Gesetzentwurf

Hannover, den 08.12.2020

Fraktion der SPD
Fraktion der CDU

Der Landtag wolle das folgende Gesetz beschließen:

Gesetz zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes

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 1 des Gesetzes vom 17.12.2019 (Nds. GVBl. S. 428), wird wie folgt geändert:

1. Die Gliederung „Dritter Teil Befugnisse der Verwaltungsbehörden und der Polizei“ erhält folgende Fassung:

„Dritter Teil

Allgemeine und besondere Befugnisse der Verwaltungsbehörden und der Polizei“.

2. Die Gliederung „1. Abschnitt Allgemeine und besondere Befugnisse“ wird gestrichen.

3. In § 12 Abs. 5 werden die Worte „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.

4. § 15 Abs. 1 Satz 1 Nr. 1 erhält folgende Fassung:

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

5. In § 15 a Abs. 1 Satz 1 wird das Wort „die“ durch die Worte „dies zur“ ersetzt und nach dem Wort „Identität“ die Worte „unerlässlich ist, insbesondere wenn dies“ eingefügt.

6. Die Gliederung „2. Abschnitt Befugnisse zur Datenverarbeitung“ erhält folgende Fassung:

„Vierter Teil

Befugnisse zur Datenverarbeitung“.

7. Nach § 29 wird die folgende neue Gliederung eingefügt:

„1. Abschnitt

Datenerhebung“.

8. § 30 wird wie folgt geändert:

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

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

c) Die Absätze 4 bis 7 werden gestrichen.

9. § 31 wird wie folgt geändert:

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

b) Es werden die folgenden Absätze 5 und 6 angefügt:

„(5) Die Verwaltungsbehörden und die Polizei dürfen besondere Kategorien personenbezogener Daten nur erheben, wenn dies für die in den Absätzen 1 bis 3 genannten Zwecke unerlässlich ist.

(6) [1]Die an Verarbeitungsvorgängen nach Absatz 5 Beteiligten sind für die besondere Schutzwürdigkeit dieser Daten zu sensibilisieren. [2]Der Zugang zu den personenbezogenen Daten ist zu beschränken. [3]Durch geeignete technische und organisatorische Maßnahmen ist sicherzustellen, dass nachträglich überprüft werden kann, ob und von wem besondere Kategorien personenbezogener Daten eingegeben, verändert oder entfernt worden sind.“

10. Nach § 31 wird der folgende § 31 a eingefügt:

„§ 31 a

Benachrichtigungspflichten

(1) Über die Erhebung personenbezogener Daten 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,
   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,
    c) die Personen, deren nicht allgemein zugängliche Wohnung betreten wurde,

11. des § 37 (Polizeiliche Beobachtung), die Zielperson und die Personen, deren personenbezogene Daten gemeldet wurden,

12. des § 45 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 Nr. 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 an deren gesetzliche Vertreterinnen und Vertreter zu richten."

11. Der bisherige § 31 a wird § 31 b.

12. Nach § 31 b wird die folgende neue Gliederung eingefügt:

„2. Abschnitt

Besondere Befugnisse und Maßnahmen der Datenerhebung".

13. § 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 erhält folgende Fassung:

„(1) [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. den Standort eines Mobilfunkendgerätes

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 Standortermittlung nach Absatz 1 Nr. 2 ausschließlich der Ermittlung des Aufenthaltsorts einer gefährdeten Person, so kann abweichend von Absatz 4 die Polizei die Anordnung treffen; § 33 a Abs. 5 Sätze 3 und 4 gilt entsprechend."

14. Nach § 37 b wird die folgende neue Gliederung eingefügt:

„3. Abschnitt

Weiterverarbeitung personenbezogener Daten".

15. § 38 wird wie folgt geändert:

    a) In der Überschrift werden die Worte „Speicherung, Veränderung und Nutzung“ durch das Wort „Weiterverarbeitung“ ersetzt.

    b) Absatz 1 wird durch die folgenden neuen Absätze 1 und 2 ersetzt:

    „(1) [1]Die Verwaltungsbehörden und die Polizei können personenbezogene Daten, die sie selbst erhoben haben, zur Erfüllung derselben Aufgaben 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]Für die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Eingriff in informationstechnische Systeme erlangt wurden, muss im Einzelfall eine Gefahr oder Gefahrenlage nach § 33 d Abs. 1 vorliegen. [5]Für die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in Wohnungen erlangt wurden, muss im Einzelfall eine dringende Gefahr nach § 35 a Abs. 1 vorliegen.

    (2) [1]Die Verwaltungsbehörden und die Polizei dürfen besondere Kategorien personenbezogener nur weiterverarbeiten, wenn dies zu den in den Absatz 1 genannten Zwecken unerlässlich ist. [2]§ 31 Abs. 6 gilt entsprechend.“

    c) Die bisherigen Absätze 2 bis 4 werden gestrichen.

16. Nach § 38 wird der folgende neue § 38 a eingefügt:

„§ 38 a

Kennzeichnung in polizeilichen Dateisystemen

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

1. Angabe des Mittels 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 Absatz 1 gekennzeichnet sind, dürfen so lange nicht weiterverarbeitet oder übermittelt werden, bis eine Kennzeichnung entsprechend den Anforderungen des Absatz 1 erfolgt ist.

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

17. § 39 erhält folgende Fassung:

„§ 39

Weiterverarbeitung personenbezogener Daten
zu anderen Zwecken

(1) Die Verwaltungsbehörden und die Polizei können zur Erfüllung ihrer Aufgaben personenbezogene Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift

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

   werden sollen und
2. sich im Einzelfall Anhaltspunkte
   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.

(2) [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 oder
2. die betroffene Person mit einer den Anforderungen des § 33 des Niedersächsischen Datenschutzgesetzes genügenden Erklärung eingewilligt hat.

[2]In den Fällen des Satzes 1 Nr. 2 sind die Daten für eine sonstige Verwendung in ihrer Verarbeitung einzuschränken.

(3) Abweichend von den Absätzen 1 und 2 können die folgenden Grunddaten einer Person stets weiterverarbeitet werden, um die Identität der 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.

(4) 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 1 Satz 1 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.

(5) [1]Die Verwaltungsbehörden und die Polizei dürfen besondere Kategorien personenbezogener Daten unter den Voraussetzungen der Absätze 1, 2 und 4 nur zu einem anderen Zweck weiterverarbeiten, wenn dies unbedingt erforderlich ist. [2]§ 31 Abs. 6 gilt entsprechend.

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

(7) [1]Die Polizei kann personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten rechtmäßig erhoben oder rechtmäßig erlangt hat, zu Zwecken der Gefahrenabwehr nach den Absätzen 1 bis 5 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 Daten in Dateisystemen 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, können zur Verfolgung von Straftaten weiterverarbeitet werden. [2]Absätze 1 bis 5 gelten entsprechend. [3]Personenbezogene Daten, die durch Herstellung von Lichtbildern oder Bildaufzeichnungen 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 Verzug 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 Verzug enthalten muss; im Übrigen gilt § 33 a Abs. 6 Sätze 3 bis 8 entsprechend."

18. Nach § 39 werden die folgenden §§ 39 a und 39 b eingefügt:

„§ 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 Niedersächsisches Datenschutzgesetz 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 gespeicherte personenbezogene Daten zu statistischen Zwecken verarbeiten. [2]Die Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren.

(3) [1]Die Verwaltungsbehörden und die Polizei dürfen personenbezogene Daten ohne Einwilligung der betroffenen Person 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 ihr 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 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]Die Weiterverarbeitung besonderer Kategorien personenbezogener Daten muss unerlässlich sein. [5]§ 31 Abs. 6 gilt entsprechend.

§ 39 b

Weiterverarbeitung zu Zwecken
der Vorgangsverwaltung und Dokumentation

(1) Die Polizei kann 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 weiterverarbeitet wurden, 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 oder Dienststellenleiter sowie Beamtinnen oder Beamte der Laufbahngruppe 2 ab dem zweiten Einstiegsamt übertragen. [6]Die Entscheidung bedarf der Schriftform; sie ist zu begründen.“

19. Der bisherige § 39 a wird gestrichen.

20. Nach § 39 b wird die folgende neue Gliederung eingefügt:

„4. Abschnitt

Datenübermittlung“.

21. § 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]Dies gilt nicht für mündliche Auskünfte, wenn zur 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 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 Unterrichtung nach § 30 Abs. 4 ein Jahr vergangen ist oder es einer Unterrichtung gemäß § 30 Abs. 7 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 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 auf Grund 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 ist entsprechend anzuwenden.

(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.

(8) Die Absätze 1 bis 6 sowie § 41 gelten entsprechend, wenn Daten innerhalb der Verwaltungs- oder Polizeibehörden weitergegeben werden.“

22. § 41 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„§ 41

Datenübermittlung
im innerstaatlichen Bereich“.

b) Der bisherige Wortlaut wird Absatz 1.

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

„(2) Die Verwaltungs- und Polizeibehörden 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. sie 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.“

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

„§ 41 a

Datenübermittlung zum Zwecke einer Zuverlässigkeitsüberprüfung

(1) [1]Die Polizei darf bei 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 nichtöffentliche 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.“

24. § 42 Abs. 1 wird wie folgt geändert:

    a) Es wird der folgende neue Satz 4 eingefügt:

    „[4]Sollen besondere Kategorien personenbezogener Daten übermittelt werden, ist die Erforderlichkeit der Übermittlung zu dokumentieren.“

    b) Der bisherige Satz 4 wird Satz 5.

25. § 42 a wird wie folgt geändert:

    a) In Satz 1 wird das Wort „Informationssysteme“ durch das Wort „Dateisysteme“ ersetzt.

    b) In Satz 2 wird das Wort „Informationssystemen“ jeweils durch das Wort „Dateisystemen“ ersetzt.

26. § 43 erhält folgende Fassung:

„§ 43

Datenübermittlung im Bereich der
Europäischen Union und deren Mitgliedstaaten

(1) §§ 41 und 42 gelten entsprechend für die Übermittlung von personenbezogenen Daten an

1. öffentliche und nichtöffentliche Stellen in Mitgliedstaaten der Europäischen Union und
2. zwischen- und überstaatlichen Stellen der Europäischen Union oder deren Mitgliedstaaten, die mit Aufgaben der Gefahrenabwehr sowie der Verhütung und Verfolgung von Straftaten befasst sind.

(2) Absatz 1 findet auch Anwendung auf die Übermittlung personenbezogener Daten an Polizeibehörden oder sonstige für Gefahrenabwehr oder die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stellen von Staaten, welche die Bestimmungen des Schengen-Besitzstandes auf Grund eines Assoziierungsübereinkommens mit der mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwenden (Schengen-assoziierte Staaten).“

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

„§ 43 a

Datenübermittlung im internationalen Bereich

(1) Die Polizei kann unter Beachtung der §§ 46 bis 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, einem Rechtsakt der Europäischen Gemeinschaften 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) [1]Die Polizei kann unter den Voraussetzungen des Absatzes 1 auch an andere als die dort genannten Stellen personenbezogene Daten übermitteln, wenn dies im besonderen Einzelfall unbedingt erforderlich ist. [2]§ 49 des Niedersächsischen Datenschutzgesetzes gilt entsprechend.“

28. § 44 wird wie folgt geändert:

    a) Die Überschrift erhält folgende Fassung:

    „Veröffentlichung von Daten“.

    b) Absatz 1 wird gestrichen.

    c) Der bisherige Absatz 2 wird einziger Absatz.

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

„§ 44 a

Übermittlungsverbote und Verweigerungsgründe

(1) Die Datenübermittlung nach den §§ 43 und 43 a unterbleibt,

1. soweit Grund zu der Annahme besteht, dass dadurch gegen den Zweck eines deutschen Gesetzes verstoßen würde, oder
2. 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) Die Datenübermittlung nach den §§ 43 und 43 a kann unterbleiben,

1. wenn hierdurch wesentliche Sicherheitsinteressen des Bundes oder der Länder beeinträchtigt würden,
2. wenn die Übermittlung der Daten unverhältnismäßig wäre oder die Daten für die Zwecke, für die sie übermittelt werden sollen, nicht erforderlich sind, oder
3. wenn hierdurch der Erfolg laufender Ermittlungen oder Leib, Leben oder Freiheit einer Person gefährdet würde.“

30. Nach § 44 a wird die folgende neue Gliederung eingefügt:

„5. Abschnitt

Datenabgleich, Verzeichnis von Verarbeitungstätigkeiten“.

31. § 45 wird wie folgt geändert:

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

    b) In Absatz 2 Satz 1 wird das Wort „Dateien“ jeweils durch das Wort „Dateisystemen“ ersetzt.

32. § 46 erhält folgende Fassung:

„§ 46

Verzeichnis von Verarbeitungstätigkeiten
für die polizeiliche Datenverarbeitung

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

33. Nach § 46 wird die folgende neue Gliederung eingefügt:

„6. Abschnitt

Prüffristen, Berichtigung, Löschung und Einschränkung der Verarbeitung“.

34. § 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 Dateisystem 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 neue 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 drei Jahre

nicht überschreiten.“

c) Der bisherige Absatz 2 wird Absatz 3.

d) Der bisherige Absatz 3 wird gestrichen.

35. Nach § 47 wird der folgende neue § 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 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 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 zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben 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 § 31 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 Dateisystemen ist die Einschränkung der Verarbeitung technisch sicherzustellen.“

36. Nach § 47 a wird die folgende neue Gliederung eingefügt:

„7. Abschnitt

Datenschutzkontrolle, Anwendung des Niedersächsischen Datenschutzgesetzes“.

37. § 49 erhält folgende Fassung:

„§ 49

Anwendung des Niedersächsischen Datenschutzgesetzes

Bei der Erfüllung von Aufgaben nach § 1 Abs. 1, 4 und 5 dieses Gesetzes durch die Verwaltungsbehörden und die Polizei finden die Vorschriften des Kapitels II der Datenschutz-Grundverordnung und der §§ 4 bis 6 des Niedersächsischen Datenschutzgesetzes sowie die Vorschriften der §§ 25 bis 32 und das Dritte Kapitel des Zweiten Teils des Niedersächsischen Datenschutzgesetzes nur Anwendung, soweit in diesem Gesetz ausdrücklich auf diese Vorschriften verwiesen wird.“

38. Die bisherigen Gliederungen „Vierter Teil“ bis „Elfter Teil“ werden „Fünfter Teil“ bis „Zwölfter Teil“.

39. 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 XXX (Inkrafttreten des Gesezes) für die betreffenden Dateien und automatisierten Verfahren geltenden Errichtungsanordnungen weiterverarbeitet, insbesondere übermittelt werden.“

Artikel 2

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 3

Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Anlass und Zielsetzung des Gesetzes

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, das Landesdatenschutzgesetz, mit dem Gesetz zur Neuordnung des niedersächsischen Datenschutzrechts vom 24. Mai 2018 (Nds. GVBl. S. 66) angepasst. Unter Berücksichtigung dieses neu gefassten Landesgesetzes und der unmittelbar geltenden Vorschriften der DS-GVO bedarf es auch einer - bereichsspezifischen - Anpassung der datenschutzrechtlichen Bestimmungen im Niedersächsischen Polizei- und Ordnungsbehördengesetz (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 Niedersächsischen Datenschutzgesetzes (NDSG) §§ 23 bis 58 wird hingewiesen. Auch im NPOG wurden Änderungen zur Umsetzung der DS-RL aufgenommen. Darüber hinaus existierten im NPOG bereits vor Inkrafttreten der Datenschutznovelle 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.

Ein weiterer gewichtiger Teil des Gesetzentwurfs dient der Umsetzung der Entscheidung des Bundesverfassungsgerichts (BVerfG) zum Bundeskriminalamtgesetz (BKAG). Mit dem Urteil vom 20. April 2016 - 1 BvR 966/09, 1 BvR 1140/09 - hat das Gericht, unter Zusammenführung der bisherigen Rechtsprechung, entschieden, dass die Ermächtigung im BKAG zum Einsatz von heimlichen Überwachungsmaßnahmen zur Abwehr von Gefahren des internationalen Terrorismus zwar im Grundsatz mit den Grundrechten vereinbar ist, die derzeitige Ausgestaltung von Befugnissen aber in verschiedener Hinsicht dem Verhältnismäßigkeitsgrundsatz nicht genügt. Die Entscheidung betrifft sowohl die Voraussetzungen für die Durchführung solcher Maßnahmen als auch die Frage der Übermittlung der Daten zu anderen Zwecken an dritte Behörden. Die Verhältnismäßigkeitsanforderungen für eine zweckändernde Datenverwendung orientieren sich gemäß den Ausführungen des Gerichts am Grundsatz der hypothetischen Datenneuerhebung. Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten.

Das Urteil bezieht sich zwar auf das BKAG. Seine grundsätzlichen Ausführungen treffen jedoch ebenso auf Ermächtigungsnormen in den Gefahrenabwehrgesetzen der Länder zu. Daher wurden mit dem Gesetz zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze, das am 20.05.2019 in Kraft getreten ist (Nds. GVBl. S. 88), bereits umfangreiche Änderungen durchgeführt, um das damalige Nds. SOG an die Anforderungen des

BVerfG anzupassen. Der Grundsatz der hypothetischen Datenneuerhebung wurde dabei nicht umgesetzt, da im NPOG vergleichbare Regelungen zur zweckändernden Nutzung von Daten enthalten sind. Dies wird mit diesem Gesetzentwurf nachgeholt, um eine bundesweit einheitliche Regelung zu gewährleisten und den ungehinderten Datenaustausch mit den für Gefahrenabwehr zuständigen Bundes- und Landesbehörden auch künftig sicherzustellen.

II. Schwerpunkte des Gesetzes

Der Gesetzentwurf sieht im Wesentlichen Folgendes vor:

1. Verbesserung der Systematik und Übersichtlichkeit des Gesetzes durch Änderung bestehender und Einfügung neuer Gliederungen.
2. Schaffung datenschutzrechtlicher Regelungen im NPOG, die sowohl der Umsetzung der DS-RL dienen als auch den Regelungen der unmittelbar geltenden DS-GVO entsprechen.
3. Anpassung an die durch die DS-RL und DS-GVO geänderten Begrifflichkeiten.
4. Regelungen zu den besonderen Kategorien personenbezogener Daten bezogen auf die unterschiedlichen Verarbeitungsphasen.
5. Überführung der Benachrichtigungsverpflichtung beim Einsatz besonderer Mittel und Methoden bzw. bei der Rasterfahndung in eine eigenständige Regelung (§ 31 a) und Konkretisierung.
6. Schaffung einer eigenständigen Rechtsgrundlage für das Versenden von sogenannten Stillen SMS (§ 33 b).
7. Überarbeitung der Bestimmungen zur Zweckbindung und Zweckänderung (§§ 38 und 39) und Anpassung an den Grundsatz der hypothetischen Datenneuerhebung.
8. Schaffung einer neuen eigenständigen Regelung zur Kennzeichnung in polizeilichen Dateisystemen (§ 38 a).
9. Schaffung neuer eigenständiger Rechtsgrundlagen für die Weiterverarbeitung personenbezogener Daten zu besonderen Zwecken und zu Zwecken der Vorgangsverwaltung und Dokumentation (§§ 39 a und 39 b).
10. Neustrukturierung und Anpassung der Datenübermittlungsbefugnisse zur Umsetzung der DS-RL und Anpassung an die DS-GVO.
11. Einführung einer spezifischen Rechtsgrundlage für Datenübermittlungen durch die Polizei an öffentliche oder nichtöffentliche Stellen zum Zwecke einer Zuverlässigkeitsüberprüfung.
12. Ergänzung der Regelung zu den Prüffristen im Hinblick auf die besonderen Kategorien personenbezogener Daten und die Personenkategorie.

III. Wesentliches Ergebnis der Gesetzesfolgenabschätzung

Mit den vorgeschlagenen gesetzlichen Änderungen sollen zwingend notwendige Umsetzungen und Anpassungen an das europäische Datenschutzrecht und die Rechtsprechung des BVerfG 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 BVerfG wahrzunehmen.

IV. Auswirkungen auf die Umwelt, den ländlichen Raum und die Landesentwicklung, auf Schwerbehinderte, auf die Verwirklichung der Gleichstellung von Männern und Frauen sowie auf Familien

Keine.

V. Voraussichtliche Kosten und haushaltsmäßige Auswirkungen

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 Bundeskriminalamtgesetz vom 20. April 2016 und dienen deren Umsetzung. Die für die IT-seitige Anpassung aufzuwendenden Mittel können derzeit noch nicht konkret beziffert werden.

Ein eventuell entstehender Haushaltsmittelmehrbedarf für Personal- und Sachkosten wird grundsätzlich mit vorhandenen Mitteln im Rahmen einer Prioritätensetzung ausgeglichen.

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, so dass 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 welchen 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 NDSG zuzurechnen sein. Entsprechend Artikel 1 Abs. 1 der DS-GVO 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 Nummern 1 und 2 (Gliederungen):

Mit diesem Gesetzentwurf soll die Systematik des Gesetzes verbessert werden, um mehr Übersichtlichkeit zu erreichen. Dazu werden neue Gliederungen eingefügt und bestehende Gliederungen 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 Gliederungen 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 Gliederung „1. Abschnitt“ gestrichen werden kann.

Zu Nummer 3 (§ 12):

Bei der Regelung zur Befragung in § 12 ist eine Anpassung der in Absatz 5 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 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 Nummern 4 und 5 (§§ 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 GSDVO 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 der Begriffe „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. 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 Nummern 6 und 7 (Gliederungen):

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 8 (§ 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:

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

Zu Buchstabe c:

Die Absätze 4 bis 7, in denen die Benachrichtigung geregelt ist, werden an dieser Stelle gestrichen. Die Benachrichtigung erhält aufgrund ihrer Bedeutung mit § 31 a (neu) eine eigenständige Rechtsgrundlage und wird grundlegend überarbeitet.

Zu Nummer 9 (§ 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 der 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 den neu eingefügten Absätzen 5 und 6 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. 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 Nummern 4 und 5 wird verwiesen.

Die nach Artikel 10 der DS-RL erforderlichen „Garantien für die Rechte und Freiheiten der betroffenen Person“ werden durch Absatz 6 und die §§ 38 ff. (neu) gewährleistet. Mit Absatz 6 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 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.

Zu Nummer 10 (§ 31 a):

Mit § 31 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 BVerfG 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.

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 Strafprozessordnung. 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 § 31 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 BVerfG 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“ zu-

fällig 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. Nach § 15 des Telemediengesetzes ist Nutzer jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen.

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. § 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 BVerfG 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 BVerfG 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 BVerfG, 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 BVerfG wird diese Sachverhaltskonstellation nunmehr als Grund für das Unterlassen einer Benachrichtigung aufgenommen.

Bei nicht erheblich betroffen Personen kann nach Satz 2 eine Benachrichtigung unterbleiben, wenn anzunehmen ist, dass ein Interesse an der Benachrichtigung nicht besteht. Die Benachrichtigung steht im Ermessen.

Bezüglich der Nachforschungen zur Identität der Personen nach Satz 3 wird den Hinweisen des BVerfG 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 § 13 Abs. 2 der 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 einen Minderjährigen muss danach auch an die gesetzlichen Vertreterinnen oder Vertreter gerichtet werden. 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 11 (§ 31 b):

Es handelt sich um eine notwendige Folgeänderung durch die Einfügung einer neuen Vorschrift.

Zu Nummer 12 (Gliederung):

Nach § 31 b (neu) 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 13 (§ 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 wiederspiegeln, 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 Buchstaben 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 14 (Gliederung):

Nach § 37 a 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 anderen Polizeigesetzen der 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 15 (§ 38):

Zu Buchstabe a:

In der Überschrift des § 38 wird der Begriff der „Weiterverarbeitung“ eingeführt. Zur Begründung wird auf die Ausführungen zu Nummer 14 verwiesen.

Zu Buchstabe b:

§ 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 BVerfG entwickelten Kriterien zur Abgrenzung von der Zweckänderung werden wie auch in § 12 BKAG im Wortlaut übernommen.

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 zugrundeliegenden Rechtfertigungsgründe stützen und unterliegt damit nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung. Die zulässige Reichweite solcher Nutzungen richtet sich nach der Ermächtigung für die Datenerhebung. Die jeweilige Eingriffsgrundlage bestimmt Behörde, Zweck und Bedingungen der Datenerhebung und definiert damit die erlaubte Verwendung. Die Zweckbindung der auf ihrer Grundlage gewonnenen Informationen beschränkt sich folglich nicht allein auf eine Bindung an bestimmte, abstrakt definierte Behördenaufgaben, sondern bestimmt sich nach der Reichweite der Erhebungszwecke in der für die jeweilige Datenerhebung maßgeblichen Ermächtigungsgrundlage. Eine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung kommt damit nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich. [...] Folglich widerspricht es nicht von vornherein dem Gebot einer dem ursprünglichen Erhebungszweck entsprechenden Verwendung, wenn die weitere Nutzung solcher Daten bei Wahrnehmung derselben Aufgabe auch unabhängig von weiteren gesetzlichen Voraussetzungen als bloßer Spurenansatz erlaubt wird. Die Behörde kann die insoweit gewonnenen Kenntnisse zum Schutz derselben Rechtsgüter und im Rahmen derselben Aufgabenstellung - allein oder in Verbindung mit anderen ihr zur Verfügung stehenden Informationen - als schlichten Ausgangspunkt für weitere Ermittlungen nutzen. (…) Für die Wahrung der Zweckbindung kommt es demnach darauf an, dass die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt.“

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.

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 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 oder 35 a erlangt wurden, sieht Satz 4 daher vor, dass eine Gefahr im Sinne der Vorschrift vorliegen muss.

Zu Absatz 2:

Ebenso wie bei der Datenerhebung in § 31 Abs. 5 (neu) wird auch für die Weiterverarbeitung von besonderen Kategorien personenbezogener Daten eine § 31 Abs. 5 (neu) entsprechende Vorschrift eingefügt. Zur Begründung wird auf die Ausführungen zu Nummer 9 verwiesen. Auch die in Absatz 6 geregelten weiteren Schutzmaßnahmen sollen entsprechend auch für die Weiterverarbeitung der Daten gelten. Dazu wird auf § 31 Abs. 6 (neu) verwiesen.

Zu Buchstabe c:

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 16 (§ 38 a):

Der vom BVerfG 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 (Nr. 1), bei Personen, zu denen Grunddaten angelegt wurden, durch die Angabe der Kategorie der betroffenen Person (Nr. 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 (Nr. 3) und durch die Angabe der Stelle, die sie erhoben hat (Nr. 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 zugrundeliegenden Mittel ergänzt werden.

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 Absatz 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 17 (§ 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 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.

Zu Absatz 1:

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 1 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. Dies wird durch den Passus „unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift“ im Gesetzestext verdeutlicht. 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 Anhaltspunkte 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 1 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.

Zu Absatz 2:

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

In den neuen Absatz 2 werden die bisher in § 39 Abs. 1 Satz 1 Nrn. 2 und 3 bestehenden zweckändernden Regelungen ohne Änderungen übernommen. § 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.

Zu Absatz 3:

Der neue Absatz 3 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.

Zu Absatz 4:

Absatz 4 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.

Zu Absatz 5:

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 BVerfG in der grundlegenden Entscheidung zum BKAG nicht gefordert.

Im neuen Absatz 5 wird auch für die zweckändernde Weiterverarbeitung eine Sonderregelung nach dem Vorbild der §§ 31 Abs. 5 (neu) und 38 Abs. 2 (neu) eingefügt. Zur Begründung wird auf die Ausführungen zu Nummer 9 verwiesen.

Zu Absatz 6:

In Absatz 6 wird neu die Verpflichtung zur Sicherstellung der Beachtung der Absätze 1 bis 4 durch organisatorische und technische Maßnahmen nach dem Vorbild des § 12 Abs. 5 BKAG normiert, um insbesondere die Einhaltung der Grundsätze der hypothetischen Datenneuerhebung in polizeilichen Informationssystemen zu gewährleisten.

Der bisherige Absatz 6 wird zu Absatz 9 (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 1 bis 5 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 1 bis 5 in Satz 2 aufgenommen.

Der neue Satz 3 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 dies nach Auffassung des Bundesverfassungsgerichts durch eine Übermittlung von Daten aus einer präventiv angeordneten optischen Wohnraumüberwachung nicht unterlaufen werden darf.

Zu Absatz 9:

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

Zu Absatz 10:

Absatz 10 entspricht inhaltlich unverändert § 39 Abs. 4.

Zu Nummer 18 (§§ 39 a und 39 b):

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 § 39 a:

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. Gleichzeitig werden mit einem Verweis auf § 25 Abs. 5 NDSG die dort enthaltenen Voraussetzungen für anwendbar erklärt. Diese Vorschrift wiederum setzt europäisches Datenschutzrecht, hier Artikel 9 Abs. 2 der DS-RL um.

Diese Regelung dient der Umsetzung der DS-RL, entspricht aber gleichzeitig auch dem Regelungsregime der DS-GVO, da § 25 Abs. 5 NDSG die Vorgaben aus § 13 Abs. 1 bis 4 NDSG für entsprechend anwendbar erklärt. Dabei handelt es sich um ergänzende Vorschriften zur DS-GVO.

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 aus § 38 Abs. 4 inhaltlich unverändert übernommen.

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.

Zu Absatz 4:

Der neue Absatz 4 enthält inhaltlich unverändert die bisherige Regelung aus § 38 Abs. 3 zur Aufnahme von fernmündlichen Hilfeersuchen und Mitteilungen. Die bisherige Regelung wird durch eine Regelung für die Verarbeitung besonderer Kategorien personenbezogener Daten ergänzt. Der Verweis auf § 31 Abs. 6 stellt sicher, dass die dort formulierten besonderen Anforderungen an die Verarbeitung dieser Daten auch hier zur Anwendung kommen.

Zu § 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. Der Geltungsbereich, des bisher ohnehin primär auf die polizeiliche Datenverarbeitung zugeschnittenen § 39 Abs. 2 wird auf die Polizei beschränkt. 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.

Zu Nummer 19 (§ 39 a):

Die bisherige Regelung zur Löschung von Daten in § 39 a wird an dieser Stelle gestrichen und aus systematischen Gründen nach den Datenübermittlungsvorschriften in einem neuen 5. Abschnitt mit der Überschrift „Berichtigung, Löschung und Einschränkung der Verarbeitung“ verortet.

Zu Nummer 20 (Gliederung):

Der neuen Systematik des Gesetzes folgend wird an dieser Stelle ein neuer 4. Abschnitt mit der Überschrift „Datenübermittlungen“ 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 im internationalen Bereich geregelt werden. Mit § 44 a werden Übermittlungsverbote und Verweigerungsgründe an einer Stelle in einer Vorschrift zusammengeführt.

Zu Nummer 21 (§ 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 BVerfG aufgestellte Grundsatz der hypothetischen Datenneuerhebung wie vom Gericht gefordert (s. 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 dahingehend 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 BVerfG 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 als neuer Satz 6 unverändert 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 ohne inhaltliche Änderung als Sätze 7 und 8 in die neue Fassung des Absatzes 1 übernommen.

Zu Absatz 2:

Absatz 2 entspricht 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.

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.

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.

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 DSGVO 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.

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.

Zu Absatz 7 und 8:

Die Absätze 7 und 8 entsprechen inhaltlich unverändert den bisherigen Absätzen 3 und 5. Durch die Änderungen in § 40 (neu) ist der Verweis in Absatz 8 (neu) auf die Absätze 1, 2 und 4 als Folgeänderung anzupassen.

Zu Nummer 22 (§ 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. Dazu ist zunächst eine Änderung der Überschrift erforderlich, um den neuen Regelungsgegenstand zu verdeutlichen. Der bisherige § 41, der die Datenübermittlung zwischen Verwaltungs- und Polizeibehörden regelt, wird inhaltlich unverändert zum neuen Absatz 1 dieser Vorschrift.

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.

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.

Zu Nummer 23 (§ 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 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 Grundgesetz.

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.

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.

Zu Nummer 24 (§ 42):

In § 42 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 besondere 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.

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

Zu Nummer 25 (§ 42 a):

In § 42 a wird jeweils der Begriff „Datenverarbeitungssystem“ durch den in der DS-GVO und der DS-RL verwendeten Begriff „Dateisystem“ ersetzt.

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.

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 Absatz 1 in § 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.

Zu Absatz 1:

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 Abs. 1 den Gleichbehandlungsgrundsatz konsequent um und stellt künftig Datenübermittlungen an Mitgliedstaaten der Europäischen Union den inländischen Datenübermittlungen gleich. Durch Satz 1 Nr. 1 wird die Übermittlung an Behörden, sonstige öffentliche und nichtöffentliche Stellen anderer Mitgliedstaaten der Europäischen Union den Regelungen über Übermittlung an inländische Stellen gleichgestellt. Über Satz 1 Nr. 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 Satz 1 Nr. 1 in Verbindung mit § 43 Abs. 1 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.

Den Regelfall von Übermittlungen nach Satz 1 Nr. 1 stellen Übermittlungen an Polizeibehörden oder sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union dar. Als solche können insbesondere jene Stellen gelten, die von diesem Staat gemäß Artikel 2 Buchst. a des Rahmenbeschlusses 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. 2006 L 386, ABLEU Jahr 2006 L Seite 89; berichtigt ABl. 2007 L 75, ABLEU Jahr 2007 L Seite 26; sogenannte Schwedische Initiative) benannt wurden.

Zu Absatz 2:

Durch den neuen Absatz 2 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, 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 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. Nach Satz 1 sollen die Vorschriften der §§ 46 bis 49 NDSG 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.

Zu Absatz 1:

Die bisherige Regelung aus § 43 Abs. 2 wird weitgehend übernommen. Lediglich in Satz 1 Nr. 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 Absatz 2:

Mit dem neuen Absatz 2 wird Artikel 39 der DS-RL umgesetzt. Mit dieser Regelung wird unter strengen Voraussetzungen der Kreis der möglichen Empfänger über die in § 43 a (neu) genannten öffentlichen Stellen hinaus, auf sonstige öffentliche Stellen und Private ausgeweitet. Damit sind unmittelbare Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister möglich. Die Regelungen aus § 49 NDSG gelten entsprechend.

Zu Nummer 28 (§ 44):

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.

Zu Nummer 28 (§ 44 a):

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

Zu Absatz 1:

Die Übermittlungsverbote in Absatz 1 tragen den vom BVerfG 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 Absatz 1 Nr. 2 explizit genannt.

Zu Absatz 2:

Zur Schaffung einer kohärenten Regelungslage im Bereich des Gefahrenabwehrrechts werden in § 44 a Abs. 3 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.

Absatz 2 dient der Umsetzung des Rahmenbeschlusses 2006/960/JI vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29.12.2006, S. 89, L 75 vom 15.03.2007, S. 26 - im Folgenden: RbDatA), der auch nach dem Erlass der DS-RL weiterhin Bestand hat. Der auf eine Initiative Schwedens zurückgehende Rahmenbeschluss regelt einerseits Datenübermittlungen im repressiv-polizeilichen Bereich, der Rahmenbeschluss lässt jedoch auch Übermittlungen zum Zwecke der Verhütung von Straftaten zu, die allein Gegenstand der Änderungen des NPOG sind.

Umgesetzt werden hier nur die im RbDatA enthaltenen Übermittlungsverbote und Verweigerungsgründe. Durch die Gleichstellung von Übermittlungen an Behörden, sonstige öffentliche und nichtöffentliche Stellen anderer Mitgliedstaaten der Europäischen Union mit den Regelungen über Übermittlungen an inländische Stellen in § 43 ist eine Umsetzung anderer Vorschriften aus dem RbDatA entbehrlich geworden.

Der neue § 44 a Abs. 2 beinhaltet die in Artikel 10 Abs. 1 und 2 des RbDatA enthaltenen Gründe, aus denen eine Datenübermittlung, die in den Anwendungsbereich des Rahmenbeschlusses fällt, verweigert werden kann. Die in Artikel 10 des RbDatA vorgenommene Aufzählung möglicher Verweigerungsgründe ist dabei abschließend.

Artikel 10 RbDatA unterscheidet grundsätzlich zwischen zwingenden und fakultativen Verweigerungsgründen. Während Artikel 10 Abs. 1 und 2 als fakultative Verweigerungsgründe ausgestaltet sind, („darf ... verweigern" bzw. „kann ...verweigern"), wird Artikel 10 Abs. 3 zwingend formuliert („hat ... zu verweigern"). Die fakultativen Verweigerungsgründe in Artikel 10 Abs. 1 und 2 des RbDatA zeigen lediglich Fallgruppen auf, in denen es den Mitgliedstaaten freigestellt ist, keine Daten zu übermitteln. Ob und inwieweit sie von dieser Möglichkeit Gebrauch machen, bleibt ihnen überlassen.

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 10 RbDatA umgesetzt. Eine Zurückhaltung von Informationen oder Erkenntnissen ist nach § 44 a Abs. 2 demnach denkbar, wenn konkrete Gründe für die Annahme bestehen, dass die Datenübermittlung nationale Sicherheitsinteressen oder laufende Ermittlungen beeinträchtigen würde oder unverhältnismäßig wäre (Artikel 10 Abs. 1 RbDatA).

Hinsichtlich Artikel 10 Abs. 3 RbDatA besteht trotz der zwingenden Ausgestaltung 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 29 (Gliederung):

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

Zu Nummer 30 (§ 45):

Die Änderungen in § 45 sind redaktioneller Art. Es wird jeweils der veraltete Begriff der „Dateien“ durch den im neuen europäischen Datenschutzrecht verwendeten Begriff der „Dateisysteme“ ersetzt.

Zu Nummer 31 (§ 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 32 (Gliederung):

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

Zu Nummer 33 (§ 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.

Zu Buchstabe a:

Zu Doppelbuchstabe aa:

Mit dem neuen Absatz 1 Satz 1 wird Artikel 5 Satz 1 der 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 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 5 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 34 (§ 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 der DS-GVO geschaffen.

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 der 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. Kann die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden, 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 der DS-RL umgesetzt. Zur Begründung wird auf die Ausführungen zu Nummer 33 zu Absatz 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 3 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 Dateisystemen eine technische Absicherung der Einschränkung der Verarbeitung sichergestellt ist. Gleichsam wird auch den Artikeln 19 und 20 der DS-RL Rechnung getragen.

Zu Nummer 35 (Gliederung):

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

Zu Nummer 36 (§ 49):

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

Zu Nummer 37 (Gliederung):

Es handelt sich um eine Folgeänderung, die aus der Einfügung neuer Gliederungen resultiert.

Nummer 36 (§ 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 § 62 vollumfänglich erfüllt. Die Übergangsregelung lässt die Möglichkeit unberührt, Altdaten durch eine nachträgliche Kennzeichnung in das neue Datenschutzregime zu überführen.

Für die Fraktion der SPD	Für die Fraktion der CDU
Wiard Siebels	Jens Nacke
Parlamentarischer Geschäftsführer	Parlamentarischer Geschäftsführer

(Verteilt am 08.12.2020)