift „Datenübermittlung“ eingefügt. Die in diesem Abschnitt befindlichen §§ 40 bis 44 a bedürfen einer Überarbeitung und Anpassung an die Bestimmungen des europäischen Datenschutzrechts. Darüber hinaus werden sie einer neuen Systematik unterworfen. § 41 wird die zentrale Vorschrift für Datenübermittlungen an öffentliche Stellen im innerstaatlichen Bereich, während in § 43 Datenübermittlungen im Bereich der Europäischen Union sowie in § 43 a Datenübermittlungen der Polizei im internationalen Bereich geregelt werden. Mit § 44 a werden Übermittlungsverbote und Verweigerungsgründe an einer Stelle in einer Vorschrift zusammengeführt.

Zu Nummer 22 (§ 40):

Zur Schaffung einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts werden in § 40 zu Artikel 5 Abs. 1 Buchst. a DS-GVO spezifische Bestimmungen im Sinne des Artikels 6 Abs. 2 und 3 in Verbindung mit Absatz 1 Buchst. e der DS-GVO geschaffen.

Zu Absatz 1:

In dem neuen Absatz 1 Satz 1 wird der vom Bundesverfassungsgericht aufgestellte Grundsatz der hypothetischen Datenneuerhebung wie vom Gericht gefordert (siehe BVerfG a. a .O., Rn. 307 ff.) auch im Hinblick auf die Datenübermittlung umgesetzt. Als Ergänzung werden die §§ 41 bis 44 a in Bezug genommen. Gleichzeitig wird das Verhältnis zwischen § 40 und den §§ 41 bis 44 a dahin gehend bestimmt, dass § 40 eine „vor die Klammer gezogene“ Regelung ist mit allgemeinen Grundsätzen über diese Phase des Umgangs mit personenbezogenen Daten, die in jedem Fall der Übermittlung einzuhalten sind, während die §§ 41 bis 44 a die dazugehörigen Befugnisnormen oder Ermächtigungsgrundlagen darstellen.

Darüber hinaus wird mit der neuen Formulierung berücksichtigt, dass eine Datenübermittlung stets eine Zweckänderung der Datennutzung darstellt und daher im Gesetzestext keine besondere Erwähnung finden muss. Dies wird auch im neuen Satz 2 umgesetzt und geregelt, dass Übermittlungen stets zu dokumentieren sind, ohne diese Pflicht auf Datenübermittlungen zu einem anderen Zweck - wie derzeit in Satz 2 vorgesehen - zu beschränken.

Der Inhalt der Dokumentationspflicht wird in einem neuen Satz 3 konkretisiert und in den Sätzen 4 und 5 Vorschriften zur Aufbewahrung und Löschung der Dokumentationen weiter ausgestaltet. Dies stellt gegenüber der bisherigen Formulierung „…ist so zu dokumentieren, dass ihre Rechtmäßigkeit überprüft werden kann…“ Anwendungssicherheit her. Darüber hinaus berücksichtigen diese Formulierungen zugleich das durch das Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 (BVerfG a. a. O., Rn. 141 ff.) für notwendig erachtete Kontrollerfordernis der oder des Landesbeauftragten für den Datenschutz.

Der bisherige Satz 3 wird unter Konkretisierung der sprachlichen Anknüpfung der Regelung als neuer Satz 6 in die Vorschrift eingefügt.

Der bisherige Satz 4, der die Aufrechterhaltung der Kennzeichnung bei einer Übermittlung regelt, kann an dieser Stelle gestrichen werden. Eine identische Regelung befindet sich in dem neuen § 38 a Abs. 3, der künftig die zentrale Vorschrift für Regelungen zur Kennzeichnung darstellt.

Die bisherigen Sätze 5 und 6 werden als Sätze 7 und 8 in die neue Fassung des Absatzes 1 übernommen. Hierbei wurde Satz 8 an die neue Rechtslage angepasst, indem die Bezugnahme auf § 31 a Abs. 1 und 6 angeglichen und der alte Begriff „Unterrichtung“ durch „Benachrichtigung“ (vgl. § 31 a) ersetzt wurde.

Die Regelungsbefugnis nach der DS-GVO ergibt sich für Absatz 1 aus Folgendem:

Bis auf die Datenübermittlung an Drittländer oder an internationale Organisationen sind in der DS-GVO keine expliziten Regelungen zu Datenübermittlungen enthalten. Die Datenübermittlung richtet sich nach den Grundsätzen der Verarbeitung nach Artikel 5 DS-GVO und der Rechtmäßigkeit der Verarbeitung nach Artikel 6 DS-GVO. Artikel 6 Abs. 2 und 3 DS-GVO ermöglicht es, spezifischere Bestimmungen zu erlassen, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten und Rechtsgrundlagen zur Anpassung der Anwendung der in der DS-GVO enthaltenen Vorschriften zu schaffen. U. a. sind Bestimmungen darüber möglich, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen und wie lange sie gespeichert werden dürfen. Danach sind spezifische Regelungen zum Zweck der Übermittlung und zu den empfangenden Stellen zulässig.

Zwar sind in § 5 NDSG Regelungen zur Übermittlung personenbezogener Daten enthalten, es fehlt jedoch die im Gefahrenabwehrrecht erforderliche Übermittlung zur Verhütung von Straftaten. Daher bedarf es einer Sondervorschrift im NPOG.

Bei den Regelungen zur Dokumentationspflicht handelt es sich um eine spezifischere Bestimmung nach Artikel 6 Abs. 2 DS-GVO, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten. Da das NDSG zu den in Absatz 1 getroffenen Regelungen keine Entsprechung enthält, ist eine Sondervorschrift im NPOG erforderlich.

Zu Absatz 2:

Absatz 2 entspricht inhaltlich unverändert der alten Fassung des Absatzes 2. Da die datenverarbeitende Stelle zwischen verschiedenen Kategorien personenbezogener Daten zu unterscheiden hat und gerade die Daten von den in § 31 Abs. 2 Nrn. 2 bis 5 genannten Personen verpflichtend als Kategorie zu unterscheiden sind, wird mit dieser Vorschrift sichergestellt, dass die Regelung in der Praxis umgesetzt wird. Die Vorschrift dient der Einhaltung des Artikels 6 DS-RL.

Bei Absatz 2 handelt es sich um eine spezifischere Bestimmung nach Artikel 6 Abs. 2 DS-GVO, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten. Das NDSG enthält hierzu keine Entsprechung, sodass insoweit eine Sondervorschrift im NPOG erforderlich ist.

Zu Absatz 3:

Mit dem neuen Absatz 3 wird die Frage der Verantwortung für die Datenübermittlung ausdrücklich geregelt und an dieser Stelle auf den bisherigen Verweis auf das NDSG (§ 40 Abs. 4) verzichtet. Dies geschieht im Interesse einer einheitlichen Regelung für Verwaltungsbehörden und Polizei im NPOG. Inhaltlich entspricht die Regelung § 5 Abs. 2 NDSG. Die Verantwortung für die Zulässigkeit der Übermittlung trägt im Regelfall die übermittelnde Stelle.

Die Regelungsbefugnis nach der DS-GVO ergibt sich für Absatz 3 aus Artikel 6 Abs. 2 und 3 DS-GVO, es werden die Voraussetzungen für die Rechtmäßigkeit der Verarbeitung näher spezifiziert. Die Regelungsbefugnis für die Übertragung der Verantwortlichkeit im Fall eines Ersuchens folgt aus Artikel 4 Nr. 7 Halbsatz 2 DS-GVO.

Zu Absatz 4:

Zur Begründung für die Aufnahme eines neuen Absatzes 4 wird auf die Begründung zu Absatz 3 verwiesen. In Absatz 4 wird in Anlehnung an § 5 Abs. 3 NDSG eine Regelung zur Übermittlung von in Akten verbundenen personenbezogenen Daten für den Fall eingeführt, dass eine Trennung derjenigen personenbezogenen Daten, die übermittelt werden dürfen, von den weiteren personenbezogenen Daten der betroffenen Person oder eines Dritten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Die Vorschrift trägt der Tatsache Rechnung, dass bei der Übermittlung nicht immer

eine Trennung nach Daten, die übermittelt werden dürfen, und anderen Daten mit vertretbarem Aufwand möglich ist.

Die Regelungsbefugnis nach der DS-GVO ergibt sich für Absatz 4 aus Artikel 6 Abs. 2 und 3 DS-GVO, es werden die Voraussetzungen für die Rechtmäßigkeit der Verarbeitung näher spezifiziert und Rechtsgrundlagen zur Anpassung der Anwendung der in der DS-GVO enthaltenen Vorschriften geschaffen.

Zu Absatz 5:

In Absatz 5 wird ein Verweis auf § 32 Abs. 1 bis 5 NDSG aufgenommen. Dort sind weitere Anforderungen zum Umgang mit personenbezogenen Daten bei Datenübermittlungen, etwa zum Umgang mit unrichtigen personenbezogenen Daten enthalten, die durch den Verweis auch im Anwendungsbereich der DS-GVO gelten sollen. Diese Vorschriften sollen auch bei Datenübermittlungen der Verwaltungsbehörden und der Polizei Anwendung finden. Auf eine Bezugnahme des § 32 Abs. 6 NDSG kann verzichtet werden, da die Regelungen aus § 5 NDSG, auf die § 32 Abs. 6 NDSG verweist, mit den neuen Absätzen 3 und 4 ausdrücklich in das NPOG aufgenommen werden.

Die Regelungsbefugnis nach der DS-GVO ergibt sich für Absatz 5 aus Artikel 6 Abs. 2 und 3 DS-GVO, es werden die Voraussetzungen für die Rechtmäßigkeit der Verarbeitung näher spezifiziert. Da das NDSG zu den in Absatz 5 getroffenen Regelungen keine Entsprechung enthält, ist eine Sondervorschrift im NPOG erforderlich.

Zu Absatz 6:

In Absatz 6 wird die Zweckbindung und Verarbeitung der übermittelten Daten durch die empfangende Stelle geregelt und insbesondere durch Satz 2 klargestellt, dass künftig auch die empfangende Stelle den Grundsatz der hypothetischen Datenneuerhebung beachten muss, wenn sie personenbezogene Daten zu anderen Zwecken als zu denen die Daten übermittelt worden sind, weiterverarbeiten will.

Die Regelungsbefugnis für Absatz 6 ergibt sich nach der DS-GVO aus Artikel 6 Abs. 2 und 3 DS-GVO, es werden die Voraussetzungen für die Rechtmäßigkeit der Verarbeitung näher spezifiziert. In § 5 Abs. 1 Satz 3 NDSG wird lediglich geregelt, dass bei einer Übermittlung an eine nicht öffentliche Stelle der Empfänger an den Datenübermittlungszweck gebunden ist. Es bedarf daher einer Sondervorschrift im NPOG, um die Zweckbindung für alle empfangenden Stellen festzulegen und eine Ausnahme zuzulassen, wenn die Voraussetzungen des § 39 NPOG vorliegen.

Zu Absatz 7:

Absatz 7 entspricht inhaltlich unverändert dem bisherigen Absatz 3.

Zu Absatz 5:

Der bisherige Absatz 5 wird gestrichen. Die Weitergabe von Daten innerhalb der Verwaltungs- oder Polizeibehörden stellt eine zweckändernde Nutzung dar, es gelten die hierfür getroffenen Regelungen. Auf Absatz 5 kann daher verzichtet werden.

Zu Nummer 23 (§ 41):

Zur Schaffung einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts werden in § 41 zu Artikel 5 Abs. 1 Buchst. a DS-GVO spezifische Bestimmungen im Sinne des Artikels 6 Abs. 2 und 3 in Verbindung mit Absatz 1 Buchst. e der DS-GVO geschaffen.

Aus systematischen Gründen wird an dieser Stelle die Datenübermittlung im innerstaatlichen Bereich zusammengeführt.

Zu Buchstabe a:

Dazu ist zunächst eine Änderung der Überschrift erforderlich, um den neuen Regelungsgegenstand zu verdeutlichen.

Zu Buchstabe b:

Zu Absatz 1:

Der bisherige § 41, der die Datenübermittlung zwischen Verwaltungs- und Polizeibehörden regelt, wird inhaltlich unverändert zum neuen Absatz 1 dieser Vorschrift.

Die Regelungsbefugnis nach der DS-GVO ergibt sich für Absatz 1 aus Folgendem:

Bis auf die Datenübermittlung an Drittländer oder an internationale Organisationen sind in der DS-GVO keine expliziten Regelungen zu Datenübermittlungen enthalten. Die Datenübermittlung richtet sich nach den Grundsätzen der Verarbeitung nach Artikel 5 DS-GVO und der Rechtmäßigkeit der Verarbeitung nach Artikel 6 DS-GVO. Artikel 6 Abs. 2 und 3 DS-GVO ermöglicht es, spezifischere Bestimmungen zu erlassen, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten und Rechtsgrundlagen zur Anpassung der Anwendung der in der DS-GVO enthaltenen Vorschriften zu schaffen. Danach sind spezifische Regelungen zum Zweck der Übermittlung und zu den empfangenden Stellen zulässig.

§ 5 Abs. 1 NDSG enthält eine vergleichbare Vorschrift, allerdings wird mit dem Hinweis auf die Voraussetzungen der Zweckänderung (§ 6 Abs. 2 NDSG) eine Übermittlung zur Verhütung von Straftaten ausgeschlossen. Es bedarf daher einer Sondervorschrift im NPOG.

Zu Buchstabe c:

Zu Absatz 2:

Der bisherige § 43 Abs. 1, der die Datenübermittlung an andere öffentliche Stellen im Inland regelt, wird als neuer Absatz 2 ebenfalls inhaltlich unverändert in § 41 aufgenommen. Es wird eine redaktionelle Änderung vorgenommen, in dem der Begriff des nicht geschlechtsneutralen „Empfängers“ durch den Begriff „empfangende Stelle“ ausgetauscht wird. § 41 regelt damit umfassend die Datenübermittlungen im Inland.

Die Regelungsbefugnis nach der DS-GVO ergibt sich zu Absatz 2 aus Artikel 6 Abs. 2 und 3 DS-GVO, der es ermöglicht, spezifischere Bestimmungen zu erlassen, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten und Rechtsgrundlagen zur Anpassung der Anwendung der in der DS-GVO enthaltenen Vorschriften zu schaffen. Da das NDSG zu den in Absatz 2 getroffenen Regelungen keine Entsprechung enthält, ist eine Sondervorschrift im NPOG erforderlich.

Zu Absatz 3:

Zur Komplettierung dieser Vorschrift wird auch § 44 Abs. 1, der die Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs regelt, als neuer Absatz 3 inhaltlich unverändert in § 41 aufgenommen. Dadurch entsteht eine Vorschrift, in der sämtliche Datenübermittlungen im innerstaatlichen Bereich zusammengeführt sind.

Die Regelungsbefugnis nach der DS-GVO ergibt sich zu Absatz 3 aus Folgendem:

Artikel 6 Abs. 2 und 3 DS-GVO ermöglicht es, spezifischere Bestimmungen zu erlassen, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten und Rechtsgrundlagen zur Anpassung der Anwendung der in der DS-GVO enthaltenen Vorschriften zu schaffen. Danach können spezifische Regelungen zum Zweck der Übermittlung und zu den empfangenden Stellen getroffen werden.

Bezogen auf Absatz 3 Nr. 1 ist insoweit ergänzend anzumerken, dass in § 5 Abs. 1 Satz 2 Nr. 1 NDSG zwar eine Regelung zur Übermittlung an eine nicht öffentliche Stelle getroffen wurde, diese Regelung ist jedoch gegenüber der im NPOG bestehenden Vorschrift, die weiter Verwendung finden soll, zu weitgehend, sodass es einer Sondervorschrift im NPOG bedarf.

Hinsichtlich Absatz 3 Nr. 2 gilt, dass insoweit in § 5 Abs. 1 Satz 2 Nr. 2 NDSG eine vergleichbare Vorschrift enthalten ist.

Zu Absatz 3 Nr. 3 existiert im NDSG keine Entsprechung, sodass eine Sondervorschrift im NPOG erforderlich ist.

Zu Nummer 24 (§ 41 a):

Mit § 41 a wird eine spezifische Ermächtigung für die Polizei geschaffen, an öffentliche und nichtöffentliche Stellen auf Ersuchen personenbezogene Daten zum Zwecke der Durchführung einer Zuverlässigkeitsüberprüfung zu übermitteln. Dies betrifft besonders gefährdete Veranstaltungen, die im Fokus der Öffentlichkeit stehen und bei denen der Veranstalter das einzusetzende Personal auf seine Zuverlässigkeit überprüfen muss, um die Sicherheit der Veranstaltung zu gewährleisten. Hierzu ist er auf die bei der Polizei vorliegenden Erkenntnisse angewiesen.

Bereits in der Vergangenheit wurden solche Zuverlässigkeitsüberprüfungen auch mit Erkenntnissen der Polizei durchgeführt. Rechtsgrundlage für diese Verfahrensweise war regelmäßig die informierte Einwilligung der betroffenen Person. Die Überprüfung ohne eine spezielle Rechtsgrundlage ist auf

Kritik bei den Datenschutzbeauftragten des Bundes und der Länder gestoßen. Diese Kritik wird nunmehr aufgenommen und mit § 41 a die spezifische Rechtsgrundlage geschaffen.

Zu Absatz 1:

In Absatz 1 werden die Voraussetzungen für die Datenübermittlung beschrieben. Der Begriff der Veranstaltung wird bereits in § 32 Abs. 1 verwendet und beschreibt hier wie dort jede organisierte räumliche Zusammenkunft von Menschen zu Vergnügungs-, Unterhaltungs-, Bildungs- oder sonstigen Zwecken. Im Gegensatz zu § 32 Abs. 1 muss es sich nicht um eine öffentliche Veranstaltung handeln. Nicht zu den Veranstaltungen gehören auch Versammlungen nach Artikel 8 des Grundgesetzes.

Für die Gefährdung einer Veranstaltung werden keine tatsächlichen Anhaltspunkte vorausgesetzt. Es genügt also eine abstrakte besondere Gefährdung der Veranstaltung. Das bedeutet, dass nach allgemeiner Lebenserfahrung oder polizeilicher Erfahrung mit schädigenden Ereignissen bei oder im Zusammenhang mit einer solchen Veranstaltung in einer Weise zu rechnen ist, die über das allgemeine Restrisiko hinausreicht. Dabei ist insbesondere an terroristische Anschläge oder Amokläufe zu denken. Denkbar sind aber auch drohende Straftaten anderer Art gegen Personen und/oder Sachen.

Die Datenübermittlung muss nach Absatz 1 Nr. 1 zunächst für eine Zuverlässigkeitsüberprüfung erforderlich sein. Die Frage der Erforderlichkeit von Zuverlässigkeitsüberprüfungen ist anhand des jeweiligen Einzelfalls in Anbetracht der jeweiligen Veranstaltung zu beantworten.

Wie bisher auch schon muss nach Absatz 1 Nr. 2 die betroffene Person der Datenverarbeitung schriftlich zugestimmt haben.

Schließlich muss die Datenübermittlung auch angemessen sein, wobei insbesondere der Zugang der betroffenen Person zu der Veranstaltung, gegebenenfalls zu bestimmten Bereichen, Art und Umfang der zu der betroffenen Person vorhandenen Erkenntnisse und die berechtigten Sicherheitsinteressen des Datenempfängers zu berücksichtigen sind.

Satz 2 stellt klar, dass sich die Übermittlung gegenüber nichtöffentlichen Stellen inhaltlich ausschließlich auf die Aussage beschränkt, ob aus polizeilicher Sicht Sicherheitsbedenken bestehen oder nicht. Der LfD hat gefordert, diese Beschränkung auch bei der Zuverlässigkeitsüberprüfung durch öffentliche Stellen zur Geltung zu bringen. Eine Rückmeldung, die sich auf die Aussage über das Bestehen oder Nichtbestehen von Zuverlässigkeitsbedenken beschränkt, lässt für die verantwortliche Stelle jedoch wenig Raum für eine eigene Beurteilung der Zuverlässigkeit und erschwert dieser die Wahrnehmung ihrer Interessen. Für öffentliche Stellen soll diese Beschränkung daher nicht gelten. Auch öffentlichen Stellen gegenüber dürfen jedoch nach Absatz 1 Satz 1 Nr. 1 nur die für die Zwecke der Zuverlässigkeitsüberprüfung erforderlichen Daten offenbart werden.

Zu Absatz 2:

Absatz 2 enthält die Verpflichtung des Empfängers zur Einhaltung der Zweckbindung und die Verpflichtung der Polizei, den Empfänger schriftlich zur Einhaltung dieser Zweckbindung und zur Löschung der Daten nach Beendigung der Veranstaltung zu verpflichten.

Die betroffene Person ist von der Polizei zu unterrichten, soweit das nicht in anderer Weise sichergestellt ist, z. B. durch den Arbeitgeber. Der LfD fordert hier, dass die Polizei die Unterrichtung immer dann vornimmt, wenn dies nicht bereits von anderer Stelle aus geschehen ist. Dies würde jedoch in vielen Fällen zu einer mehrfachen Unterrichtung durch verschiedene Stellen führen und würde für die Betroffenen eher eine Belastung darstellen.

Zu Nummer 25 (§ 42):

Zu Buchstabe a:

Zu Doppelbuchstabe aa:

In § 42 Abs. 1 wird durch einen neuen Satz 4 speziell für die automatisierten Abrufverfahren eine gesonderte Behandlung für die besonderen Kategorien personenbezogener Daten eingefügt. Dies folgt sowohl aus Artikel 10 als auch aus Artikel 29 Abs. 1 DS-RL, die besonderen Schutzvorkehrungen bei der Verarbeitung dieser besonders sensiblen Daten verlangen. Die eingefügte Darlegungsverpflichtung ist eine organisatorische Maßnahme, die eine explizite Entscheidung zur gesteigerten Erforderlichkeit sicherstellt. Zudem ist diese Darlegung zu dokumentieren.

Zu Doppelbuchstabe bb:

Die Einfügung eines neuen Satzes 4 ist Anlass für eine Folgeänderung.

Zu Buchstabe b:

Der bisherige Absatz 4 wird gestrichen, da der Regelungsgehalt des § 7 NDSG durch die in § 42 getroffenen Regelungen ausreichend abgedeckt wird. Auf Absatz 4 kann daher verzichtet werden.

Zu Buchstabe c:

Die Streichung des Absatzes 4 ist Anlass für eine Folgeänderung.

Zu Nummer 26 (§ 43):

Zur Schaffung einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts werden in § 43 zu Artikel 5 Abs. 1 Buchst. a DS-GVO spezifische Bestimmungen im Sinne des Artikels 6 Abs. 2 und 3 in Verbindung mit Absatz 1 Buchst. e der DS-GVO geschaffen. Artikel 6 Abs. 2 und 3 DS-GVO ermöglicht es, spezifischere Bestimmungen zu erlassen, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten und Rechtsgrundlagen zur Anpassung der Anwendung der in der DS-GVO enthaltenen Vorschriften zu schaffen. Danach können spezifische Regelungen zum Zweck der Übermittlung und zu den empfangenden Stellen geschaffen werden. Da das NDSG zu den in § 43 vorgesehenen Regelungen keine Entsprechung enthält, ist eine Sondervorschrift im NPOG erforderlich.

In § 43 soll künftig nur noch die Datenübermittlung ins EU-Ausland und die Schengen-assoziierten Staaten geregelt werden. Dazu wird zunächst die Überschrift entsprechend dem Regelungszweck angepasst.

Nach Artikel 9 Abs. 4 DS-RL sind Datenübermittlungen ins EU-Ausland unter den gleichen Voraussetzungen zulässig wie Datenübermittlungen im Inland. Das wird durch den neuen § 43 umgesetzt und konkretisiert. Durch den Verweis auf die Regelungen des § 41 gilt der in § 39 verankerte Grundsatz der hypothetischen Datenneuerhebung auch für die innereuropäische Datenübermittlung.

Ein effektiver und wirksamer Informationsaustausch zwischen den Sicherheitsbehörden der Mitgliedstaaten der Europäischen Union ist ein Schlüsselelement für die Gewährleistung der Sicherheit der Bundesrepublik Deutschland und der Europäischen Union. Nur durch die intensive grenzübergreifende Zusammenarbeit der europäischen Sicherheitsbehörden bei der Gefahrenabwehr und der Straftatenverhütung und -verfolgung können europaweit Straftaten verhindert, verfolgt und aufgedeckt werden. Vor diesem Hintergrund und der sich stetig vertiefenden europäischen Integration, welche die Europäische Union zu einem gemeinsamen Raum der Freiheit, der Sicherheit und des Rechts gemacht hat, setzt § 43 den Gleichbehandlungsgrundsatz konsequent um und stellt künftig Datenübermittlungen an Mitgliedstaaten der Europäischen Union den inländischen Datenübermittlungen gleich.

Durch Nummer 1 wird die Übermittlung an Behörden, sonstige öffentliche und nichtöffentliche Stellen anderer Mitgliedstaaten der Europäischen Union den Regelungen über die Übermittlung an inländische Stellen gleichgestellt. Den Regelfall von Übermittlungen nach Nummer 1 stellen Übermittlungen an Polizeibehörden oder sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stellen eines Mitgliedstaates der Europäischen Union dar. Als solche können insbesondere jene Stellen gelten, die von diesem Staat gemäß der Richtlinie (EU) 2023/977 des Europäischen Parlaments und des Rates vom 10. Mai 2023 über den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten und zur Aufhebung des Rahmenbeschlusses 2006/960/JI des Rates (ABL 2023 L 134, ABLEU Jahr 2023 L Seite 1) als zentrale Kontaktstelle oder benannte Strafverfolgungsbehörde bestimmt wurden.

Über Nummer 2 wird klargestellt, dass sich auch Datenübermittlungen an zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten, die mit Aufgaben der Verhütung und Verfolgung von Straftaten befasst sind, nach Regelungen über die Übermittlung an Polizeibehörden der Mitgliedstaaten nach Nummer 1 in Verbindung mit § 43 richten. Dies betrifft die nach Kapitel 4 und 5 des V. Titels des dritten Teils des Vertrags über die Arbeitsweise der Europäischen Union errichteten Einrichtungen und sonstigen Stellen, so etwa Europol.

Durch Nummer 3 werden die Schengen-assoziierten Staaten den Mitgliedstaaten der Europäischen Union gleichgestellt. Das sind die Staaten, die die Bestimmungen des Schengen-Besitzstandes aufgrund eines Assoziierungsabkommens mit der Europäischen Union über die Umsetzung,

Anwendung und Entwicklung des Schengen-Besitzstandes anwenden und den Mitgliedstaaten der Europäischen Union insoweit gleichstehen (§ 24 Nr. 16 NDSG), z. B. die Länder Norwegen und Schweiz.

Die bisherigen Absätze 2 bis 5 des § 43 werden an dieser Stelle gestrichen. Die Regelungen aus Absatz 2 zur Datenübermittlung an ausländische öffentliche Stellen werden, mit Ausnahme der EU-Staaten, einer eigenen Rechtgrundlage in § 43 a zugeführt. Die bisherige Regelung in Absatz 3 zur Übermittlung von Daten, die mit besonderen Mitteln oder Methoden erhoben worden sind, wurde als allgemeine Regel zur Datenübermittlung in § 40 aufgenommen. Die Vorschriften des bisherigen Absatzes 4 finden sich in den §§ 46 bis 49 des NDSG und werden in einem neuen § 43 a in Bezug genommen. Auf Absatz 5 kann an dieser Stelle verzichtet werden, da die Übermittlungsverbote und Verweigerungsgründe nunmehr in einer eigenständigen Rechtgrundlage in einem neuen § 44 a zusammengeführt werden.

Zu Nummer 27 (§ 43 a):

Im neuen § 43 a finden sich künftig die Regelungen zu Datenübermittlungen der Polizei im internationalen Bereich, außerhalb der EU-Staaten, die bisher in § 43 Abs. 2 enthalten sind. Bei § 43 a handelt es sich um eine fachspezifische Konkretisierung der Vorgaben in den §§ 46 bis 49 NDSG für Datenübermittlungen an Drittstaaten und an internationale Organisationen, die Artikel 35 bis 39 der DS-RL umsetzen sollen. Die Vorschriften der §§ 46 bis 48 NDSG (Absatz 1 Satz 2) und § 49 NDSG (Absatz 1 Satz 1) sollen aber Beachtung finden.

Mit § 43 a werden lediglich die Artikel 35 bis 39 der DS-RL für die Polizei umgesetzt, da eine einheitliche Regelung für den gesamten Aufgabenbereich des NPOG durch eine Präzisierung der Regelungen in den Artikeln 44 bis 49 der DS-GVO nicht möglich ist. Soweit die Datenübermittlung außerhalb des Anwendungsbereichs der Richtlinie erfolgt, richtet sich diese somit direkt nach den Vorgaben der Artikel 44 bis 49 der DS-GVO. Da im Regelfall eine Übermittlung an Stellen außerhalb der Europäischen Union zu Zwecken der DS-RL erfolgen wird, ist in der Praxis nicht mit nachträglichen Auswirkungen zu rechnen.

Die bisherige Regelung aus § 43 Abs. 2 wird weitgehend übernommen. Nummer 1 enthält wie bisher die Fälle, in denen die Datenübermittlung durch eine andere nationale, europäische oder internationale Rechtsvorschrift vorgesehen ist. Es wird allerdings klargestellt, dass dies auch untergesetzliche Normen sein können. In Nummer 2 wird der Zweck „zur Abwehr einer Gefahr“ auf die „Erfüllung polizeilicher Aufgaben“ erweitert. Damit wird sichergestellt, dass künftig auch die Verhütung von Straftaten, die ebenfalls Aufgabe der Polizei ist, Grund für eine Datenübermittlung sein kann.

Zu Nummer 28 (§ 44):

Zu Buchstaben a, b und c:

Durch die Zusammenführung der Regelungen zu Datenübermittlungen im innerstaatlichen Bereich, im EU-Ausland und im internationalen Bereich in den §§ 41, 43 und 43 a verbleibt als Regelungsgehalt dieser Vorschrift nur die bisherige „Bekanntgabe an die Öffentlichkeit“, die bisher in Absatz 2 vorgesehen ist, der nunmehr inhaltlich unverändert einziger Absatz einer neuen Regelung wird. Gleichzeitig wird die Überschrift geändert, um den Regelungsgehalt der Vorschrift „Veröffentlichung von Daten“ besser zum Ausdruck zu bringen.

Satz 2 bleibt inhaltlich unverändert, wird jedoch zur Erhöhung der Verständlichkeit der Regelung neu gefasst.

Die Regelungsbefugnis nach der DS-GVO ergibt sich für § 44 aus Artikel 6 Abs. 2 und 3 DS-GVO, der es ermöglicht, spezifischere Bestimmungen zu erlassen, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten und Rechtsgrundlagen zur Anpassung der Anwendung der in der DS-GVO enthaltenen Vorschriften zu schaffen. Danach können spezifische Regelungen zum Zweck der Übermittlung und zu den empfangenden Stellen getroffen werden, insbesondere aber auch dazu, an welche Einrichtungen und für welche Zwecke die Daten offengelegt werden dürfen. Da das NDSG zum Regelungsinhalt des § 44 keine Entsprechung enthält, ist eine Sonderregelung im NPOG erforderlich.

Zu Nummer 29 (§ 44 a):

In § 44 a werden Übermittlungsverbote und Verweigerungsgründe an einer Stelle im Gesetz zusammengeführt.

Die Vorschrift soll auf den Bereich der Polizei und damit auf den Anwendungsbereich der DS-RL beschränkt werden.

Für die Verwaltungsbehörden gilt die DS-GVO direkt. Die sich aus Artikel 5 und 6 der DS-GVO ergebenden Grundsätze zur Verarbeitung und die Vorschriften zur Rechtmäßigkeit der Verarbeitung sind insoweit ausreichend.

Die Übermittlungsverbote in Nummer 1 tragen den vom Bundesverfassungsgericht aufgestellten Anforderungen an die Vergewisserung über das Vorhandensein eines datenschutzrechtlich angemessenen und mit elementaren Menschenrechtsgewährleistungen zu vereinbarenden Umgang mit den übermittelten Daten im Empfängerstaat und Artikel 38 der DS-RL Rechnung.

Das Bundesverfassungsgericht (BVerfG, a. a. O., Rn. 339) hat ausgeführt: „*Die Vergewisserung über das geforderte Schutzniveau - sei es generalisiert, sei es im Einzelfall - ist eine nicht der freien politischen Disposition unterliegende Entscheidung deutscher Stellen. Sie hat sich auf gehaltvolle wie realitätsbezogene Informationen zu stützen und muss regelmäßig aktualisiert werden. Ihre Gründe müssen nachvollziehbar dokumentiert werden. Die Entscheidung muss durch die Datenschutzbeauftragten überprüfbar sein und einer gerichtlichen Kontrolle zugeführt werden können*.“

Um diesen Anforderungen gerecht zu werden, wird die Besorgnis der Verletzung von elementaren Rechtsstaatsgrundsätzen und Menschenrechten als Regelbeispiel in Nummer 1 explizit genannt.

Zur Schaffung einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts werden in § 44 a Nr. 2 bis 4 zu Artikel 5 Abs. 1 Buchst. a, b und d DS-GVO spezifische Bestimmungen im Sinne des Artikels 6 Abs. 2 und 3 in Verbindung mit Absatz 1 Buchst. e der DS-GVO geschaffen.

Nrn. 2 bis 4 dienen der Umsetzung der Richtlinie (EU) 2023/977 des Europäischen Parlaments und des Rates vom 10. Mai 2023 über den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten und zur Aufhebung des Rahmenbeschlusses 2006/960/JI des Rates (ABL 2023 L 134, ABLEU Jahr 2023 L Seite 1 - im Folgenden: Richtlinie (EU) 2023/977).

Die Richtlinie (EU) 2023/977 bezweckt, den bestehenden Rechtsrahmen zu modernisieren und den Informationsaustausch innerhalb des Schengen-Raums zu vereinheitlichen. U. a. regelt die Richtlinie (EU) 2023/977 einerseits Datenübermittlungen im repressiv-polizeilichen Bereich, lässt jedoch auch Übermittlungen zum Zwecke der Verhütung von Straftaten zu, die allein Gegenstand der Änderungen des NPOG sind.

Umgesetzt werden hier die in der Richtlinie (EU) 2023/977 enthaltenen Übermittlungsverbote und Verweigerungsgründe.

Der neue § 44 a Nrn. 2 bis 4 beinhaltet die in Artikel 6 Abs. 1 Satz 1 Buchst. f) i), ii) und Satz 2 der Richtlinie (EU) 2023/977 enthaltenen Gründe, aus denen eine Datenübermittlung, die in den Anwendungsbereich der Richtlinie fällt, verweigert werden kann. Die in Artikel 6 der Richtlinie (EU) 2023/977 vorgenommene Aufzählung möglicher Verweigerungsgründe ist dabei abschließend.

In Anlehnung an § 28 BKAG und im Interesse eines effektiven und wirksamen polizeilichen Informationsaustausches in Europa und im internationalen Bereich werden im NPOG drei Fallgruppen aus Artikel 6 Abs. 1 der Richtlinie (EU) 2023/977 umgesetzt. Eine Zurückhaltung von Informationen oder Erkenntnissen ist nach § 44 a Nrn. 2 bis 4 demnach geboten, wenn konkrete Gründe für die Annahme bestehen, dass die Datenübermittlung nationale Sicherheitsinteressen oder laufende Ermittlungen beeinträchtigen würde oder unverhältnismäßig wäre (Artikel 6 Abs. 1 Satz 1 Buchst. f) i), ii) und Satz 2 der Richtlinie (EU) 2023/977).

Hinsichtlich Artikel 6 Abs. 1 Satz 1 Buchst. g) i) der Richtlinie (EU) 2023/977 besteht kein legislativer Umsetzungsbedarf im nationalen Recht, denn ein genereller Einwilligungs- bzw. Genehmigungsvorbehalt der Justiz, wie in der Vorschrift vorausgesetzt, besteht im deutschen Recht nicht. § 478 Abs. 1 Satz 5 StPO befreit vielmehr den innerstaatlichen polizeilichen Datenaustausch ausdrücklich von der vorherigen Einholung einer staatsanwaltschaftlichen oder gerichtlichen Einwilligung bzw. Genehmigung.

Zu Nummer 30 (Überschrift):

An dieser Stelle wird im Gesetz eine weitere neue Überschrift eingefügt, mit der die Vorschriften zum Datenabgleich und zum Verzeichnis von Verarbeitungstätigkeiten in einen 5. Abschnitt zusammenfasst werden.

Zu Nummer 31 (§ 45):

Zu Buchstaben a und b:

Die Änderungen in § 45 sind redaktioneller Art. Es wird jeweils der veraltete Begriff der „Dateien“ durch den Begriff der „Informationssysteme“ ersetzt.

Zu Nummer 32 (§ 45 a):

Vor dem Hintergrund der durch die fortschreitende Digitalisierung stetig wachsenden Datenmengen besteht auch auf Seiten der niedersächsischen Polizei ein hoher Bedarf an einer Fortentwicklung der technischen Instrumente zur Bewältigung großer Datenmengen. In der täglichen Polizeiarbeit ist es mit den derzeit vorhandenen konventionellen Softwarelösungen nicht möglich, besonders große Datensätze im Rahmen einer angemessenen Bearbeitungszeit zu analysieren. Zudem nimmt auch die Kriminalität im digitalen Raum stetig zu, sodass eine effektive Kriminalitätsbekämpfung durch geeignete informationstechnische Systeme zu gewährleisten ist. Die Einrichtung und Nutzung einer automatisierten Anwendung zur Datenanalyse ist daher erforderlich, um auch in Zukunft die polizeilichen Aufgaben vor dem Hintergrund steigender Datenmengen effektiv wahrnehmen zu können. Die automatisierte Datenanalyse ist im Vergleich zum bloßen Datenabgleich darauf gerichtet, neues Wissen erzeugen (BVerfG, Urt. v. 16.02.2023, 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 67).

Für die Einführung einer bereichsspezifischen Rechtsgrundlage für den Einsatz der automatisierten Datenanalyse durch die Polizei hat das Bundesverfassungsgericht mit Urteil vom 16. Februar 2023 zur automatisierten Datenanalyse die verfassungsrechtliche Legitimität von Eingriffsbefugnissen zur automatisierten Datenanalyse sowie die verfassungsrechtlichen Anforderungen an die Regelung einer entsprechenden Rechtsgrundlage für den Einsatz festgestellt. Durch die nun zu schaffende Neuregelung sollen die Vorgaben des Bundesverfassungsgerichts umgesetzt werden.

Das Bundesverfassungsgericht hat in seiner Entscheidung festgelegt, unter welchen Voraussetzungen Eingriffe durch Datenverarbeitungen nicht mehr von den Grundsätzen der Zweckbindung oder hypothetischen Datenneuerhebung gedeckt sind und daher einer eigenen Rechtsgrundlage bedürfen. Maßgebliche Kriterien sind etwa die Fähigkeit zur Auswertung großer und komplexer Informationsbestände (BVerfG, a. a. O., Rn. 69) sowie der Einsatz komplexer Formen des Datenabgleichs (BVerfG, a. a. O., Rn. 90). Anhand dieser Kriterien lässt sich die Eingriffsintensität der Datenverarbeitung bestimmen.

Durch die vorliegende Vorschrift soll für die niedersächsische Polizei die Möglichkeit geschaffen werden, unter Einhaltung der durch das Bundesverfassungsgericht vorgegebenen verfassungsrechtlichen Maßstäbe automatisierte Datenanalysen durchführen zu können. Durch die Datenanalyse sollen bereits vorhandene Datenbestände, die auf Grundlage der jeweils einschlägigen Rechtsgrundlagen bereits rechtmäßig erhoben wurden, ausschließlich zum Zweck der Analyse zusammengeführt und weiterverarbeitet werden.

Auf dieser rechtlichen Grundlage wird die niedersächsische Polizei in die Lage versetzt, die in den polizeilichen Datenbanken vorhandenen Informationen effektiver auszuwerten und komplexe Zusammenhänge zwischen einzelnen Datensätzen transparent darstellen zu können. Die Regelung ist technikneutral formuliert, um auch zukünftig technische Entwicklungen zu erfassen.

Von dieser Vorschrift bleiben die allgemeinen Regelungen zum Datenschutz unberührt und sind daher auch im Rahmen der Anwendung von Systemen zur automatisierten Datenanalyse zu beachten. In diesem Kontext sind vor allem die Anforderungen an die Sicherheit der Datenverarbeitung, die Durchführung einer Datenschutz-Folgeabschätzung, die vorherige Anhörung der oder des Landesbeauftragten für den Datenschutz sowie deren oder dessen Kontrollbefugnisse von Bedeutung.

Zu Absatz 1

Absatz 1 Satz 1 regelt die Eingriffsschwellen für den Einsatz der automatisierten Datenanalyse und beschreibt das technische Verfahren. Dieses besteht aus zwei aufeinander aufbauenden, aber praktisch zeitgleich stattfindenden Schritten. Zunächst erfolgt das Zusammenführen unterschiedlicher Dateisysteme. Anschließend wird die Recherche innerhalb der zusammengeführten Datenbestände durchgeführt, die durch die zuvor erfolgte technische Zusammenführung der Daten ermöglicht wird. Durch das Zusammenführen der Dateien in einem ersten Schritt wird das strukturelle Problem überwunden, dass die polizeilichen Daten in unterschiedlichen Dateiformaten und verschiedenen Dateien gespeichert und damit nicht in demselben Bearbeitungskontext gleichzeitig verfügbar sind. Der

zweite Schritt stellt die eigentliche Analyse dar. Der Prozess der Datenanalyse wird in Absatz 2 näher konkretisiert.

Insofern enthält die Regelung zwei Befugnisse für die niedersächsische Polizei. Zum einen wird die Befugnis der Polizei geregelt, zur Erfüllung ihrer Aufgaben personenbezogene Daten, die sie zur Erfüllung der ihr obliegenden Aufgaben weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat, mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenzuführen. Darüber hinaus wird die Befugnis geregelt, die so zusammengeführten Daten zum Zweck der Analyse weiterzuverarbeiten, sofern die Eingriffsvoraussetzungen erfüllt sind.

Der Einsatz der automatisierten Datenanalyse erfolgt auf Grundlage angemessener Eingriffsschwellen, die sich an den jeweiligen, durch das Bundesverfassungsgericht vorgegebenen Parametern orientieren. In Satz 1 Nr. 1 bis 3 sind drei unterschiedliche Eingriffsschwellen enthalten, welche jeweils die Voraussetzungen für die Nutzung der automatisierten Datenanalyse festlegen. Die Eingriffsschwellen bestehen in Verbindung zu ihrem jeweiligen Eingriffsgewicht, um die Verhältnismäßigkeit der Maßnahme zu wahren.

In Satz 1 werden die im Rahmen der automatisierten Datenanalyse verarbeitbaren Daten zunächst nach Art und Umfang dergestalt begrenzt, dass nur Daten zusammengeführt und weiterverarbeitet werden dürfen, die die Polizei zur Erfüllung der ihr obliegenden Aufgaben weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat. Die Weiterverarbeitung der Daten darf zudem nur zum Zweck der Analyse erfolgen. Dies bedeutet, dass die bereits zusammengeführten Daten im jeweiligen Einzelfall nur in dem Maße verarbeitet werden dürfen, das für den jeweiligen Analysezweck erforderlich ist. Daraus folgt, dass Datenbestände auf der Plattform zusammengeführt werden dürfen, der Inhalt der so zusammengeführten Dateien jedoch nur in dem Umfang verwendet werden darf, wie es die Zweckbindung vorsieht. Diese Vorgaben gelten für sämtliche der in Satz 1 Nr. 1 bis 3 aufgezählten Eingriffsschwellen.

Die in Nummer 1 geregelte Eingriffsschwelle orientiert sich an den engen Voraussetzungen, wie sie im Allgemeinen für eingriffsintensive heimliche Überwachungsmaßnahmen gelten. Die Aufzählung der in Nummer 1 geregelten Rechtsgüter knüpft eng an der Rechtsprechung des Bundesverfassungsgerichts (BVerfG, a. a. O., Rn. 105) an. Zum einen sind besonders gewichtige Rechtsgüter wie Leib, Leben oder Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes umfasst. Zum anderen weist auch der Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt, ein vergleichbares Gewicht auf. Dieses Tatbestandsmerkmal ist jedoch eng auszulegen, sodass darunter etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen zu fassen sind (ebenda).

Voraussetzung ist zudem das Vorliegen einer konkreten Gefahr für ein besonders gewichtiges Rechtsgut. Gemäß § 2 Nr. 1 handelt es sich dabei um eine Sachlage, bei der im einzelnen Fall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für die öffentliche Sicherheit oder Ordnung eintreten wird. Im Vergleich zu den in den Nummern 2 und 3 geregelten Eingriffsschwellen darf das Eingriffsgewicht der Datenanalyse hoch sein, da der Eingriffsanlass unter Voraussetzung einer konkreten Gefahr streng begrenzt ist und zudem hohe Anforderungen an das zu schützende Rechtsgut gestellt werden.

Demgegenüber erlaubt die Eingriffsschwelle in Absatz 1 Nr. 2 weniger gewichtige Eingriffe. Die Formulierung orientiert sich dabei an dem Wortlaut bereits bestehender Rechtsgrundlagen im NPOG für den Einsatz eingriffsintensiver Maßnahmen, wie etwa §§ 34 Abs. 1 Nr. 2 oder 37 Abs. 1 NPOG. Die Eingriffe auf Grundlage des Absatzes 1 Satz 1 Nr. 2 können beim Vorliegen einer konkretisierten Gefahr bereits dann zu rechtfertigen sein, wenn sie dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht dienen, wie dies etwa bei der Verhütung von Straftaten von zumindest erheblicher Bedeutung der Fall ist (BVerfG, a. a. O., Rn. 107). Der Gesetzgeber kann darauf verzichten, das erforderliche Rechtsgut unmittelbar zu benennen, und stattdessen an entsprechende Straftaten anknüpfen, deren Verhütung mit der Befugnis bezweckt ist (BVerfG, a. a. O., Rn. 105). Das Eingriffsgewicht auf Grundlage dieser Eingriffsschwelle wird durch die Einschränkungen in § 45 a Abs. 1 Satz 6 und Abs. 3 Satz 3 NPOG-E gemindert.

Eine hinreichend konkretisierte Gefahr setzt voraus, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen. Allgemeine Erfahrungssätze reichen insoweit allein nicht aus. Es müssen vielmehr Tatsachen festgestellt sein, die im Einzelfall die Prognose eines Geschehens, das zu einer zurechenbaren Verletzung der hier relevanten Schutzgüter führt, tragen. Eine hinreichend konkretisierte Gefahr in diesem Sinne kann danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender

Wahrscheinlichkeit vorhersehen lässt, sofern bereits Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfG, a. a. O., Rn. 106).

Weiterhin ist zu beachten, dass unter den Begriff der Straftat von erheblicher Bedeutung gemäß § 2 Nr. 14 NPOG auch Vorfeldstraftaten wie etwa §§ 89 a und 89 c StGB fallen. Grundsätzlich ist es dem Gesetzgeber verfassungsrechtlich nicht verwehrt, zur Bestimmung der Eingriffsvoraussetzungen auch an die Gefahr der Begehung von Vorfeldtatbeständen anzuknüpfen. Er muss dann jedoch sicherstellen, dass in jedem Einzelfall eine konkrete oder konkretisierte Gefahr für die durch den Straftatbestand geschützten Rechtsgüter vorliegt (BVerfG, a. a. O., Rn. 170; BVerfG, Beschl. v. 28. September 2022, 1 BvR 2354/13, NVwZ-RR 2023, Rn. 134). Dieser Vorgabe trägt die Formulierung der Nummer 2 dadurch Rechnung, dass als tatbestandliche Voraussetzung geregelt ist, dass dann, wenn es sich bei einer Straftat von erheblicher Bedeutung um eine Vorfeldstraftat handelt, die Verwirklichung der Straftat zu einer Gefahr für das geschützte Rechtsgut führen würde. Ergänzend wird auf die Ausführungen in § 34 zu Vorfeldstraftaten verwiesen.

Nach der Eingriffsschwelle in Nummer 3 ist eine automatisierte Datenanalyse bereits im Gefahrenvorfeld möglich. Die Eingriffsschwelle bleibt damit noch hinter einer konkretisierten Gefahr zurück. Dies ist bei weniger gewichtigen Eingriffen zulässig, wenn die Maßnahme dem Schutz hochrangiger, überragend wichtiger oder auch besonders gewichtiger Rechtsgüter dient (BVerfG, Urt. v. 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 107). Die verfassungsrechtliche Voraussetzung der Beschränkung des Eingriffs nur auf besonders gewichtige Rechtsgüter wird durch die Begrenzung der Maßnahme auf terroristische Straftaten gemäß § 2 Nr. 15 erfüllt.

Sofern der Gesetzgeber der Polizei eine Befugnis zur automatisierten Datenanalyse oder -auswertung bereits für die vorbeugende Bekämpfung von Straftaten einräumen will, muss er nach der Rechtsprechung des Bundesverfassungsgerichts zur Wahrung der Verhältnismäßigkeit die Eingriffsintensität der Maßnahme reduzieren (BVerfG, a. a. O., Rn. 112). Die Eingriffsintensität der Maßnahmen nach Nummer 3 wird insbesondere durch die im Weiteren noch zu erläuternden Regelungen in Absatz 1 Satz 6 und Absatz 3 Satz 3 begrenzt.

Gemäß Absatz 1 Satz 2 dürfen ausschließlich rechtmäßig erhobene und gespeicherte Daten in die automatisierte Datenanalyse einbezogen werden. In der Vorschrift wird beispielhaft aufgeführt, welche Datensätze auf der Analyseplattform zusammengeführt werden dürfen. Gemäß Satz 2 können zum Zweck der automatisierten Datenanalyse insbesondere Vorgangsdaten, Falldaten, Daten aus den polizeilichen Auskunftssystemen, Verkehrsdaten, Telekommunikationsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch einbezogen werden.

Von Bedeutung sind insbesondere Daten im Zusammenhang mit der Vorgangsverwaltung. Ein Vorgang umfasst die Unterlagen, die im Zusammenhang mit einer polizeilichen Tätigkeit über eine bestimmte Person, Sache oder sonstigen Gegenstand polizeilichen Handels geführt werden. In dem Vorgang werden vor allem Anzeigen, Ermittlungsberichte und Vermerke, die nicht nur Daten zu Verdächtigen, Beschuldigten oder sonstigen Anlasspersonen enthalten, aufgenommen, sondern etwa auch Daten zu Anzeigeerstattern, Hinweisgebern oder Zeugen. Unter die Vorgangsdaten fallen sowohl die Vorgangssachbearbeitungsdaten als auch die Vorgangsverwaltungsdaten.

Falldaten aus Fallbearbeitungssystemen sollen die polizeiliche Fallbearbeitung bei komplexen, fallübergreifenden Ermittlungen oder Strukturermittlungen unterstützen. Ein Fallbearbeitungssystem geht über die reine Verwaltung von Vorgangsdaten hinaus. Es gibt dem Anwender ein benutzerfreundliches, speziell auf die Aufhellung von Strukturen hin ausgerichtetes Werkzeug an die Hand. Dieses ist weniger personen- als vielmehr ereignisbezogen ausgerichtet und zeigt vor allem Beziehungen zwischen Personen, Institutionen, Objekten und Sachen auf und kann sowohl für präventive als auch repressive Zwecke eingesetzt werden.

Soweit der LfD fordert, die Verwendung von Vorgangs- und Falldaten für die automatisierte Datenanalyse gesetzlich auszuschließen, da auch personenbezogene Daten von Unbeteiligten in den Datensätzen enthalten sind, ist dies abzulehnen. Aus der oben zitierten Rechtsprechung des BVerfG ergibt sich kein konkretes Verbot der Einbeziehung von Fall- oder Vorgangsdaten.

Polizeiliche Auskunftssysteme enthalten personenbezogene Informationen, die im Wesentlichen aus strafrechtlichen Ermittlungsverfahren stammen und in den Systemen sowohl zum Zweck der

vorbeugenden Straftatenbekämpfung als auch zum Zweck der Strafverfolgung und -vollstreckung gespeichert werden. Das polizeiliche Auskunftssystem der niedersächsischen Polizei besteht aus unterschiedlichen Datengruppen. Dazu gehören insbesondere:

– Kriminalaktennachweise: Diese beinhalten Informationen über laufende und abgeschlossene Ermittlungsverfahren, insbesondere die Straftatbestände, wegen derer ermittelt wurde, Datum und Art der Einstellungsverfügung, deren Gründe, Angaben zur Anklageerhebung sowie zum Ausgang des Hauptverfahrens.

– Personenfahndung: Diese listet in einem Katalog den Anlass und den Zweck der Ausschreibung einer Person zur Fahndung mit dem Ziel auf, fahndungsrelevante Erkenntnisse über Täterinnen oder Täter, Tathergang, Zeuginnen oder Zeugen, Geschädigte etc. zu erlangen. Die Personenfahndung dient u. a. der Festnahme oder Aufenthaltsermittlung von Straftäterinnen oder Straftätern (Strafverfolgung) oder dem Schutz von vermissten Personen (Gefahrenabwehr).

– Sachfahndung: Sie dient u. a. der Beweissicherung sowie der Ermittlung von Eigentümern und Besitzern von Sachen, die durch eine Straftat oder auf andere Weise abhandengekommen sind.

– Haftdatei: Sie beinhaltet Daten von Personen, die wegen des Verdachts oder des Nachweises einer rechtswidrigen Tat einer richterlich angeordneten Freiheitsentziehung unterliegen.

– Erkennungsdienst und DNA-Analyse-Datei: Die Erfassung und Speicherung von biometrischen Merkmalen (insbesondere Fingerabdrücke, Lichtbilder und DNA-Identifizierungsmuster) bilden die Grundlage für die Ermittlung von Täterinnen oder Tätern in Strafverfahren, die Zuordnung von Tatortspuren, das Erkennen von Tatzusammenhängen, aber auch die Identifizierung von hilflosen Personen oder unbekannten Toten. Die aus der DNA-Analyse nach § 81 g Strafprozessordnung (StPO) oder § 15 a gewonnenen Identifizierungsmuster werden in einer zentralen DNA-Analyse-Datei (DAD) gespeichert.

Polizeiliche Auskunftssysteme fördern einen schnellen Informationsaustausch über bereits einschlägig in Erscheinung getretene Straftäterinnen oder Straftäter und dienen als Grundlage der Personenüberprüfung und Identifizierung im Rahmen der Aufklärung fahndungsrelevanter Sachverhalte wie Haftbefehle als auch Vermisstenfahndungen. Durch die Einbeziehung dieser Daten in die automatisierte Datenanalyse können beispielsweise Mittäterinnen oder Mittäter identifiziert, Verbindungen skizziert sowie Falldaten miteinander abgeglichen oder Tatbeteiligungen anhand der Haftdaten auch ausgeschlossen werden.

Unter den Begriff der Verkehrsdaten fallen gemäß § 3 Nr. 70 TKG Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind. Darunter fallen Standortdaten (§ 9 Abs. 1 Nr. 1 TDDDG), die im repressiven Bereich über Funkzellenabfragen (§ 100 g Abs. 3 StPO) sowie durch Nutzung eines IMSI-Catchers (§ 100 i Abs. 1 Nr. 2 StPO) erhoben werden können. Im präventiven Bereich ist eine Standortermittlung etwa unter den Voraussetzungen in § 32 b möglich.

Der Begriff der Telekommunikationsdaten umfasst die bei der niedersächsischen Polizei gesondert gespeicherten Datensätze, in denen ausschließlich Daten aus polizeilichen Telefonüberwachungsmaßnahmen gemäß § 100 a StPO und § 33 a zusammengeführt werden. Insbesondere erscheint vor dem Hintergrund der für die polizeiliche Telekommunikationsüberwachung gemäß §100 d StPO im repressiven sowie gemäß § 33 Abs. 1 i. V. m. § 30 Abs. 2 Satz 2 Nr. 2 im präventiven Bereich geltender Kernbereichsschutz sowie die für die durch Telekommunikationsüberwachungsmaßnahmen geltende Zweckbindung, die Einbeziehung von Telekommunikationsdaten in die automatisierte Datenanalyse vertretbar.

Daten aus Asservaten sind aus sichergestellten oder beschlagnahmten Datenträgern extrahierte Daten.

Unter Daten aus dem polizeilichen Informationsaustausch ist das bundesweite webbasierte Fernschreibsystem EPOST 810 zu verstehen. Damit werden polizeiinterne Informationen zwischen den Länderpolizeien ausgetauscht, z. B. Informationen mit hoher Relevanz zu überregionalen Straftäterinnen oder Straftätern und serienmäßig begangenen Straftaten.

Absatz 1 Satz 3 bestimmt, dass Datensätze aus gezielten Abfragen in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen ergänzend einbezogen werden können, soweit dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. Daten aus staatlichen Registern sind etwa Daten aus Melderegistern, dem zentralen

Verkehrsinformationssystem (ZEVIS) oder dem Nationalen Waffenregister, die über die Analyseplattform auf direktem Weg abgefragt werden können, soweit dies für die Aufklärung des jeweiligen Sachverhalts im Einzelfall erforderlich ist. Darüber hinaus erlaubt Satz 3 auch die ergänzende Einbeziehung von einzelnen gesondert gespeicherten Datensätzen aus Internetquellen.

Gemäß Absatz 1 Satz 4 sind die in der Analyseplattform gespeicherten Verkehrsdaten nach Ablauf von zwei Jahren zu löschen, soweit die weitere Speicherung der Daten für die Fallbearbeitung nicht ausnahmsweise erforderlich ist. Durch die hier geregelte Löschpflicht soll beim Einsatz der automatisierten Datenanalyse die Datenmenge begrenzt werden, was sich eingriffsmildernd auswirkt. Soweit mit der Einbeziehung von Verkehrsdaten, insbesondere den aus Funkzellenabfragen gewonnenen Daten (vgl. etwa § 100 g Abs. 3 StPO), in den für die automatisierte Datenanalyse oder -auswertung bereitstehenden Datenpool eine breitere bevorratende Speicherung von Verkehrsdaten möglich ist, müssen jedenfalls die erfassbaren Datenmengen substanziell begrenzt und eine Höchstspeicherungsdauer geregelt sein (BVerfG, Urt. v. 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 85). Die Frist steht jedoch unter dem Vorbehalt, dass die Daten auch nach Ablauf der Zwei-Jahres-Frist im Ausnahmefall nicht zu löschen sind, soweit sie für die Fallbearbeitung erforderlich sind. Aus Transparenzgründen und um eine effektive aufsichtliche Kontrolle gewährleisten zu können, ist die Entscheidung, die Daten nicht zu löschen, gemäß Satz 5 zu begründen.

Gemäß Absatz 1 Satz 6 dürfen personenbezogene Daten, die gemäß Satz 1 Nr. 1 verarbeitet werden sollen und durch den verdeckten Einsatz technischer Mittel in Wohnungen oder den verdeckten Eingriff in informationstechnische Systeme gewonnen wurden, nur zur Abwehr einer dringenden Gefahr in die automatisierte Datenanalyse einbezogen werden. Im Übrigen dürfen diese personenbezogenen Daten nicht in die automatisierte Datenanalyse einbezogen werden. Infolgedessen ist eine Einbeziehung der genannten Datensätze auf Grundlage der Eingriffsschwellen in Satz 1 Nr. 2 und 3 nicht erlaubt. Es handelt sich bei personenbezogenen Daten, die durch den verdeckten Einsatz technischer Mittel in Wohnungen oder den verdeckten Eingriff in informationstechnische Systeme gewonnen wurden, um solche, die aus besonders schwerwiegenden Grundrechtseingriffen herrühren. Die Regelung zielt darauf ab, die Eingriffsintensität der Datenanalyse zu verringern.

Zu Absatz 2:

In Absatz 2 wird die zulässige Methode und Funktionsweise der automatisierten Datenanalyse geregelt. Es wird insbesondere festgelegt, dass es sich um ein technisches Hilfsmittel handelt, durch welches die Polizei in ihrer täglichen Arbeit unterstützt wird, nicht jedoch ihre Arbeitsweise grundsätzlich verändert. So schließt die Regelung aus, dass die Software, losgelöst von menschlichem Zutun, eigenständig kriminelles Verhalten vorhersagt und die zu betrachtenden Sachverhalte bewertet. Die Bewertung der zusammengeführten Informationen ist auch unter Einsatz der automatisierten Datenanalyse nach wie vor durch die polizeilichen Sachbearbeitenden durchzuführen. Der Mensch bleibt daher auch unter Zuhilfenahme des neuen Rechercheinstruments das zentrale Element polizeilicher Tätigkeit.

Absatz 2 Satz 1 bestimmt, dass die automatisierte Datenanalyse die Polizei bei der Erfüllung ihrer Aufgaben unterstützt, indem sie auf Grundlage vordefinierter Regeln Informationen bereitstellt, die es der Polizei ermöglichen, eigene Bewertungen, Prognosen und Entscheidungen zu treffen. Durch die Vorgabe, dass die Software auf Grundlage vordefinierter Regeln einzusetzen ist, wird sichergestellt, dass die Anwendung unveränderlich vorprogrammiert ist und sich daher nicht eigenständig verändern kann (BVerfG, a. a. O., Rn. 101). Durch die Vorgabe wird sichergestellt, dass die Ergebnisse der Datenanalyse aufgrund der (Vor-)Festlegung der einzelnen Verarbeitungsschritte durch einen Menschen grundsätzlich nachvollziehbar sind und infolgedessen auch eine unabhängige Kontrolle ermöglichen (BVerfG, Urt. v. 19. Mai 2020, 1 BvR 2835/17, NJW 2020, 2235 Rn. 192). Der gesamte Vorgang wird von Menschen gelenkt und beherrscht.

Durch die Regelung in Satz 2 werden explizit maschinelle Entscheidungen ausgeschlossen. Auf diese Weise wird gewährleistet, dass Entscheidungen, die das weitere Verfahren betreffen, stets durch einen Menschen getroffen werden. Im Hinblick auf automatisierte Sachverhaltsbewertung in Form von personenbezogenen Gefährlichkeitsaussagen im Sinne eines „predictive policing“ sind die unmittelbar geltende Verbotsvorschrift in Artikel 5 Abs. 1 Buchst. d) KI-VO sowie die dort geregelte Ausnahme zu beachten. Danach ist das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen, verboten. Das Verbot

gilt jedoch nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen. Satz 3 enthält eine nicht abschließende Aufzählung möglicher Einsatzformen der Weiterverarbeitung personenbezogener Daten durch die automatisierte Datenanalyse.

In Satz 4 wird konkretisiert, dass bereits die Auslösung eines Rechercheprozesses durch den Menschen initiiert wird und daher nicht automatisiert erfolgen darf. Der Vorgang der automatisierten Datenanalyse ist daher manuell auszulösen. Aus den Regelungen in den Sätzen 2 und 4 ergibt sich daher, dass der Mensch sowohl am Anfang als auch am Ende eines Analysevorgangs steht. Weiterhin wird das Eingriffsgewicht der Datenanalyse dadurch gemindert, dass die Methode des Suchvorgangs weiter konkretisiert wird. Diese Konkretisierung in den Sätzen 1 bis 4 erfolgt vor dem Hintergrund, dass das Bundesverfassungsgericht in seiner Entscheidung zur automatisierten Datenanalyse festgelegt hat, dass das Eingriffsgewicht der automatisierten Datenanalyse umso höher ist, „*je offener die Methode des Suchvorgangs gestaltet ist und je weniger die automatisierte Datenanalyse oder -auswertung durch - auch mit Erkenntnissen und Annahmen zu dem konkreten Sachverhalt gespeiste - polizeiliche Suchmuster gesteuert wird*“ (BVerfG, a. a. O., Rn. 93). So können die mit einer offenen Suche verbundenen Gefahren „*auch schon durch eine Einschränkung der Datenverarbeitungsmethode gesenkt werden, wenn der Suchvorgang eingrenzend so geregelt ist, dass er einen Bezug zu einem konkreteren Suchanlass voraussetzt*“ (BVerfG, a. a. O., Rn. 95). Vor diesem Hintergrund bestimmt Satz 4, dass die automatisierte Datenanalyse anhand von Suchbegriffen erfolgt, die sich aus einem konkreten Sachverhalt, bezogen auf einen Anlass im Sinne des Absatzes 1 ergeben.

Eine automatisierte Einbeziehung der Datensätze aus Internetquellen ist aufgrund der Regelung in Satz 5 unzulässig, mit der eine direkte Anbindung der Analyseplattform an Internetdienste ausgeschlossen wird. Internetquellen müssen daher für jeden Analysevorgang manuell hinzugezogen werden. Die aus diesen Quellen herangezogenen Rechercheergebnisse müssen jedoch stets zur Aufklärung des Sachverhalts im Einzelfall erforderlich sein.

Durch die Verweisung auf die entsprechende Geltung der §§ 38, 39 und 39 a in Satz 6 wird sichergestellt, dass die weitere Nutzung der Daten im Rahmen der automatisierten Datenanalyse nach den Grundsätzen der Zweckbindung und Zweckänderung verfassungsrechtlich gerechtfertigt ist. Die Verarbeitung personenbezogener Daten im Rahmen der automatisierten Datenanalyse ist daher nur unter den entsprechend geltenden Voraussetzungen der §§ 38, 39 und 39 a möglich.

Zu Absatz 3:

Durch den Einsatz selbstlernender Systeme (KI-Systeme) ergibt sich ein erhöhtes, spezifisches Eingriffsgewicht. Für deren Einsatz werden daher besondere Regelungen in Satz 1 und 2 getroffen. Die Polizei wird durch die Regelung verpflichtet, technisch-organisatorische Maßnahmen für den Einsatz der automatisierten Datenanalyse zu treffen, um die Bildung und Verwendung diskriminierender Algorithmen zu vermeiden und die Nachvollziehbarkeit des verwendeten Verfahrens sicherzustellen. Gemäß Satz 3 ist der Einsatz selbstlernender Systeme bei Maßnahmen nach Absatz 1 Satz 1 Nrn. 2 und 3 ausgeschlossen.

Zu Absatz 4:

Absatz 4 legt fest, dass vor dem Einsatz der automatisierten Datenanalyse durch das Fachministerium in einer Verwaltungsvorschrift die näheren Einzelheiten zum Einsatz der automatisierten Datenanalyse zu bestimmen sind. Das Bundesverfassungsgericht hat dem Gesetzgeber die Möglichkeit eingeräumt, die Verwaltung zu verpflichten, die im Gesetz geregelten Vorgaben in abstrakt-genereller Form, etwa durch eine Verwaltungsvorschrift, weiter zu konkretisieren. Diese bedarf jedoch einer gesetzlichen Grundlage. In dieser hat der Gesetzgeber sicherzustellen, dass die für die Anwendung der Bestimmungen im Einzelfall maßgebliche Konkretisierung und Standardisierung seitens der Behörden nachvollziehbar dokumentiert und veröffentlicht wird. Sofern die Vorgaben zu Art und Umfang der in die automatisierte Datenanalyse oder -auswertung einbeziehbaren Daten und der zulässigen Verarbeitungsmethoden aus dem Gesetz selbst nur begrenzt erkennbar sind, bedürfen sie nachvollziehbarer Konkretisierung und Standardisierung durch die Verwaltung. Der Gesetzgeber hat zu gewährleisten, dass die Verwaltung die für die Durchführung einer automatisierten Datenanalyse oder -auswertung im Einzelfall maßgeblichen Vorgaben und Kriterien in abstrakt-genereller Form festlegt und verlässlich dokumentiert wie auch in einer vom Gesetzgeber näher zu bestimmenden Weise veröffentlicht (BVerfG, a. a. O., Rn. 113).

Insofern bestimmt Satz 1 zunächst, dass in der Verwaltungsvorschrift das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und nähere Vorgaben zu Art und Umfang der verarbeiteten Daten zu bestimmen sind. Durch nähere Vorgaben zum technischen Verfahren in der zu veröffentlichenden Verwaltungsvorschrift soll die Methode der automatisierten Datenanalyse transparent dargestellt werden und von anderen Anwendungen abgegrenzt werden. Durch diese einschränkenden Vorgaben soll konkretisiert werden, welche Anwendungsmodalitäten und technischen Schritte bei dem Einsatz der automatisierten Datenanalyse zulässig sind (siehe auch BVerfG, a. a. O., Rn. 122). Von hoher Bedeutung ist zudem, dass die zusammengeführten und verarbeiteten Daten auch ausreichend vor dem Zugriff nicht berechtigter Personen geschützt sind. Aus diesem Grund hat die Verwaltung vor dem Einsatz der Analysesoftware konkrete Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe in abstrakt-genereller Form festzulegen und zu regeln, um so aufgrund der teils sehr sensiblen Datensätze einen hohen Datenschutz zu gewährleisten. Weiterhin sollen auch nähere Vorgaben zu Art und Umfang der verarbeiteten Daten erfolgen. Auch diese Vorgabe wirkt sich eingriffsmildernd aus, da dadurch Art und Umfang der verarbeiteten Daten weiter eingeschränkt wird. Die Verwaltung muss aus fachlicher Sicht konkret festlegen, welche Daten im Rahmen der bereits vorhandenen gesetzlichen Vorgaben und unter Beachtung des Grundsatzes der Datensparsamkeit für den Einsatz der automatisierten Datenanalyse erforderlich sind. Die durch die Verwaltung erstellte Verwaltungsvorschrift ist des Weiteren in dem jeweiligen Verkündungsblatt zu veröffentlichen. Zudem ist auch die oder der Landesbeauftragte für den Datenschutz bei der Erstellung der Verwaltungsvorschrift mit einzubeziehen, um ein ausreichend hohes Datenschutzniveau auch bereits bei der Festlegung abstrakter Vorgaben für die Datenanalyse zu gewährleisten.

Satz 2 legt durch eine nicht abschließende Aufzählung fest, welche Inhalte die Verwaltungsvorschrift insbesondere aufweisen muss. Inhalt der Verwaltungsvorschrift sind das in Satz 3 näher konkretisierte Rollen- und Rechtekonzept sowie das in Satz 4 beschriebene Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten. Auf Anregung des LfD wurde zudem in Nummer 1 noch ergänzt, dass auch Anforderungen an die Qualifikation der handelnden Personen in der Verwaltungsvorschrift zu regeln sind (vgl. BVerfG, a. a. O., Rn. 117). Weiterhin ist die Art der im Rahmen der automatisierten Datenanalyse zu verarbeitenden Daten durch die Verwaltungsvorschrift ex ante festzulegen. Zudem muss jederzeit gewährleistet werden, dass konkret ersichtlich ist, welche Personen von der Maßnahme betroffen ist. Insofern ist auch der Personenkreis festzulegen, der von der Verarbeitung betroffen ist. Weiterhin sind auch besondere Regelungen über die Verarbeitung von Daten, die durch besonders eingriffsintensive Maßnahmen nach § 33 a bis 37 a erhoben wurden, zu treffen. So sollen Maßnahmen, die besonders intensiv in das Grundrecht auf informationelle Selbstbestimmung Einzelner eingreifen, auch durch flankierende Sonderregelungen in ihrem Eingriffsgewicht gemildert werden, um eine verfassungskonforme Datenverarbeitung zu gewährleisten. Um eine hinreichende Kontrolle der automatisierten Datenanalyse, insbesondere durch außenstehende Stellen, zu gewährleisten, ist eine lückenlose Dokumentation des Verarbeitungsprozesses vorzuweisen. Insofern ist in der Verwaltungsvorschrift konkret zu regeln, welche Prozesse und Sachverhalte in welchem Umfang während des Einsatzes der automatisierten Datenanalyse zu protokollieren sind. Dabei ist insbesondere auch eine personelle Zuordnung durch Protokollierung der individuellen Kennung der jeweils handelnden Personen sicherzustellen.

Aus Satz 3 ergibt sich, dass das Rollen- und Rechtekonzept die Verteilung sachlich eingeschränkter Zugriffsrechte anhand von Aufgabenbereichen regelt. In diesem Konzept wird vorgeschrieben, welche Personen innerhalb der Polizeiorganisation Zugriff auf welche Dateien haben können und mit welchen Rechten und Pflichten dieser Zugriff verbunden ist.

Durch die Bindung an Aufgabenbereiche im Rahmen des Rollen- und Rechtekonzepts wird sichergestellt, dass grundsätzlich niemand sämtliche auf der Analyseplattform zusammengeführten Datenbestände einsehen kann. Die jeweilige zugriffsberechtigte Person kann bei der Bearbeitung nur auf denjenigen Ausschnitt der Datenbestände eines Aufgabenbereichs zugreifen, der ihr auch zugewiesen ist. Auch diese Vorgabe wirkt sich daher eingriffsmindernd aus, da sie den Umfang der jeweils verarbeitbaren Daten reduziert.

In Satz 4 wird das durch Verwaltungsvorschrift einzuführende Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten näher konkretisiert. Durch das Konzept soll der Datenbestand begrenzt und die Eingriffsintensität der Maßnahme weiter verringert werden. Das Konzept regelt, welche personenbezogenen Daten in welcher Weise in die automatisierte Analyse einbezogen werden dürfen.

Zu Absatz 5:

Nach Satz 1 besteht auch für die Einrichtung und wesentliche Änderung eines Systems zur automatisierten Datenanalyse ein Behördenleitervorbehalt. In Satz 2 wird der Behördenleitung die Möglichkeit zur Delegation der Anordnungsbefugnis eingeräumt. Zusätzlich ist die oder der Landesbeauftragte für den Datenschutz vor der Einrichtung und wesentlichen Änderung eines Systems nach Satz 1 anzuhören. Bei Gefahr im Verzug kann auf eine Anhörung verzichtet werden. Die Anhörung ist jedoch im Anschluss an die Gefahrenlage unverzüglich nachzuholen.

Zu Nummer 33 (§ 46):

Durch die grundlegende Neugestaltung des europäischen Datenschutzrechts haben sich weitere Begrifflichkeiten verändert. Die ehemals als „Dateibeschreibung“ und „Verfahrensbeschreibung“ bezeichnete Aufstellung über die beim Verantwortlichen vorgenommenen Datenverarbeitungen wird nunmehr in Artikel 24 der DS-RL als „Verzeichnis von Verarbeitungstätigkeiten“ bezeichnet.

Zu Nummer 34 (Überschrift):

Zur weiteren Vervollständigung der neuen Systematik wird nach § 46 ein neuer 6. Abschnitt mit der Überschrift „Benachrichtigungspflichten, Prüffristen, Berichtigung, Löschung und Einschränkung der Verarbeitung“ eingeführt.

Zu Nummer 35 (§ 46 a):

Mit § 46 a (neu) wird die Benachrichtigung aus § 30 Abs. 4 bis 7 herausgelöst und in eine eigenständige Regelung überführt. Zusätzlich werden die bisherigen Regelungen konkretisiert und damit eine einheitliche und rechtssichere Anwendung ermöglicht.

Die Benachrichtigungspflicht bleibt weiterhin beschränkt auf Daten, die durch besondere Mittel oder Methoden erhoben worden sind. Das steht mit Artikel 12 und 13 der DS-RL im Einklang. Die dort geregelte allgemeine Informationspflicht findet sich als Teil der allgemein datenschutzrechtlich gebotenen Betroffenenrechte in § 50 NDSG. § 50 NDSG ist unabhängig von der bisher in § 30 Abs. 4 geregelten Benachrichtigungspflicht anwendbar. Eine darüber hinausgehende erweiterte Informationspflicht, etwa in Form der Benachrichtigung, wie sie in § 30 Abs. 4 und 5 bisher vorgesehen ist, ist nach Artikel 13 Abs. 2 der DS-RL nur „in besonderen Fällen“ vorzusehen. Diese besonderen Fälle sind auch unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts zum BKAG-Urteil gegeben, wenn Daten verdeckt mit besonderen Mitteln oder Methoden erhoben werden. Eine ähnliche Eingriffsintensität ist auch bei verdeckt angefertigten Aufzeichnungen nach § 32 Abs. 2 und im Rahmen der Befugnis zur Rasterfahndung nach § 37 a angezeigt, sodass für diese Maßnahmen ebenfalls eine Benachrichtigungspflicht im bisherigen § 30 Abs. 4 besteht.

Der LfD hat auch für den Einsatz intelligenter Videoüberwachung nach § 32 Abs. 4, die biometrische Echtzeit-Fernidentifizierung nach § 32 b, den nachträglichen biometrischen Internetabgleich nach § 32 c und den Einsatz von unbemannten Fahrzeugsystemen nach § 32 d eine Benachrichtigung betroffener Personen gefordert. Diese Maßnahmen sind zwar teilweise für die betroffene Person meist ebenfalls nicht wahrnehmbar, sind in der Eingriffstiefe jedoch nicht mit verdeckten Maßnahmen vergleichbar, denn erst im Trefferfall wird eine Betroffenheit erzeugt. Im Hinblick auf die Nutzung intelligenter Videotechnik ergibt sich ebenfalls kein erheblich weitergehender Eingriff, der eine Benachrichtigungspflicht auslösen könnte.

Zu Absatz 1:

In Absatz 1 wird für alle verdeckten Maßnahmen eindeutig geregelt, welche Personen jeweils zu benachrichtigen sind. Die Vorschrift orientiert sich an Vorschriften des Bundes wie § 74 BKAG und § 101 StPO. Es wird die dortige Systematik übernommen. Die zu benachrichtigenden Personen werden in einer differenzierten Terminologie erfasst. Systematisch unterscheidet die neue Regelung Zielpersonen bzw. Personen, gegen die sich die Überwachung richtet, und erheblich mitbetroffene Personen, die grundsätzlich zu benachrichtigen sind. Bei weiteren betroffenen Personen differenzieren die einzelnen Regelungen.

Zunächst gehört zum Kreis der zu Benachrichtigenden die Person, gegen die sich die Maßnahme richtet. Dazu werden je nach Maßnahme verschiedene Begrifflichkeiten verwendet, „Zielperson“, „die Person, gegen die sich die Maßnahme richtete“ und „die von der Maßnahme betroffene Person“. Bei der Rasterfahndung nach § 46 a Abs. 1 Nr. 12 (neu) wird eine weitere Konkretisierung vorgenommen. Danach sind nur diejenigen Personen zu benachrichtigen, gegen die, nach Auswertung der Daten, weitere Maßnahmen getroffen wurden. Die Regelung basiert auf der bundesverfassungsgerichtlichen Rechtsprechung zum Grundrechtseingriff, den es bei der Rasterfahndung dann nicht als

gegeben ansieht, wenn erfasste Daten unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden; in diesem Fall verneint das Bundesverfassungsgericht das Vorliegen eines Eingriffs (BVerfGE 115, 320, 343 ff.).

Die Pflicht zur Benachrichtigung beschränkt sich nicht auf die Zielpersonen. Zu benachrichtigen sind auch erheblich mitbetroffene Personen. Die Beschränkung auf erheblich mitbetroffene Personen ist dem Umstand geschuldet, dass durch die Streubreite der entsprechenden Maßnahmen eine Vielzahl von Personen in vergleichsweise unerheblicher Weise erfasst wird, sodass nicht bei allen aus verfassungsrechtlichen Gründen eine Benachrichtigung geboten ist. Wird etwa in einer Parkanlage ein Gespräch zwischen den Zielpersonen abgehört und werden hierbei auch einzelne „Wortfetzen“ zufällig vorübergehender Personen miterfasst, so erscheint es weder sachgerecht noch aus verfassungsrechtlichen Gründen geboten, diese „vorbeispazierenden“ Personen von der Maßnahme zu benachrichtigen. Gesellen sich hingegen zu den Zielpersonen weitere Personen für einige Dauer hinzu, sodass deren Kommunikationsbeiträge in erheblichem Umfang miterfasst werden, greift die Maßnahme auch in deren Grundrechte in nicht unerheblicher Weise ein und lässt damit die Benachrichtigungspflicht auch diesen gegenüber zur Entstehung gelangen.

Bei einer Telekommunikationsüberwachung und bei dem Auskunftsverlangen zu Verkehrsdaten sollen nach Absatz 1 Nr. 2 und 6 (neu) die Beteiligten der überwachten Telekommunikation bzw. die Beteiligten der betroffenen Kommunikation benachrichtigt werden. Die Benachrichtigungspflicht besteht danach zugunsten aller Anrufer und Angerufenen, in deren Grundrechte durch die polizeiliche Maßnahme eingegriffen wurde.

Bei einem Auskunftsverlangen zu Nutzungsdaten soll nach Absatz 1 Nr. 4 (neu) der Nutzer benachrichtigt werden.

Werden Daten durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen erhoben, sollen nach Absatz 1 Nr. 9 (neu) sowohl der Inhaber als auch die Bewohner der Wohnung benachrichtigt werden. Da Artikel 13 GG die „räumliche Privatsphäre“ schützt, sind auch solche Personen zu benachrichtigen, in deren Grundrecht auf Unverletzlichkeit der Wohnung durch eine Maßnahme eingegriffen wird. Dies sind nach Absatz 1 Nr. 10 Buchst. c) (neu) beim Einsatz einer Vertrauensperson und eines verdeckten Ermittlers auch die Personen, deren nicht allgemein zugängliche Wohnung die Vertrauensperson oder der verdeckte Ermittler betreten hat. Da der Schutz an die Ausgestaltung der Privatsphäre durch den Wohnungsinhaber anknüpft, hat er allerdings den Zutritt verdeckter Ermittler oder Vertrauenspersonen hinzunehmen, wenn er, was insbesondere bei Geschäftsräumen zutrifft, diese dem allgemeinen Verkehr öffnet.

Ist eine Ausschreibung zur polizeilichen Beobachtung erfolgt, so soll nach Absatz 1 Nr. 11 (neu) neben der Zielperson auch eine Benachrichtigung gegenüber demjenigen erfolgen, dessen personenbezogene Daten gemeldet wurden.

Zu Absatz 2:

In dem neuen Absatz 2 werden bisher nicht geregelte Ausnahmen von der Benachrichtigungspflicht aufgenommen. Artikel 13 Abs. 3 DS-RL lässt „gesetzgeberische Maßnahmen“ zu, „nach denen die Unterrichtung der betroffenen Person (…) soweit und solange aufgeschoben werden kann, wie diese Maßnahme in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und sofern den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird.“ Darüber hinaus ist es nach Auffassung des Bundesverfassungsgerichts in bestimmten Fällen sogar geboten, die grundsätzlich zu fordernde Benachrichtigung zu unterlassen. Dies ist insbesondere der Fall, wenn die Benachrichtigung den Eingriff in das Grundrecht vertiefen würde, wenn etwa das kurzfristige Bekanntwerden der Daten keine Spuren hinterlässt bzw. keine Folgen für den Betroffenen hat oder die Überwachung zu keinen verwertbaren Ergebnissen geführt hat (vgl. BVerfGE 109, 279, 365; BVerfGE NJW 2012, 833 ff.).

Mit dem neuen Absatz 2 werden diese Fälle im Fachgesetz normiert und entsprechen den Parallelvorschriften in § 74 Abs. 1 Sätze 2 bis 4 BKAG und § 101 Abs. 4 Sätze 3 bis 5 StPO. Zu der Regelung in § 101 Abs. 4 Sätze 3 bis 5 StPO hat das Bundesverfassungsgericht entschieden, dass diese einer verfassungsrechtlichen Überprüfung standhalten (BVerfG NJW 2012, 833 ff.).

Die Forderung von überwiegenden schutzwürdigen Interessen nach Satz 1 entspricht der Wertung des Bundesverfassungsgerichts, dass es verfassungsrechtlich nicht geboten ist, vergleichbar strenge Benachrichtigungspflichten gegenüber Personen zu begründen, deren Daten nur zufällig

miterfasst wurden oder wenn der Eingriff in das Grundrecht vertieft würde (vgl. BVerfGE NJW 2012, 833 ff.). Entgegenstehende schutzwürdige Interessen sind vor allem der persönliche Lebens- und Intimbereich, die Gefährdung von Leib, Leben oder Gesundheit und von bedeutenden Sachwerten. Es hat eine Abwägung der Interessen im Einzelfall stattzufinden, bei Überwiegen der Gründe für ein Unterbleiben - z. B. bei Konsequenzen geschäftlicher, familiärer oder arbeitsplatzbezogener Art - unterbleibt die Benachrichtigung zwingend. Bisher führten überwiegende schutzwürdige Interessen nach § 30 Abs. 5 Nr. 4 zur Zurückstellung der Benachrichtigung. Angesichts der Rechtsprechung des Bundesverfassungsgerichts wird diese Sachverhaltskonstellation nunmehr als Grund für das Unterlassen einer Benachrichtigung aufgenommen.

Bei nur unerheblich betroffen Personen kann nach Satz 2 eine Benachrichtigung über eine Überwachung der Telekommunikation nach § 33 a, ein Auskunftsverlangen zu Verkehrsdaten nach § 33 c oder einen verdeckten Eingriff in informationstechnische Systeme nach § 33 d unterbleiben, wenn anzunehmen ist, dass ein Interesse an der Benachrichtigung nicht besteht. Von den hier genannten besonders eingriffsintensiven Überwachungsmaßnahmen sind nach Satz 1 grundsätzlich alle direkt betroffenen Personen zu benachrichtigen. In Fällen, in denen die Betroffenheit trotz der Eingriffsintensität der Maßnahme nur unerheblich ist, ist dies jedoch nicht erforderlich. Maßgeblich für die Erheblichkeit des Eingriffs sind dabei insbesondere Zeitdauer, erfasste Datenmenge, Persönlichkeitsrelevanz der erfassten Daten und die Intensität der Auswertung der Daten. Die Bewertung hängt damit von den Umständen des Einzelfalles ab und kann sachgerecht von der sachbearbeitenden Stelle getroffen werden. Sie ist an keine besondere Form gebunden. Dem Vorschlag des LfD, hier den behördlichen Datenschutzbeauftragten oder die behördliche Datenschutzbeauftragte einzubinden, wird nicht gefolgt.

Bezüglich der Nachforschungen zur Identität der Personen nach Satz 3 wird den Hinweisen des Bundesverfassungsgerichts gefolgt, weil sich bei Nachforschungen zur Feststellung der Identität der Betroffenen der Grundrechtseingriff sowohl für die Zielperson als auch für sonstige Beteiligte vertiefen kann und deshalb eine Abwägung getroffen werden muss (BVerfGE 109, 279 ff.). Dabei sind neben der Intensität des Eingriffs der Aufwand zur Identitätsfeststellung und die weiteren Beeinträchtigungen für die Zielperson und andere Beteiligte zu berücksichtigen. Ist demnach die Nachforschung nicht geboten, unterbleibt die Benachrichtigung. Zur Identität der betroffenen Person gehört auch der Wohn- oder Aufenthaltsort.

Zu Absatz 3:

Der neue Absatz 3 entspricht im Wesentlichen der bisher in § 30 Abs. 4 Satz 3 getroffenen Regelung zum Inhalt der Benachrichtigung. Eine Ergänzung ergibt sich aus Artikel 13 Abs. 2 DS-RL. Danach ist auch eine Unterrichtung zur Dauer der Datenspeicherung bzw. zu Kriterien für die Speicherdauer, die Mitteilung der Kategorien von Empfängern der personenbezogenen Daten und die Angabe erforderlich, ob auch Empfänger in Drittländern oder internationale Organisationen als Empfänger in Betracht kommen. Diese Ergänzung wird in dem neuen Absatz 3 umgesetzt.

Zu Absätzen 4 bis 6:

Die neuen Absätze 4 bis 6 entsprechen überwiegend den bisherigen Absätzen 5 bis 7 des § 32, die hier eingefügt werden. Redaktionell wird jeweils der Begriff der „Unterrichtung“ durch den aus dem europäischen Datenschutzrecht stammenden Begriff der „Benachrichtigung“ ersetzt.

Eine inhaltliche Änderung wird in dem bisherigen § 32 Abs. 5, in dem die Zurückstellungsgründe enthalten sind, vorgenommen. In der dortigen Nummer 3 werden neben der Gefährdung von Individualrechtgütern wie Leib, Leben, Freiheit oder anderen ähnlich schützenswerten Belangen einer Person auch die Gefährdung von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, als Zurückstellungsgrund aufgenommen. Eine Gefährdung derartiger Sachen ist ein ähnlich unverzichtbarer und hinreichend gewichtiger Zurückstellungsgrund für eine Beschränkung der Benachrichtigungspflicht, wie die bislang in dieser Regelung aufgenommenen Individualrechtsgüter.

Zu Absatz 7:

An die neuen Absätze 4 bis 6 schließt sich noch ein neuer Absatz 7 an, der eine Regelung für die Benachrichtigung Minderjähriger enthält. Die Benachrichtigung an eine minderjährige Person ist zugleich auch deren gesetzlichen Vertreterinnen und Vertretern zuzuleiten. Absatz 7 trägt damit den Rechten der vertretungsberechtigten Person sowie dem Schutz Minderjähriger Rechnung. Die

Begriffe „gesetzliche Vertreterinnen oder Vertreter“ haben bereits in § 12 a Gefährderansprache, Gefährderanschreiben Verwendung gefunden.

Zu Nummer 36 (§ 47)

Zur Schaffung einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts werden in § 47 zu Artikel 5 Abs. 1 Buchst. d DS-GVO spezifische Bestimmungen im Sinne des Artikels 6 Abs. 2 und 3 in Verbindung mit Absatz 1 Buchst. e der DS-GVO geschaffen. Artikel 6 Abs. 2 und 3 DS-GVO ermöglicht es, spezifischere Bestimmungen zu erlassen, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten und Rechtsgrundlagen zur Anpassung der Anwendung der in der DS-GVO enthaltenen Vorschriften zu schaffen. Danach können spezifische Regelungen zum Zweck der Übermittlung und zu den empfangenden Stellen getroffen werden, insbesondere aber auch dazu, wie lange Daten gespeichert werden dürfen. Da das NDSG zum Regelungsinhalt des § 47 keine Entsprechung enthält, ist eine Sonderregelung im NPOG erforderlich.

Zu Buchstabe a:

Zu Doppelbuchstabe aa:

Mit dem neuen Absatz 1 Satz 1 wird Artikel 5 Satz 1 DS-RL fachgesetzlich umgesetzt und der Grundsatz ausdrücklich formuliert, dass angemessene Fristen für die Überprüfung der Speichererforderlichkeit vorzusehen sind. Gleichzeitig wird der bisherige Satz 1 an die Begrifflichkeiten des europäischen Datenschutzrechts angepasst.

Zu Doppelbuchstabe bb:

Mit dem neuen Satz 5 wird Artikel 5 Satz 2 DS-RL in das NPOG übernommen und geregelt, dass die Beachtung der Aussonderungsprüffristen durch geeignete technische Maßnahmen zu gewährleisten ist.

Zu Buchstabe b:

In einem neuen Absatz 2 werden die Speicherhöchstfristen für bestimmte Kategorien von Personen begrenzt und die Vorgaben des Artikels 6 DS-RL im Fachgesetz umgesetzt. Dies betrifft die in § 31 Abs. 2 Nrn. 2 bis 5 genannten Personen, wie Kontakt- oder Begleitpersonen, Zeuginnen und Zeugen, Hinweisgerberinnen und Hinweisgeber sowie Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie Opfer von Straftaten werden. Diese Personen stehen nicht im unmittelbaren Zusammenhang mit einer abzuwehrenden Gefahr oder einer zu verhütenden Straftat. Insofern sollen für diese Kategorien von Personen verkürzte Speicherhöchstfristen gelten.

Zu Buchstabe c:

Es handelt sich um eine notwendige Folgeänderung, die aufgrund der Einfügung eines neuen Absatzes 2 veranlasst wurde.

Zu Buchstabe d:

Absatz 3 kann an dieser Stelle gestrichen werden. In dem neuen § 47 a, der Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten regelt, wird jeweils klargestellt, dass diese Pflichten nicht nur bei der Durchführung der Prüffristen, sondern auch aus Anlass einer Einzelfallbearbeitung durchzuführen sind.

Zu Nummer 37 (§ 47 a):

Nach § 47 wird mit dem neuen § 47 a eine Vorschrift eingeführt, in der die Berichtigung, die Löschung und die Einschränkung der Verarbeitung personenbezogener Daten geregelt ist.

Zur Schaffung einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts werden in § 47 a zu Artikel 5 Abs. 1 Buchst. d DS-GVO spezifische Bestimmungen im Sinne des Artikels 6 Abs. 2 und 3 in Verbindung mit Absatz 1 Buchst. e DS-GVO geschaffen. Die Vorschrift soll auf den Bereich der Polizei beschränkt werden. Für die Verwaltungsbehörden gilt die DS-GVO direkt. In Artikel 16 bis 20 DS-GVO sind ausreichende Regelungen vorhanden, die keiner Ergänzung im NPOG bedürfen.

Zu Absatz 1:

In einem neuen Absatz 1 wird die bisher nicht im NPOG vorgesehene Berichtigung personenbezogener Daten eingeführt.

Die Vorschrift dient der Umsetzung des Artikels 16 DS-RL, aus dem sich das Recht der betroffenen Person auf „Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung“ ergibt. Aus diesem Recht ergibt sich die Pflicht der verantwortlichen Stelle, diese Verarbeitungsvorgänge vorzunehmen. Diese Pflicht besteht unabhängig davon, ob die betroffene Person darum ersucht. Wenn die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt nach Satz 2 an die Stelle der Berichtigung eine Einschränkung der Verarbeitung.

Zu Absatz 2:

Aus systematischen Gründen wird die Löschung personenbezogener Daten in § 47 a eingefügt und konkretisiert.

Mit § 47 a Abs. 2 wird Artikel 16 DS-RL umgesetzt. Zur Begründung wird auf die Ausführungen zu § 47 Abs. 1 verwiesen.

Neben der Erforderlichkeit, die nunmehr ausführlicher in Absatz 2 Nr. 3 geregelt ist, werden in Nummern 1 und 2 zwei weitere Gründe für eine Löschung personenbezogener Daten eingefügt. Mit Nummer 1 wird berücksichtigt, dass an einzelnen Stellen im Gesetz Löschvorschriften geregelt sind (z. B. § 33 Abs. 5), und klargestellt, dass diese Vorschriften zu beachten sind. In Nummer 2 wird ausdrücklich klargestellt, dass personenbezogene Daten zu löschen sind, wenn die Speicherung unzulässig ist.

Zu Absatz 3:

In Absatz 3 wird die bisherige Regelung aus § 39 a Satz 2 und 3 inhaltlich unverändert, aber redaktionell der neuen Struktur des Gesetzes nachkommend, übernommen und der neue Satz 2 redaktionell an die neuen Begrifflichkeiten angepasst.

Zu Absatz 4:

In Absatz 4 wird eine neue Regelung zur Verarbeitung eingeschränkter Daten aufgenommen. Wie in § 28 Abs. 2 Satz 2 und § 52 Abs. 3 NDSG vorgesehen, wird dies auch im Fachgesetz geregelt. Daten, die in ihrer Verarbeitung eingeschränkt sind, dürfen nur mit Einwilligung der betroffenen Person oder zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand, also, wenn Grund zu der Annahme besteht, dass schutzwürdige Belange der betroffenen Person beeinträchtigt würden (§ 39 a Abs. 1 Nr. 1).

Zu Absatz 5:

Es handelt sich um eine ähnliche Regelung wie in § 28 Abs. 3 NDSG, mit der im Fachgesetz garantiert werden soll, dass gerade bei Informationssystemen eine technische Absicherung der Einschränkung der Verarbeitung sichergestellt ist. Gleichsam wird auch den Artikeln 19 und 20 DS-RL Rechnung getragen.

Zu Nummer 38 (Überschrift):

Zur Umsetzung der neuen systematischen Ordnung des Gesetzes wird nach dem Abschnitt zu Benachrichtigungspflichten, Prüffristen, Berichtigung, Löschung und Einschränkung der Verarbeitung ein neuer 7. Abschnitt eingefügt, mit der Überschrift „Datenschutzkontrolle, Anwendung des Niedersächsischen Datenschutzgesetzes“.

Zu Nummer 39 (§ 48):

Zu Buchstabe a:

Zu Doppelbuchstabe aa:

In § 48 werden besondere Dokumentationspflichten für die dort aufgeführten Maßnahmen geregelt. Durch die Ergänzung der §§ 32 b und 32 c in der Aufzählung wird auch für die biometrische Echtzeit-Fernidentifizierung sowie den nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet eine Dokumentationspflicht eingeführt. Vor dem Hintergrund der potenziellen Eingriffsintensität ist die Aufnahme einer Dokumentationspflicht für diese Maßnahmen geboten. Hierdurch wird auch für diese Maßnahmen eine nachträgliche Kontrolle, insbesondere durch externe Stellen, ermöglicht. Durch die Dokumentation sind die Maßnahmen zudem auch für Dritte nachvollziehbar und führen zu einer größeren Transparenz.

Zu Doppelbuchstabe bb:

Es handelt sich um eine sprachliche Anpassung des § 48 Abs. 1 Satz 2 Nr. 1, da nunmehr nicht alleine Datenerhebungen von der Dokumentationspflicht des § 48 Abs. 1 umfasst sind, sondern auch Datenverarbeitungsvorgänge gemäß den §§ 32 b und 32 c umfasst sind.

Zu Buchstabe b:

Aufgrund der Eingriffsintensität der biometrischen Echtzeit-Fernidentifizierung, des nachträglichen biometrischen Abgleichs mit öffentlich zugänglichen Daten aus dem Internet und der automatisierten Datenanalyse ist eine effektive Kontrolle der Einhaltung datenschutzrechtlicher Vorgaben zu gewährleisten. Aus diesem Grund erhält die oder der Landesbeauftragte für den Datenschutz auch für diese polizeilichen Maßnahmen eine Kontrollbefugnis in § 48 Abs. 2. Durch diese Regelung wird eine hohes Datenschutzniveau gewährleistet.

Zu Nummer 40 (§ 49):

Zur besseren Handhabbarkeit für die Rechtsanwendung erhält § 49 eine neue Struktur. § 49 legt fest, welche Vorschriften des NDSG für die Verarbeitung personenbezogener Daten durch die Verwaltungsbehörden und die Polizei grundsätzlich Anwendung finden, und trifft zugleich klare Abgrenzungsregelungen für das Verhältnis der Vorschriften des NDSG zu den Bestimmungen nach diesem Gesetz. Die Regelung wird an die veränderten Bestimmungen in beiden Gesetzen angepasst.

Zu Nummer 41 (Überschriften):

Es handelt sich um Folgeänderungen, die aus der Einfügung neuer Überschriften resultieren.

Nummer 42 (§ 112):

Entsprechend der Regelung in § 91 BKAG sowie der Begründung hierzu soll eine Weiterverarbeitung und Übermittlung von Daten zunächst auch dann möglich sein, wenn die Daten nicht oder noch nicht nach § 38 a gekennzeichnet sind. In diesem Fall ist für die Weiterverarbeitung und Übermittlung die Errichtungsanordnung maßgeblich, die für die zugrunde liegende Datei bzw. das automatisierte Verfahren am Tag vor dem Inkrafttreten dieses Gesetzes gilt. Im Ergebnis bewirkt die Vorschrift eine Fortgeltung der bisherigen Errichtungsanordnungen für die Altdatenbestände. Die Vorschrift bezieht sich einerseits auf polizeiliche Datenbestände, die bereits vor Inkrafttreten dieses Gesetzes nach den für sie jeweils geltenden Rechtsvorschriften erhoben worden sind. Da eine vollständige technische Umsetzung in den polizeilichen Datenbeständen und Systemen nur sukzessive erfolgen kann und sich über einen längeren Zeitraum erstrecken wird, bezieht sich die Vorschrift andererseits ebenso wie § 91 BKAG aber auch auf künftig (d. h. nach dem Inkrafttreten) auf zu erhebende Datenbestände, bei denen zum Zeitpunkt der Erhebung eine Kennzeichnung aus technischen Gründen nicht möglich ist. Durch die Übergangsvorschrift wird eine ressourcenaufwändige Nachkennzeichnung der (Alt-) Datenbestände vermieden und die Funktionsfähigkeit der Polizei weiterhin gewährleistet. Die (Alt-) Datenbestände unterliegen der regulären Aussonderungsprüfung und Löschung, sodass sich ihr Bestand - und damit auch das Anwendungsfeld der Vorschrift - sukzessive reduziert bei gleichzeitigem Aufwachsen des Datenbestandes, der die Voraussetzungen des § 38 a vollumfänglich erfüllt. Die Übergangsregelung lässt die Möglichkeit unberührt, Altdaten durch eine nachträgliche Kennzeichnung in das neue Datenschutzregime zu überführen.

Zu Artikel 2:

Infolge der Aufwertung des bisherigen 2. Abschnitts des Dritten Teils (Befugnisse zur Datenverarbeitung) des NPOG zu einem eigenen - nunmehr Vierten - Teil rücken die übrigen Teile des Gesetzes auf (Artikel 1 Nr. 48). Der bisherige Sechste Teil etwa wird Siebenter Teil. Der bisherige Sechste Teil regelt den Zwang und in seinem 1. Abschnitt die Erzwingung von Handlungen, Duldungen und Unterlassungen. Nach § 70 Abs. 1 NVwVG werden Verwaltungsakte, die auf die Herausgabe einer Sache oder auf eine sonstige Handlung oder eine Duldung oder Unterlassung gerichtet sind und die nicht unter § 2 Abs. 1 NVwVG fallen, auch wenn sie nicht der Gefahrenabwehr dienen, nach dem Sechsten Teil des Niedersächsischen Polizei- und Ordnungsbehördengesetzes durchgesetzt. Diese Verweisung auf den Sechsten Teil wird zukünftig nicht mehr zutreffen und muss angepasst werden. Um eine reibungslose Verwaltungsvollstreckung nach dem Zweiten Teil des Niedersächsischen Verwaltungsvollstreckungsgesetzes gewährleisten zu können, ist eine Folgeänderung erforderlich, die gleichzeitig mit Artikel 1 Nr. 9 und 48 in Kraft tritt.

Zu Artikel 3:

Artikel 2 trägt dem Zitiergebot aus Artikel 19 Abs. 1 Satz 2 des Grundgesetzes Rechnung.

Zu Artikel 4:

In Artikel 2 wird eine Evaluierungspflicht in das Gesetz aufgenommen. Die Intelligente Videoüberwachung (§ 32 Abs. 4), die biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen (§ 32 b), der nachträgliche biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§ 32 c) und die automatisierte Datenanalyse (§ 45 a), die alle in Artikel 1 dieses Gesetzes neu eingefügt wurden, müssen drei Jahre nach Aufnahme des Wirkbetriebs der hierfür jeweils eingerichteten Systeme unter wissenschaftlicher Begleitung durch die Landesregierung evaluiert werden. Hier sollen insbesondere auch die Fehlerhäufigkeit (z. B. Fehlmeldungen im Rahmen der Intelligenten Videoüberwachung oder Fehlidentifizierungen beim Einsatz der biometrischen Echtzeit-Fernidentifizierung) sowie unbeabsichtigte Auswirkungen (z. B. Ausbildung diskriminierender Algorithmen bei Verwendung KI-basierter Anwendungen) einbezogen werden. Dies ist geboten, da alle Maßnahmen mit zum Teil erheblichen Grundrechtseingriffen für die Betroffenen verbunden sind und deren Wirksamkeit zur Gefahrenabwehr noch nicht ausreichend belegt sind. Dies trägt dem verfassungsrechtlichen Grundsatz Rechnung, dass nur geeignete Maßnahmen rechtlich zulässig sind.

Der Landtag ist jeweils über das Ergebnis der Evaluierung von der Landesregierung zeitnah zu unterrichten.

Zu Artikel 5:

Die umfassenden Änderungen lassen eine Neubekanntmachung zweckmäßig erscheinen.

Zu Artikel 6:

Die Vorschrift bestimmt das Inkrafttreten.

(Verteilt am 12.11.2025)