

09.05.2018

Gesetzentwurf

der Landesregierung

Gesetz zur Anpassung des Polizeigesetzes des Landes Nordrhein-Westfalen und des Gesetzes über Aufbau und Befugnisse der Ordnungsbehörden

A Problem

Die EU-Datenschutzreform, bestehend aus der sog. Datenschutz-Grundverordnung (DSGVO¹) und der sog. Datenschutz-Richtlinie für Justiz und Inneres (JI-Richtlinie²) ist zum 25. Mai 2016 in Kraft getreten. Die JI-Richtlinie ist bis zum 6. Mai 2018 in nationales Recht umzusetzen. Die DSGVO gilt unmittelbar in den Mitgliedstaaten. Sie wird ab dem 25. Mai 2018 europaweit unmittelbar anwendbar sein.

Der Bund hat mit der Neufassung des Bundesdatenschutzgesetzes (BDSG) vom 30. Juni 2017 bereits den allgemeinen Teil des Datenschutzrechts angepasst. Weitere besondere Bereiche werden noch folgen. Auf Landesebene werden bereichsübergreifende Regelungen mit dem vom Ministerium des Innern vorgelegten Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Nordrhein-Westfälisches Datenschutz-Anpassungs- und Umsetzungsgesetz EU - NRWDSAnpUG-EU - LT-Drs. 17/1981) umgesetzt.

Darauf aufbauend besteht auch im Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW) sowie im Gesetz über Aufbau und Befugnisse der Ordnungsbehörden (OBG) ein datenschutzrechtlicher Anpassungsbedarf. Systematisch gilt das neugefasste Datenschutzge-

¹ 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72)

² 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

Datum des Originals: 08.05.2018/Ausgegeben: 14.05.2018

Die Veröffentlichungen des Landtags Nordrhein-Westfalen sind einzeln gegen eine Schutzgebühr beim Archiv des Landtags Nordrhein-Westfalen, 40002 Düsseldorf, Postfach 10 11 43, Telefon (0211) 884 - 2439, zu beziehen. Der kostenfreie Abruf ist auch möglich über das Internet-Angebot des Landtags Nordrhein-Westfalen unter www.landtag.nrw.de

setz des Landes Nordrhein-Westfalen (DSG NRW-Neu) grundsätzlich für den gesamten Anwendungsbereich des PolG NRW und des OBG. Bereichsspezifische Regelungen gehen jedoch solchen des DSG NRW-Neu vor.

Neben dem EU-Gesetzgeber hat auch das Bundesverfassungsgericht (BVerfG) in seinem sog. BKA-Urteil vom 20. April 2016³ grundsätzliche Aussagen zum polizeilichen Datenschutz getroffen. Wenngleich sich das Urteil formal lediglich auf das bestehende Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) bezieht, gelten die Vorgaben mittelbar auch für die vergleichbaren Regelungen in den Polizeigesetzen der Länder und müssen dementsprechend auch dort umgesetzt werden.

Vor dem Hintergrund der ohnehin anstehenden Umsetzung des EU-Datenschutzpaketes werden mit diesem Gesetzentwurf die o.g. vom BVerfG vorgegebenen Datenschutzgrundsätze gleichzeitig im PolG NRW angepasst. Die gemeinsame Umsetzung ist aufgrund des überschneidenden Sachzusammenhangs zwingend notwendig. Die Erforderlichkeit der Umsetzung der weiteren Vorgaben des BVerfG in Bezug auf die Verhältnismäßigkeit der einzelnen polizeilichen Eingriffsbefugnisse wird demgegenüber parallel überprüft und in einer separaten Novelle eingebracht.

Mit Artikel 2 des Gesetzentwurfs werden die Verweise in § 24 OBG an die Änderungen des PolG NRW unter Berücksichtigung der europäischen Datenschutzreform angepasst. Anders als das Handeln der Polizeibehörden zur Verhütung Ermittlung, Aufdeckung oder Verfolgung von Straftaten unterfällt die nichtpolizeiliche Gefahrenabwehr nach dem OBG unmittelbar und vorrangig dem Geltungsbereich der Datenschutz-Grundverordnung. Der Bereich der Verfolgung und Ahndung von Ordnungswidrigkeiten durch die Ordnungsbehörden ist von der vorliegenden Gesetzesanpassung nicht betroffen. Diese richtet sich nach dem Gesetz über Ordnungswidrigkeiten (OWiG) und gem. § 46 OWiG nach den allgemeinen Gesetzen über das Strafverfahren und nicht nach dem OBG. Die Verfolgung und Ahndung von Ordnungswidrigkeiten durch die Ordnungsbehörden unterfällt der JI-Richtlinie und gem. § 35 Abs. 2 DSG NRW-Neu den richtlinienbezogenen Regelungen des Teils 3 des DSG NRW-Neu.

B Lösung

Der datenschutzrechtliche Änderungsbedarf, der sich zum einen aus der EU-Datenschutzreform und zum anderen aus den Datenschutz-Vorgaben des BVerfG ergibt, soll einheitlich durch diesen Gesetzentwurf im PolG NRW umgesetzt werden, da diese Regelungsmaterien in engem systematischen und sachlichen Zusammenhang stehen. Der vorgelegte Gesetzentwurf wahrt den bisherigen Aufbau des Polizeigesetzes so weit wie möglich und soll damit der Kohärenz, Transparenz und der Erleichterung der Arbeit der Polizei dienen. Die Umsetzung der genannten Vorgaben der EU-Datenschutzreform und des Bundesverfassungsgerichts führen in weiten Teilen zu einer deutlichen Anhebung des datenschutzrechtlichen Niveaus. Aber auch in Bereichen, für die sich kein Regelungsbedarf ergibt, soll das bestehende Datenschutzniveau des PolG NRW beibehalten werden.

Die Änderungen des PolG NRW und die europäische Datenschutzreform haben Auswirkungen auf die Verweise des § 24 des Gesetzes über Aufbau und Befugnisse der Ordnungsbehörden des Landes Nordrhein-Westfalen (OBG), soweit nicht vorrangig die Regelungen der DSGVO und des DSG NRW-Neu gelten.

³ Vgl. Urteil des BVerfG vom 20.04.2016, 1 BvR 966/09 und 1 BvR 1140/09.

C Alternativen

Keine.

D Kosten

Aufgrund einzuhaltender datenschutzrechtlicher Mindeststandards resultierend aus der europäischen Datenschutzrechtsreform werden voraussichtlich ein erhöhter Personal- und Sachkostenbedarf und damit höhere Kosten entstehen. Diese sind jedoch durch die Datenschutzgrundverordnung selbst bzw. die Vorgaben der JI-Richtlinie veranlasst, und nicht durch den vorliegenden Gesetzentwurf. Der Gesetzentwurf versucht unter Berücksichtigung der europäischen Datenschutzreform die bestehenden Eingriffsbefugnisse der Polizei und Ordnungsbehörden zu erhalten und - soweit möglich - keine zusätzlichen Pflichten für die Kommunen zu begründen.

E Zuständigkeit

Zuständig ist das Ministerium des Innern. Beteiligt sind die Staatskanzlei und alle Ressorts.

F Auswirkungen auf die Selbstverwaltung und die Finanzlage der Gemeinden und Gemeindeverbände

s.o. D.

G Finanzielle Auswirkungen auf die Unternehmen und die privaten Haushalte

Keine.

H Geschlechterdifferenzierte Betrachtung der Auswirkungen des Gesetzes

Keine.

G e g e n ü b e r s t e l l u n g

Gesetzentwurf der Landesregierung

Auszug aus den geltenden Gesetzesbestimmungen

Gesetz zur Anpassung des Polizeigesetzes des Landes Nordrhein-Westfalen und des Gesetzes über Aufbau und Befugnisse der Ordnungsbehörden

Artikel 1

Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen

Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW)

Das Polizeigesetz des Landes Nordrhein-Westfalen in der Fassung der Bekanntmachung vom 25. Juli 2003 (GV. NRW. S. 441), das zuletzt durch Artikel 1 des Gesetzes vom [einsetzen: Ausfertigungsdatum und Fundstelle des Sechsten Gesetzes zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen] geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) Die Angabe zu § 9 wird wie folgt gefasst:

„§ 9 Allgemeine Regeln, Befragung, Auskunftspflicht“.

§ 9 Befragung, Auskunftspflicht, allgemeine Regeln der Datenerhebung

b) Die Angabe zum Zweiten Titel wird wie folgt gefasst:

„Zweiter Titel

Verarbeitung von personenbezogenen Daten“.

Zweiter Titel

Datenspeicherung, Datenveränderung und Datennutzung

c) Die Angabe zu § 22 wird wie folgt gefasst:

„§ 22 Datenspeicherung, Prüfungstermine“.

§ 22 Allgemeine Regeln über die Dauer der Datenspeicherung

d) Nach der Angabe zu § 22 werden folgende Angaben eingefügt:

„§ 22a Verarbeitung besonderer Kategorien personenbezogener Daten

- § 22b Kennzeichnung in polizeilichen Dateisystemen“.
- e) Die Angabe zu § 23 wird wie folgt gefasst:
- „§ 23 Weiterverarbeitung von personenbezogenen Daten, Zweckbindung, Zweckänderung“.
- § 23 Zweckbindung bei der Datenspeicherung, Datenveränderung und Datennutzung
- f) Die Angabe zu § 24 wird wie folgt gefasst:
- „§ 24 Weiterverarbeitung zu besonderen Zwecken“.
- § 24 Speicherung, Veränderung und Nutzung von Daten
- g) Nach der Angabe zu § 24 wird folgende Angabe eingefügt:
- „§ 24a Weiterverarbeitung zu wissenschaftlichen Zwecken“.
- h) In der Angabe zu § 26 werden nach dem Wort „Datenübermittlung“ die Wörter „, Übermittlungsverbote und Verweigerungsgründe“ eingefügt.
- § 26 Allgemeine Regeln der Datenübermittlung
- i) Die Angabe zu § 27 wird wie folgt gefasst:
- „§ 27 Datenübermittlung im innerstaatlichen Bereich“.
- § 27 Datenübermittlung zwischen Polizeibehörden
- j) Die Angabe zu § 28 wird wie folgt gefasst:
- „§ 28 Datenübermittlung im Bereich der Europäischen Union und deren Mitgliedsstaaten“.
- § 28 Datenübermittlung an öffentliche Stellen, an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen
- k) Die Angabe zu § 29 wird wie folgt gefasst:
- „§ 29 Datenübermittlung im internationalen Bereich“.
- § 29 Datenübermittlung an Personen oder an Stellen außerhalb des öffentlichen Bereichs
- l) In der Angabe zu § 32 wird das Wort „Sperrung“ durch die Wörter „Einschränkung der Weiterverarbeitung“ ersetzt.
- § 32 Berichtigung, Löschung und Sperrung von Daten

- m) Die Angabe zu § 33 wird wie folgt gefasst:

„§ 33 Benachrichtigung bei verdeckten und eingriffsintensiven Maßnahmen“

§ 33 Errichtung von Dateien, Umfang des Verfahrensverzeichnisses, Freigabe von Programmen, automatisiertes Abrufverfahren

- n) Nach der Angabe zu § 33 werden folgende Angaben eingefügt:

„§ 33a Benachrichtigung im Falle der Verletzung des Schutzes personenbezogener Daten

§ 33b Protokollierung bei verdeckten oder eingriffsintensiven Maßnahmen

§ 33c Datenschutzkontrolle“.

- o) Nach der Angabe zu § 67 wird folgende Angabe eingefügt:

„§ 68 Berichtspflichten gegenüber dem Landtag“.

2. § 9 wird wie folgt geändert:

- a) Die Überschrift zu § 9 wird wie folgt gefasst:

**„§ 9
Allgemeine Regeln, Befragung, Auskunftspflicht“.**

**§ 9
Befragung, Auskunftspflicht,
allgemeine Regeln der Datenerhebung**

- b) Dem Absatz 1 wird der folgende Absatz 1 vorangestellt:

„(1) Die Polizei kann personenbezogene Daten erheben, wenn

1. ihre Kenntnis zur Erfüllung der ihr durch dieses Gesetz oder andere Rechtsvorschriften übertragenen Aufgaben erforderlich ist, soweit nicht die §§ 9 bis 46 die Erhebung besonders regeln. Dies gilt auch für personenbezogene Daten, die von der betroffenen Person offensichtlich öffentlich gemacht wurden oder

2. die betroffene Person wirksam im Sinne des § 38 des Datenschutzgesetzes Nordrhein-Westfalen [einsetzen: Ausfertigungsdatum und Fundstelle], das zuletzt durch Artikel 1 des Gesetzes vom [einsetzen: Änderungsdatum und Fundstelle des (Name des Änderungsgesetzes)] geändert worden ist, eingewilligt hat.

Die Erhebung von besonderen Kategorien personenbezogener Daten richtet sich nach § 22a.“.

- | | |
|--|--|
| <p>c) Der bisherige Absatz 1 wird Absatz 2.</p> | <p>(1) Die Polizei kann jede Person befragen, wenn Tatsachen die Annahme rechtfertigen, dass sie sachdienliche Angaben machen kann, die für die Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich sind. Für die Dauer der Befragung kann die Person angehalten werden.</p> |
| <p>d) Der bisherige Absatz 2 wird Absatz 3 und in Satz 1 wird die Angabe „1“ durch die Angabe „2“ ersetzt.</p> | <p>(2) Eine Person, deren Befragung nach Absatz 1 zulässig ist, ist verpflichtet, auf Frage Namen, Vornamen, Tag und Ort der Geburt, Wohnanschrift und Staatsangehörigkeit anzugeben. Sie ist zu weiteren Auskünften verpflichtet, soweit gesetzliche Handlungspflichten bestehen.</p> |
| <p>e) Der bisherige Absatz 2 wird Absatz 4 und in Satz 2 wird die Angabe „1“ durch die Angabe „2“ ersetzt.</p> | <p>(3) Die Befragung richtet sich an die betroffene Person. Ist deren Befragung nicht oder nicht rechtzeitig möglich oder würde sie die Erfüllung der polizeilichen Aufgabe erheblich erschweren oder gefährden, können die Daten auch ohne Kenntnis der betroffenen Person erhoben werden, wenn dies zur Aufgabenwahrnehmung gemäß Absatz 1 erforderlich ist.</p> |
| <p>f) Der bisherige Absatz 4 wird Absatz 5.</p> | <p>(4) Befragung und Datenerhebung sind offen durchzuführen; eine verdeckte Datenerhebung ist nur zulässig, wenn dies durch Gesetz zugelassen ist.</p> |
| <p>Der bisherige Absatz 5 wird aufgehoben.</p> | <p>(5) Die Erhebung personenbezogener Daten zu unbestimmten oder noch nicht bestimmbar Zwecken ist unzulässig. Eine Datenerhebung über nicht gefahren- oder tatbezogene Merkmale sowie über Erkrankungen oder besondere Verhaltensweisen</p> |

der betroffenen Person ist nur zulässig, soweit dies für Identifizierungszwecke oder zum Schutz der betroffenen Person, von Polizeivollzugsbeamten oder Dritten erforderlich ist.

(6) Werden durch Befragung Daten bei der betroffenen Person oder bei Personen oder Stellen außerhalb des öffentlichen Bereichs erhoben, sind diese in geeigneter Weise über die Rechtsvorschriften für die Datenerhebung sowie entweder über die bestehende Auskunftspflicht oder über die Freiwilligkeit der Auskunft aufzuklären, es sei denn, dies ist wegen besonderer Umstände offenkundig nicht angemessen oder die Erfüllung der polizeilichen Aufgaben wird hierdurch erheblich erschwert oder gefährdet.

g) Folgender Absatz 7 wird angefügt:

„(7) Die Erhebung personenbezogener Daten zu unbestimmten oder noch nicht bestimmbar Zwecken ist unzulässig.“.

§ 14

Erkennungsdienstliche Maßnahmen

3. § 14 Absatz 1 wird wie folgt geändert:

a) In Nummer 1 werden vor dem Wort „eine“ die Wörter „dies für“ und nach dem Wort „Identitätsfeststellung“ die Wörter „unbedingt erforderlich ist, insbesondere wenn dies“ eingefügt.

b) In Nummer 2 wird nach dem Wort „Straftaten“ das Wort „unbedingt“ eingefügt.

(1) Die Polizei kann erkennungsdienstliche Maßnahmen vornehmen, wenn

1. eine nach § 12 zulässige Identitätsfeststellung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist,
2. das zur vorbeugenden Bekämpfung von Straftaten erforderlich ist, weil die betroffene Person verdächtig ist, eine Tat begangen zu haben, die mit Strafe bedroht ist und wegen der Art und Ausführung der Tat die Gefahr der Wiederholung besteht.

(2) Ist die Identität festgestellt, sind in den Fällen des Absatzes 1 Nr. 1 die im Zusammenhang mit der Feststellung angefallenen erkennungsdienstlichen Unterlagen zu vernichten, es sei denn, ihre weitere Aufbewahrung ist nach Absatz 1 Nr. 2 oder anderen Rechtsvorschriften zulässig.

(3) Die betroffene Person ist bei Vornahme der Maßnahme darüber zu belehren, dass sie die Vernichtung der erkennungsdienstlichen Unterlagen verlangen kann, wenn die Voraussetzungen für ihre weitere Aufbewahrung entfallen sind.

(4) Erkennungsdienstliche Maßnahmen sind insbesondere

1. die Abnahme von Finger- und Handflächenabdrücken,
2. die Aufnahme von Lichtbildern,
3. die Feststellung äußerer körperlicher Merkmale,
4. Messungen.

§ 14a

Molekulargenetische Untersuchungen zur Identitätsfeststellung

4. In § 14a Absatz 1 Satz 1 werden die Wörter „die Feststellung der Identität“ durch die Wörter „dies zur Feststellung der Identität unbedingt erforderlich ist, insbesondere wenn dies“ ersetzt.

(1) Zur Feststellung der Identität einer Leiche oder einer hilflosen Person können deren DNA-Identifizierungsmuster mit denjenigen einer vermissten Person abgeglichen werden, wenn die Feststellung der Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist. Zu diesem Zweck dürfen

1. der hilflosen Person oder der Leiche Körperzellen entnommen werden,
2. Proben von Gegenständen mit Spurenmaterial der vermissten Person genommen und
3. die Proben nach den Nummern 1 und 2 molekulargenetisch untersucht werden.

Für die Entnahme gilt § 81a Absatz 1 Satz 2 der Strafprozessordnung entsprechend. Die Untersuchungen nach Satz 2 Nummer 3 sind auf die Feststellung des DNA-Identifizierungsmusters und des Geschlechts zu beschränken. Entnommene Körperzellen sind unverzüglich zu vernichten, wenn sie für die Untersuchung nach Satz 2 nicht mehr benötigt werden. Die DNA-Identifizierungsmuster können zum Zweck des Abgleichs in einer Datei gespeichert werden. Die in der Datei gespeicherten DNA-Identifizierungsmuster dürfen

ausschließlich zum Zweck der Gefahrenabwehr verwendet werden. Sie sind unverzüglich zu löschen, wenn sie zur Identitätsfeststellung nach Satz 1 nicht mehr benötigt werden.

(2) Molekulargenetische Untersuchungen werden auf Antrag der Polizei durch das Amtsgericht angeordnet, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der Freiwilligen Gerichtsbarkeit entsprechend. Für die Durchführung der Untersuchungen gilt § 81f Absatz 2 der Strafprozessordnung entsprechend.

§ 15 Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen

(1) Die Polizei kann bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, personenbezogene Daten, auch durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen, von Teilnehmern erheben, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten oder Ordnungswidrigkeiten begangen werden. Dabei dürfen auch personenbezogene Daten über andere Personen erhoben werden, soweit dies erforderlich ist, um eine Datenerhebung nach Satz 1 durchführen zu können. Bild- und Tonaufzeichnungen, in Dateien suchfähig gespeicherte personenbezogene Daten sowie zu einer Person suchfähig angelegte Akten sind spätestens einen Monat nach der Datenerhebung zu löschen oder zu vernichten, es sei denn, sie werden zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt oder Tatsachen rechtfertigen die Annahme, dass die Person künftig Straftaten begehen wird, und die Aufbewahrung ist zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich.

5. In § 15 Absatz 2 wird die Angabe „Abs. 6 und 7“ durch die Wörter „Absatz 2 und 3 und die Angabe „Abs. 5 und 6“ durch die Wörter „Absatz 3 und 4“ ersetzt.

6. § 15c wird wie folgt geändert:

(2) § 24 Abs. 6 und 7 sowie § 32 Abs. 5 und 6 bleiben unberührt.

§ 15c

Datenerhebung durch den Einsatz körpernah getragener Aufnahmegeräte

(1) Die Polizei kann bei der Durchführung von Maßnahmen zur Gefahrenabwehr und zur Verfolgung von Straftaten oder Ordnungswidrigkeiten mittels körpernah getragener Aufnahmegeräte offen Bild- und Tonaufzeichnungen anfertigen, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine konkrete Gefahr für Leib oder Leben erforderlich ist. Die Erhebung personenbezogener Daten kann auch dann erfolgen, wenn Dritte unvermeidbar betroffen sind. Über die Anfertigung der technischen Aufzeichnungen entscheidet die das Aufnahmegerät tragende Polizeivollzugsbeamtin oder der das Aufnahmegerät tragende Polizeivollzugsbeamte anhand der konkreten Umstände des Einzelfalls.

(2) In Wohnungen (§ 41 Absatz 1 Satz 2) ist die Anfertigung von technischen Aufzeichnungen bei der Durchführung von Maßnahmen zur Gefahrenabwehr und zur Verfolgung von Straftaten oder Ordnungswidrigkeiten nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine dringende Gefahr für Leib oder Leben erforderlich ist. Über die Anfertigung der technischen Aufzeichnungen in Wohnungen entscheidet außer bei Gefahr im Verzug die den Einsatz leitende Polizeivollzugsbeamtin oder der den Einsatz leitende Polizeivollzugsbeamte. Absatz 1 Satz 2 gilt entsprechend.

(3) Der Einsatz der Aufnahmegeräte ist durch geeignete Maßnahmen erkennbar zu machen und den betroffenen Personen mitzuteilen. Bei Gefahr im Verzug kann die Mitteilung unterbleiben. Aufzeichnungen

- sind unzulässig in Bereichen, die der Ausübung von Tätigkeiten von Berufsgeheimnisträgern nach §§ 53 und 53a der Strafprozessordnung dienen. Aufzeichnungen werden verschlüsselt sowie manipulationssicher gefertigt und aufbewahrt.
- a) Absatz 4 Satz 5 wird durch folgenden Satz ersetzt:
- „§ 32 Absatz 3 bleibt unberührt.“
- (4) Die nach Absatz 1 und 2 angefertigten Aufzeichnungen sind zwei Wochen nach ihrer Anfertigung zu löschen. Dies gilt nicht, wenn die Aufzeichnungen zur Gefahrenabwehr oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt werden. Über die Löschung entscheidet die aufzeichnende Beamtin oder der aufzeichnende Beamte mit Zustimmung einer oder eines Vorgesetzten. Für die Verwertung der aus Aufzeichnungen nach Absatz 2 erlangten Erkenntnisse gilt Absatz 6. § 23 Absatz 1 und § 32 Absatz 5 bleiben unberührt.
- (5) Die Aufzeichnung personenbezogener Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, ist unzulässig. Der Aufzeichnungsvorgang ist unverzüglich zu unterbrechen, sofern sich während der Aufzeichnung tatsächliche Anhaltspunkte dafür ergeben, dass Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Aufzeichnungen über solche Äußerungen und Handlungen sind unverzüglich zu löschen. Nach einer Unterbrechung darf die Aufzeichnung nur fortgesetzt werden, wenn auf Grund geänderter Umstände davon ausgegangen werden kann, dass die Gründe, die zur Unterbrechung geführt haben, nicht mehr vorliegen.
- (6) Eine Verwertung der nach Absatz 2 sowie der nach Absatz 5 Satz 4 erlangten Erkenntnisse ist zum Zweck der Gefahrenabwehr nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist. Bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen. Bei Weitergabe der Daten ist zu vermerken, dass sie aus einer Maßnahme nach Absatz 2 herrühren. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrecht zu erhalten. Die Regelungen der Strafprozessordnung bleiben unberührt.

- b) In Absatz 7 wird die Angabe „6 und 7“ durch die Angaben „2 und 3“ ersetzt.
- (7) § 24 Absatz 6 und 7 bleibt unberührt.
- c) Absatz 8 Satz 3 wird aufgehoben.
- (8) Maßnahmen nach Absatz 1 bis 6 sind zu dokumentieren. Näheres regelt das für Inneres zuständige Ministerium durch Verwaltungsvorschrift. Die Landesregierung unterrichtet den Landtag jährlich zum 31. Dezember über die Maßnahmen nach Absatz 2 und 5.
- (9) Die Auswirkungen dieser Vorschrift und die praktische Anwendung werden bis zum 30. Juni 2019 durch die Landesregierung unter Mitwirkung einer oder eines unabhängigen sozialwissenschaftlichen Sachverständigen und einer oder eines polizeiwissenschaftlichen Sachverständigen geprüft. Die Landesregierung berichtet dem Landtag über das Ergebnis der Evaluierung. § 15c tritt am 31. Dezember 2019 außer Kraft.

7. § 16a wird wie folgt geändert:

§ 16a
Datenerhebung durch Observation

- (1) Die Polizei kann personenbezogene Daten erheben durch eine durchgehend länger als 24 Stunden oder an mehr als an zwei Tagen vorgesehene oder tatsächlich durchgeführte und planmäßig angelegte Beobachtung (längerfristige Observation)
1. über die in den §§ 4 und 5 genannten und unter den Voraussetzungen des § 6 über die dort genannten Personen, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,
 2. über Personen, soweit Tatsachen die Annahme rechtfertigen, dass diese Personen Straftaten von erheblicher Bedeutung begehen wollen, sowie über deren Kontakt- oder Begleitpersonen, wenn die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist.

Dabei dürfen auch personenbezogene Daten über andere Personen erhoben werden, soweit dies erforderlich ist, um eine

Datenerhebung nach Satz 1 durchführen zu können. Als Kontaktpersonen gelten nur die Personen, die enge persönliche, dienstliche oder geschäftliche Beziehungen zu den Personen gemäß Absatz 1 Satz 1 Nummer 2 unterhalten. Begleitpersonen sind Personen, die nicht nur kurzfristig mit diesen Personen angetroffen werden, ohne jedoch enge persönliche, dienstliche oder geschäftliche Beziehungen zu diesen zu unterhalten. Berufsgeheimnisträger gemäß § 53 der Strafprozessordnung gehören, soweit das geschützte Vertrauensverhältnis reicht, nicht zu den Kontakt- oder Begleitpersonen.

a) Absatz 2 Satz 2 und 3 werden aufgehoben.

(2) Eine längerfristige Observation darf nur durch die Behördenleiterin oder den Behördenleiter angeordnet werden. Nach Absatz 1 erlangte personenbezogene Daten sind besonders zu kennzeichnen. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

b) Absatz 3 wird aufgehoben.

(3) Über die Datenerhebung ist die betroffene Person zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Maßnahme erfolgen kann. Im Übrigen gilt § 17 Absatz 5 und 6 entsprechend.

c) Absatz 4 wird Absatz 3 und in Satz 1 wird die Angabe „bis 3“ durch die Angabe „und 2“ ersetzt.

(4) Auf eine Observation, die nicht die in Absatz 1 genannten Voraussetzungen erfüllt (kurzfristige Observation), finden die Absätze 1 bis 3 keine Anwendung. Durch eine kurzfristige Observation kann die Polizei personenbezogene Daten über die in den §§ 4 und 5 genannten und andere Personen nur erheben, soweit dies zum Zwecke der Gefahrenabwehr (§ 1 Abs. 1) erforderlich ist und ohne diese Maßnahme die Erfüllung der polizeilichen Aufgabe gefährdet wird.

8. § 17 wird wie folgt geändert:

§ 17

Datenerhebung durch den verdeckten Einsatz technischer Mittel

(1) Die Polizei kann personenbezogene Daten erheben durch den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen

sowie zum Abhören und Aufzeichnen des gesprochenen Wortes

1. über die Personen, die in den §§ 4 und 5 genannt werden, sowie unter den Voraussetzungen des § 6 über die dort genannten Personen, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,
2. über Personen, soweit Tatsachen die Annahme rechtfertigen, dass diese Personen Straftaten von erheblicher Bedeutung begehen wollen, sowie über deren Kontakt- oder Begleitpersonen, wenn die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist.

Dabei dürfen auch personenbezogene Daten über andere Personen erhoben werden, soweit dies erforderlich ist, um eine Datenerhebung nach Satz 1 durchführen zu können. § 16a Absatz 1 Satz 3 bis 5 gilt entsprechend.

(2) Der verdeckte Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen darf nur durch die Behördenleiterin oder den Behördenleiter angeordnet werden. Die Anordnung bedarf der Schriftform und ist auf höchstens einen Monat zu befristen; soweit die Voraussetzungen der Anordnung fortbestehen, sind Verlängerungen um jeweils einen weiteren Monat zulässig. Der Einsatz der Mittel zum Abhören und Aufzeichnen des gesprochenen Wortes bedarf der Anordnung durch das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat; hinsichtlich einer Verlängerung gilt § 18 Absatz 2 Satz 4 entsprechend. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Bei Gefahr im Verzug kann die Maßnahme durch die Behördenleiterin oder den Behördenleiter angeordnet werden. Die richterliche Bestätigung ist unverzüglich zu beantragen. Die Anordnung nach Satz 5 tritt spätestens mit Ablauf des dritten Tages nach ihrem Erlass außer Kraft, wenn sie bis dahin nicht richterlich

- bestätigt wird. Erfolgt keine richterliche Bestätigung, dürfen bereits erhobene Daten nicht verwendet werden. Die Daten sind unverzüglich zu löschen.
- a) Absatz 3 wird aufgehoben. (3) Hinsichtlich der Datenkennzeichnung gilt § 16a Absatz 2 Satz 2 und 3 entsprechend.
- b) Absatz 4 wird Absatz 3 und in Satz 4 werden die Angaben „7“ und „5“ jeweils durch die Angabe „3“ ersetzt. (4) Wenn das technische Mittel gemäß Absatz 1 ausschließlich zum Schutz der bei einem polizeilichen Einsatz tätigen Personen mitgeführt und verwendet wird, kann die Maßnahme durch die Behördenleiterin oder den Behördenleiter oder eine von ihnen beauftragte Leitungsperson des höheren Polizeivollzugsdienstes angeordnet werden. Eine anderweitige Verwertung der erlangten Erkenntnisse ist nur zum Zwecke der Strafverfolgung oder der Gefahrenabwehr und nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen. Aufzeichnungen, die nicht im Sinne des Satzes 2 verwendet werden, sind unverzüglich nach Beendigung des Einsatzes zu löschen. § 24 Absatz 7 sowie § 32 Absatz 5 Nummer 1 und 2 bleiben unberührt.
- c) Die Absätze 5 und 6 werden aufgehoben. (5) Über die Datenerhebung ist die betroffene Person zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Maßnahme erfolgen kann. Dies gilt nicht, wenn zur Durchführung der Unterrichtung in unverhältnismäßiger Weise weitere Daten der betroffenen Person erhoben werden müssten. Auf die Möglichkeit nachträglichen Rechtsschutzes ist hinzuweisen. Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen die betroffene Person eingeleitet worden, ist die Unterrichtung in Abstimmung mit der Staatsanwaltschaft nachzuholen, sobald dies der Stand des Ermittlungsverfahrens zulässt. Die Unterrichtung wird zurückgestellt, solange durch das Bekanntwerden der Datenerhebung Leib, Leben oder Freiheit einer Person gefährdet werden oder der Unterrichtung überwiegend schutzwürdige Belange einer anderen betroffenen Person entgegenstehen.

(6) Erfolgt eine Unterrichtung gemäß Absatz 5 Satz 1 nicht binnen sechs Monaten nach Abschluss der Maßnahme, bedarf die weitere Zurückstellung der Unterrichtung der richterlichen Zustimmung. Die richterliche Entscheidung ist jeweils nach einem Jahr erneut einzuholen. Über die Zustimmung entscheidet das Gericht, das für die Anordnung der Maßnahme zuständig gewesen ist. Bedurfte die Maßnahme nicht der richterlichen Anordnung, ist für die Zustimmung das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat, zuständig. Nach zweimaliger Verlängerung ist die Zustimmung des für die Einlegung einer Beschwerde zuständigen Gerichts einzuholen. § 68 Absatz 4 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit findet keine Anwendung. Fünf Jahre nach der erstmaligen Entscheidung gemäß Satz 5 darf dieses Gericht allein wegen Vorliegens der Zurückstellungsgründe des § 19 Absatz 3 und des § 20 Absatz 5 keine Zustimmung erteilen.

d) Absatz 7 wird Absatz 4.

(7) Bild- und Tonaufzeichnungen, die ausschließlich Personen betreffen, gegen die sich die Maßnahme nicht richtete, sind unverzüglich zu vernichten; es sei denn, sie werden zur Verfolgung von Straftaten jener Personen, gegen die sich die Maßnahme richtete, benötigt.

9. § 18 wird wie folgt geändert:

§ 18

Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen

(1) Die Polizei kann personenbezogene Daten in oder aus Wohnungen (§ 41 Absatz 1 Satz 2) durch den verdeckten Einsatz technischer Mittel gemäß § 17 Absatz 1 über Personen, die in den §§ 4 und 5 genannt werden, sowie unter den Voraussetzungen des § 6 über die dort genannten Personen erheben, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist und diese auf andere Weise nicht abgewendet werden kann. Dabei dürfen auch personenbezogene Daten über andere

Personen erhoben werden, soweit dies erforderlich ist, um eine Datenerhebung nach Satz 1 durchführen zu können. § 16a Absatz 1 Satz 3 bis 5 gilt entsprechend. Eine ausschließlich automatisierte Datenerhebung ist unzulässig.

(2) Die Datenerhebung nach Absatz 1 bedarf der Anordnung durch die in § 74a Absatz 4 des Gerichtsverfassungsgesetzes genannte Kammer des Landgerichts, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Sie bedarf der Schriftform und ist auf höchstens einen Monat zu befristen. Sie muss, soweit bekannt, Name und Anschrift der Person, gegen die sich die Datenerhebung richtet, Art und Umfang der zu erhebenden Daten sowie die betroffenen Wohnungen bezeichnen und ist zu begründen. Soweit die Voraussetzungen der Anordnung fortbestehen, sind auf Antrag Verlängerungen um jeweils einen weiteren Monat zulässig. Bei Gefahr im Verzug kann die Maßnahme durch die Behördenleiterin oder den Behördenleiter angeordnet werden. Die richterliche Bestätigung ist unverzüglich zu beantragen. Die Anordnung nach Satz 6 tritt spätestens mit Ablauf des dritten Tages nach ihrem Erlass außer Kraft, wenn sie bis dahin nicht richterlich bestätigt wird. Erfolgt keine richterliche Bestätigung, dürfen bereits erhobene Daten nicht verwendet werden. Die Daten sind unverzüglich zu löschen.

(3) Die Maßnahme darf nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Erhebung Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Dabei ist insbesondere auf die Art der zu überwachenden Räumlichkeiten und das Verhältnis der dort anwesenden Personen zueinander abzustellen. Der Kernbereich umfasst auch das durch Berufsgeheimnis geschützte Vertrauensverhältnis der in §§ 53 und 53a der Strafprozessordnung genannten Berufsheimnisträger. Gespräche in Betriebs- und Geschäftsräumen sind, soweit sie nicht zur Berufsausübung bestimmte Räume von Berufsheimnisträgern gemäß §§ 53 und 53a der Strafprozessordnung sind, in der

Regel nicht dem Kernbereich privater Lebensgestaltung zuzurechnen.

(4) Die Datenerhebung ist unverzüglich zu unterbrechen, sofern sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Bestehen insoweit Zweifel, darf statt der unmittelbaren Wahrnehmung nur noch eine automatisierte Aufzeichnung erfolgen. Nach einer Unterbrechung oder einer Aufzeichnung gemäß Satz 2 darf die Erhebung fortgesetzt werden, wenn zu erwarten ist, dass die Gründe, die zur Unterbrechung oder zur Aufzeichnung geführt haben, nicht mehr vorliegen. Die automatisierte Aufzeichnung ist unverzüglich dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Für die nicht verwertbaren Teile ordnet das Gericht die unverzügliche Löschung an. Das Gericht unterrichtet die Polizeibehörde unverzüglich über den Inhalt der verwertbaren Teile der Aufzeichnung. Die Tatsachen der Datenerfassung und der Löschung sind zu dokumentieren. Die Maßnahme ist abzubrechen, wenn die Voraussetzungen des Absatzes 1 nicht mehr vorliegen.

- a) In Absatz 5 Satz 4 werden die Angaben „7“ und „5“ jeweils durch die Angabe „3“ ersetzt.

(5) Werden technische Mittel ausschließlich zum Schutz der bei einem polizeilichen Einsatz in Wohnungen tätigen Personen verwendet, kann die Datenerhebung nach Absatz 1 durch die Behördenleiterin oder den Behördenleiter angeordnet werden. Eine anderweitige Verwertung der gemäß Satz 1 erlangten Erkenntnisse ist nur zum Zwecke der Strafverfolgung oder der Gefahrenabwehr und nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen. Aufzeichnungen, die nicht im Sinne des Satzes 2 verwendet werden, sind unverzüglich nach Beendigung des Einsatzes zu löschen. § 24 Absatz 7 sowie § 32 Absatz 5 Nummer 1 und 2 bleiben unberührt.

b) Absatz 6 wird aufgehoben.

(6) Nach Absätzen 1 und 5 erlangte personenbezogene Daten sind besonders zu kennzeichnen. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

c) Absatz 7 wird Absatz 6 und die Wörter „Absätze 5 bis 7“ werden durch die Angabe „Absatz 4“ ersetzt.

(7) § 17 Absätze 5 bis 7 gilt entsprechend.

10. § 19 wird wie folgt geändert:

§ 19
Datenerhebung
durch den Einsatz von Personen,
deren Zusammenarbeit mit der Polizei
Dritten nicht bekannt ist

(1) Die Polizei kann personenbezogene Daten erheben durch den Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist,

1. über die in den §§ 4 und 5 genannten und unter den Voraussetzungen des § 6 über die dort genannten Personen, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,
2. über Personen, soweit Tatsachen die Annahme rechtfertigen, dass diese Personen Straftaten von erheblicher Bedeutung begehen wollen, sowie über deren Kontakt- oder Begleitpersonen, wenn die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist.

Dabei dürfen auch personenbezogene Daten über andere Personen erhoben werden, soweit dies erforderlich ist, um eine Datenerhebung nach Satz 1 durchführen zu können. § 16a Absatz 1 Satz 3 bis 5 sowie § 17 Absatz 7 gelten entsprechend.

a) In Absatz 1 Satz 3 wird die Angabe „7“ durch die Angabe „4“ ersetzt.

(2) Der Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist, darf nur durch die Behördenleiterin oder den Behördenleiter oder eine von ihnen beauftragte Leitungsperson des höheren Polizeivollzugsdienstes angeordnet werden. § 16a Absatz 2 Satz 2 und 3 gilt entsprechend.

b) Absatz 3 wird aufgehoben.

(3) Bezüglich der Unterrichtung über die Maßnahme gilt § 17 Absatz 5 und 6 entsprechend mit der Maßgabe, dass sie auch zurückgestellt werden kann, wenn durch das Bekanntwerden der Datenerhebung der weitere Einsatz dieser Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist, gefährdet wird.

11. § 20 wird wie folgt geändert:

§ 20
Datenerhebung durch den Einsatz
Verdeckter Ermittler

(1) Die Polizei kann durch einen Polizeivollzugsbeamten, der unter einer ihm verliehenen, auf Dauer angelegten Legende eingesetzt wird (Verdeckter Ermittler), personenbezogene Daten über die in den §§ 4 und 5 genannten und andere Personen erheben, wenn

1. dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,
2. Tatsachen die Annahme rechtfertigen, dass Straftaten von erheblicher Bedeutung begangen werden sollen, und dies zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist.

(2) Soweit es für den Aufbau und zur Aufrechterhaltung der Legende unerlässlich ist, dürfen entsprechende Urkunden hergestellt oder verändert werden. Ein Verdeckter Ermittler darf unter der Legende zur Erfüllung seines Auftrages am Rechtsverkehr teilnehmen.

(3) Ein Verdeckter Ermittler darf unter der Legende mit Einverständnis der berechtigten Personen deren Wohnung betreten. Das Einverständnis darf nicht durch ein über die Nutzung der Legende hinausgehendes Vortäuschen eines Zutrittsrechts herbeigeführt werden. Im Übrigen richten sich die Befugnisse eines Verdeckten Ermittlers nach diesem Gesetz oder anderen Rechtsvorschriften.

- a) Absatz 4 Satz 2 wird wie folgt gefasst:
 „§ 17 Absatz 4 gilt entsprechend.“
- (4) Der Einsatz eines Verdeckten Ermittlers darf nur durch die Behördenleiterin oder den Behördenleiter angeordnet werden. § 16a Absatz 2 Satz 2 und 3 sowie § 17 Absatz 7 gelten entsprechend.
- b) Absatz 5 wird aufgehoben.
- (5) Bezüglich der Unterrichtung über die Maßnahme gilt § 17 Absatz 5 und 6 entsprechend mit der Maßgabe, dass sie auch zurückgestellt werden kann, wenn durch das Bekanntwerden der Datenerhebung der weitere Einsatz des Verdeckten Ermittlers gefährdet wird.

12. § 20a wird wie folgt geändert:

§ 20a

Abfrage von Telekommunikations- und Telemediendaten

- (1) Die Polizei kann soweit erforderlich von jedem, der geschäftsmäßig Telekommunikationsdienste oder Telemediendienste erbringt oder daran mitwirkt (Diensteanbieter), Auskunft verlangen über
1. Bestandsdaten im Sinne der §§ 95, 111 Telekommunikationsgesetz und § 14 Telemediengesetz; die Auskunft darf auch anhand einer zu bestimmten Zeitpunkten zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 Telekommunikationsgesetz),
 2. folgende Verkehrsdaten im Sinne des § 96 Telekommunikationsgesetz:
 - a) die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtungen, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartenummer, bei mobilen Telekommunikationsendgeräten auch die Standortdaten,
 - b) den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit,
 3. folgende Nutzungsdaten im Sinne des § 15 Telemediengesetz:

- a) Merkmale zur Identifikation der Nutzerin oder des Nutzers,
- b) Angaben über den Beginn und das Ende sowie den Umfang der jeweiligen Nutzung nach Datum und Uhrzeit.

Die Maßnahmen nach Satz 1 sind nur zulässig

1. wenn die hohe Wahrscheinlichkeit eines Schadens für Leben, Gesundheit oder Freiheit einer Person besteht oder
2. zur Abwehr einer gemeinen Gefahr

und nur, soweit die Erreichung des Zwecks der Maßnahme auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Die Daten sind der Polizei unverzüglich zu übermitteln. Dritten dürfen die Daten nur mit Zustimmung der betroffenen Person zugänglich gemacht werden.

(2) Bei Maßnahmen nach Absatz 1 dürfen personenbezogene Daten Dritter nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. Sämtliche nach Absatz 1 erhobene personenbezogene Daten Dritter sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(3) Maßnahmen nach Absatz 1 bedürfen der Anordnung durch die Behördenleiterin oder den Behördenleiter. Der Antrag bedarf der Schriftform. In der schriftlichen Anordnung sind

1. die tragenden Erkenntnisse für das Vorliegen der Gefahr nach Absatz 1 und die Begründung der Verhältnismäßigkeit der Maßnahme,
2. die Art der Maßnahme anzugeben sowie, soweit vorhanden,
3. der Name und die Anschrift der Betroffenen, gegen die sich die Maßnahme richtet und
4. eine Kennung des Telekommunikationsanschlusses oder Endgerätes.

Abweichend von Satz 1 bis 3 können Antrag und Anordnung bei Gefahr im Verzug fernmündlich erfolgen; die Schriftform ist binnen drei Tagen nachzuholen.

a) Absatz 4 wird aufgehoben.

(4) Sind die nach dieser Vorschrift durchgeführten Maßnahmen abgeschlossen, sind die Betroffenen zu unterrichten, sobald dies ohne Gefährdung des Zweckes der Maßnahme geschehen kann. § 17 Absatz 5 und 6 gilt entsprechend. Im Anschluss an die Unterrichtung der Betroffenen sind die personenbezogenen Daten unverzüglich zu löschen, es sei denn, sie werden zur Verfolgung von Straftaten durch oder zum Nachteil jener Personen benötigt, gegen die sich die Maßnahme richtete.

b) Absatz 5 wird Absatz 4.

(5) Die in Anspruch genommenen Diensteanbieter werden entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes vom 5. Mai 2004 (BGBl. I S. 718, 776), zuletzt geändert durch Artikel 13 des Gesetzes vom 5. Dezember 2012 (BGBl. I S. 2418), entschädigt.

c) Absatz 6 wird aufgehoben.

(6) Die Landesregierung unterrichtet den Landtag jährlich über die nach Absatz 1 erfolgten Maßnahmen.

d) Absatz 7 wird Absatz 6.

(7) Die Auswirkungen dieser Vorschrift und die praktische Anwendung werden nach einem Erfahrungszeitraum von drei Jahren durch die Landesregierung unter Mitwirkung einer oder eines unabhängigen wissenschaftlichen Sachverständigen geprüft. Die Landesregierung berichtet dem Landtag über das Ergebnis der Evaluierung.

§ 20b

Einsatz technischer Mittel bei Mobilfunkendgeräten

Die Polizei darf unter den Voraussetzungen des § 20a auch technische Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes und zur Ermittlung der Geräte- und Kartennummern einsetzen. Die Maßnahme ist nur zulässig, wenn ohne die Ermittlung die Erreichung des Zwecks nach Satz 1 aussichtslos oder wesentlich erschwert wäre. Personenbezo-

13. In § 20b Satz 5 werden die Wörter „4, 6 und 7 gelten“ durch die Angabe „5 gilt“ ersetzt.

gene Daten einer dritten Person dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Satz 1 unvermeidbar ist. Sie unterliegen einem absoluten Verwendungsverbot und sind nach Beendigung der Maßnahme unverzüglich zu löschen. § 20a Absatz 4, 6 und 7 gelten entsprechend.

14. § 20c wird wie folgt geändert:

*Gesetz zur Stärkung der Sicherheit in Nordrhein-Westfalen -
Sechstes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen*

*„§ 20c
Datenerhebung durch die Überwachung der Telekommunikation*

(...)

- a) Absatz 8 wird wie folgt geändert:

(8) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach den Absätzen 1 und 2 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit im Rahmen von Maßnahmen nach den Absätzen 1 und 2 neben einer automatischen Aufzeichnung eine unmittelbare Kenntniserhebung erfolgt, ist die Maßnahme unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den Absätzen 1 und 2 erlangt worden sind, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Unterrichtung nach Absatz 9 oder sechs Monate nach Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung zu löschen. Ist die Datenschutz-

- aa) In Satz 6 wird nach dem Wort „Datenschutzkontrolle“ die Angabe „gemäß § 33c“ eingefügt.
- bb) In Satz 7 werden die Wörter „Unterrichtung nach Absatz 9“ durch die Wörter „Benachrichtigung nach § 33 Absatz 2

Satz 1“ und die Wörter „über das endgültige Absehen von der Benachrichtigung“ durch die Wörter „nach § 33 Absatz 4 Satz 7“ ersetzt.

kontrolle noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren. Im Übrigen gilt § 18 Absatz 4 Satz 2 bis 7 entsprechend.

b) Absatz 9 wird aufgehoben.

(9) § 17 Absatz 5 und 6 gilt entsprechend.

c) Absatz 10 wird Absatz 9 und wie folgt gefasst:

„(9) Bei der Erhebung von Daten nach den Absätzen 1 und 2 sind zusätzlich zu den in § 33b Absatz 1 und 2 genannten Angaben die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen, nicht nur flüchtigen Veränderungen zu protokollieren, sofern die Überwachung mit einem Eingriff in von der betroffenen Person genutzte informationstechnische Systeme verbunden ist.“.

(10) Bei der Erhebung von Daten nach den Absätzen 1 und 2 sind zu protokollieren

- 1. das zur Datenerhebung eingesetzte Mittel,*
- 2. der Zeitpunkt des Einsatzes,*
- 3. Angaben, welche die Feststellung der erhobenen Daten ermöglichen,*
- 4. die Organisationseinheiten, welche die Maßnahmen durchführen,*
- 5. die Beteiligten der überwachten Kommunikation und*
- 6. sofern die Überwachung mit einem Eingriff in von der betroffenen Person genutzte informationstechnische Systeme verbunden ist, die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen, nicht nur flüchtigen Veränderungen.*

Die Protokolldaten dürfen nur verwendet werden für Zwecke der Unterrichtung nach Absatz 9 oder um der betroffenen Person oder einer dazu befugten Stelle die Prüfung zu ermöglichen, ob die Maßnahmen rechtmäßig durchgeführt worden sind.

d) Absatz 11 wird aufgehoben.

(11) Die Landesregierung unterrichtet den Landtag jährlich über die nach den Absätzen 1 und 2 erfolgten Maßnahmen.

Der bisherige Buchstabe d wird Buchstabe e.

(...)

§ 21 **Polizeiliche Beobachtung**

(1) Die Polizei kann personenbezogene Daten, insbesondere die Personalien einer Person sowie Kennzeichen des von ihr benutzten oder eingesetzten Kraftfahrzeuges, zur Polizeilichen Beobachtung in einer Datei speichern (Ausschreibung zur Polizeilichen Beobachtung), wenn

1. die Gesamtwürdigung der Person und der von ihr bisher begangenen Straftaten erwarten lässt, dass sie auch künftig Straftaten von erheblicher Bedeutung begehen wird,
2. Tatsachen die Annahme rechtfertigen, dass die Person Straftaten von erheblicher Bedeutung begehen wird,

und dies zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist.

(2) Im Falle eines Antreffens der Person oder des von ihr benutzten oder eingesetzten Kraftfahrzeuges können Erkenntnisse über das Antreffen sowie über Kontakt- und Begleitpersonen und mitgeführte Sachen an die ausschreibende Polizeibehörde übermittelt werden.

(3) Die Ausschreibung zur Polizeilichen Beobachtung darf nur durch den Richter angeordnet werden. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Die Anordnung ist auf höchstens ein Jahr zu befristen. Eine Verlängerung um nicht mehr als jeweils ein Jahr ist zulässig, soweit die Voraussetzungen des Absatzes 1 weiterhin vorliegen. Spätestens nach Ablauf von jeweils sechs Monaten ist von der ausschreibenden Polizeibehörde zu prüfen, ob die Voraussetzungen für die Anordnung noch bestehen. Das Ergebnis dieser Prüfung ist aktenkundig zu machen.

15. § 21 Absatz 4 wird aufgehoben.

(4) Für gemäß Absatz 1 und 2 erhobene personenbezogene Daten gilt § 16a Absatz 2 Satz 2 und 3 entsprechend. Die betroffene Person ist nach Beendigung der Ausschreibung zur Polizeilichen Beobachtung durch die Polizei über die Ausschreibung und die Löschung zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Maßnahme erfolgen kann. Im Übrigen gilt § 17 Absatz 5 und 6 entsprechend.

16. Die Überschrift zu „Zweiter Titel“ wird wie folgt gefasst:

**„Zweiter Teil
Weiterverarbeitung von personenbezo-
genen Daten“.**

**Zweiter Titel
Datenspeicherung, Datenveränderung
und Datennutzung**

17. § 22 wird wie folgt gefasst:

**„§ 22
Datenspeicherung, Prüfungstermine**

**§ 22
Allgemeine Regeln
über die Dauer der Datenspeicherung**

(1) Die Polizei kann rechtmäßig erlangte personenbezogene Daten in Akten und Dateisystemen speichern, soweit dies zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist.

Die Dauer der Speicherung ist auf das erforderliche Maß zu beschränken. Für automatisierte Dateien sind Termine festzulegen, zu denen spätestens überprüft werden muss, ob die suchfähige Speicherung von Daten weiterhin erforderlich ist (Prüfungstermine). Für nichtautomatisierte Dateien und Akten sind Prüfungstermine oder Aufbewahrungsfristen festzulegen. Dabei sind der Speicherungszweck sowie Art und Bedeutung des Anlasses der Speicherung zu berücksichtigen. Prüfungstermine oder Aufbewahrungsfristen für die in Dateien oder Akten suchfähig gespeicherten personenbezogenen Daten von Kindern dürfen zwei Jahre nicht überschreiten; die Frist beginnt mit dem Tag der ersten Speicherung.

(2) Die Dauer der Speicherung ist auf das erforderliche Maß zu beschränken. Für automatisierte Dateisysteme sind Termine festzulegen, zu denen spätestens überprüft werden muss, ob die suchfähige Speicherung von Daten weiterhin erforderlich ist (Prüfungstermine). Für nichtautomatisierte Dateisysteme und Akten sind Prüfungstermine oder Aufbewahrungsfristen festzulegen. Dabei sind der Speicherungszweck sowie Art und Bedeutung des Anlasses der Speicherung zu berücksichtigen. Die festzulegenden Prüfungstermine dürfen bei Erwachsenen zehn Jahre und bei Jugendlichen fünf Jahre nicht überschreiten. Die Frist beginnt regelmäßig mit dem Ende des Jahres, in dem das letzte Ereignis erfasst worden ist, das zur Speicherung der Daten geführt hat, jedoch nicht vor Entlassung des Betroffenen aus einer Justizvollzugsanstalt

oder der Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. Werden innerhalb der in Satz 2 und 3 genannten Frist weitere personenbezogene Daten über dieselbe Person gespeichert, so gilt für alle Speicherungen gemeinsam der Prüftermin, der als letzter eintritt, oder die Aufbewahrungsfrist, die als letzte endet. Die Beachtung der Prüfungstermine und Aufbewahrungsfristen ist durch geeignete technische und organisatorische Maßnahmen zu gewährleisten.

(3) Wird die betroffene Person rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen sie unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt, so ist die Speicherung unzulässig, wenn sich aus Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat. Sollte eine Speicherung wegen eines Restverdachts einer Straftat weiterhin zulässig sein, ist dessen Gewicht und der Grad des Verdachts zu dokumentieren.

(4) Prüfungstermine oder Aufbewahrungsfristen für die in Dateisystemen oder Akten suchfähig gespeicherten personenbezogenen Daten von Kindern dürfen zwei Jahre nicht überschreiten. Die Frist beginnt mit dem Tag der ersten Speicherung.

(5) Über Kontakt- oder Begleitpersonen einer Person, bei der Tatsachen die Annahme rechtfertigen, dass sie künftig Straftaten begehen wird, sowie über Auskunftspersonen kann die Polizei personenbezogene Daten suchfähig in Dateien speichern, verändern und nutzen, soweit dies zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist. Die festzulegenden Prüftermine bei der Speicherung von Kontakt- und Begleitpersonen dürfen die Dauer eines Jahres nicht überschreiten. Die Verlängerung für jeweils ein weiteres Jahr ist zulässig, soweit die Voraussetzungen des Satzes

1 weiterhin vorliegen, jedoch darf die Speicherdauer insgesamt drei Jahre nicht überschreiten. Die Entscheidung über die jeweilige Verlängerung trifft die Behördenleiterin oder der Behördenleiter oder ein von ihr oder ihm beauftragter Beamter.

(6) Werden wertende Angaben über eine Person in Dateien gespeichert, muss feststellbar sein, bei welcher Stelle die den Angaben zugrunde liegenden Informationen vorhanden sind. Wertende Angaben dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen wurden.“

18. Nach § 22 werden die folgenden § 22a und 22b eingefügt:

„§ 22a

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung von Daten im Sinne des § 36 Nummer 18 des Datenschutzgesetzes Nordrhein-Westfalen ist nur zulässig, wenn dies zur polizeilichen Aufgabenerfüllung gemäß dieses Gesetzes oder einer anderen Rechtsvorschrift unbedingt erforderlich ist.

(2) Die an Verarbeitungsvorgängen im Sinne des Absatz 1 Beteiligten sind für die besondere Schutzwürdigkeit dieser Daten zu sensibilisieren. Der Zugang zu den personenbezogenen Daten ist zu beschränken. Das gilt auch für Auftragsverarbeiter im Sinne des § 36 Nummer 10 des Datenschutzgesetzes Nordrhein-Westfalen. Durch geeignete technische und organisatorische Maßnahmen ist sicherzustellen, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten im Sinne des Absatz 1 eingegeben, verändert oder entfernt worden sind.

§ 22b
Kennzeichnung in polizeilichen Dateisystemen

(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 im Sinne des § 42 des Datenschutzgesetzes Nordrhein-Westfalen, zu denen die zur Identifizierung dienenden Daten angelegt wurden,
3. Angabe der
 - a) Rechtsgüter, deren Schutz die Erhebung dient oder
 - b) Straftaten, deren Verhütung oder vorbeugende Bekämpfung die Erhebung dient oder
4. Angabe der Stelle, die sie erhoben hat.

Die Kennzeichnung nach Satz 1 soll auch durch die Angabe der Rechtsgrundlage der Datenerhebung ergänzt werden.

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

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

(4) Eine Weiterverarbeitung oder Übermittlung ist auch zulässig, soweit in besonderen Einzelfällen eine Kennzeichnung tatsächlich nicht möglich ist oder

einen unverhältnismäßigen Aufwand erfordern würde.

(5) Abweichend von Absatz 2 und 3 ist eine Weiterverarbeitung oder Übermittlung personenbezogener Daten auch ohne eine Kennzeichnung zulässig nach den Bestimmungen des für die Daten am 23. Mai 2018 jeweils geltenden Verzeichnisses gemäß § 8 des Datenschutzgesetzes Nordrhein-Westfalen in der Fassung der Bekanntmachung vom 9. Juni 2000 (GV. NRW. S. 542), das zuletzt durch Artikel 2 des Gesetzes vom 6. Dezember 2016 (GV. NRW. S. 1052) geändert worden ist, in der bis zum 24. Mai 2018 geltenden Fassung.“.

19. § 23 wird wie folgt gefasst:

**„§ 23
Weiterverarbeitung von personenbe-
zogenen Daten, Zweckbindung,
Zweckänderung**

(1) Die Polizeibehörde kann personenbezogene Daten, die sie selbst erhoben hat, weiterverarbeiten

1. zur Erfüllung derselben Aufgabe und
2. zum Schutz derselben Rechtsgüter oder sonstigen Rechte oder zur Verhütung oder vorbeugenden Bekämpfung derselben Straftaten.

Satz 1 gilt entsprechend für personenbezogene Daten, denen keine Erhebung vorausgegangen ist, mit der Maßgabe, dass für die Weiterverarbeitung der Zweck der Verarbeitung zu berücksichtigen ist. Für die Weiterverarbeitung von personenbezogenen Daten, die aus Maßnahmen nach § 18 erlangt wurden, muss im Einzelfall eine Gefahr im Sinne des § 18 Absatz 1 vorliegen.

**§ 23
Zweckbindung bei der Datenspeiche-
rung, Datenveränderung und Datennut-
zung**

(1) Die Speicherung, Veränderung und Nutzung darf nur zu dem Zweck erfolgen, zu dem die Daten erlangt worden sind. Die Nutzung sowie die weitere Speicherung und Veränderung zu einem anderen Zweck sind jedoch zulässig, soweit die Polizei die Daten auch zu diesem Zweck erheben darf. Satz 2 gilt nicht für die nach § 11 erhobenen Daten.

(2) Werden wertende Angaben über eine Person in Dateien gespeichert, muss feststellbar sein, bei welcher Stelle die den Angaben zugrundeliegenden Informationen vorhanden sind. Wertende Angaben dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen wurden.

(2) Die Polizeibehörde kann zur Erfüllung ihrer Aufgaben personenbezogene Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn

1. mindestens
 - a) vergleichbar schwerwiegende Straftaten verhütet oder vorbeugend bekämpft oder
 - b) vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte geschützt werden sollen und
2. sich im Einzelfall Anhaltspunkte
 - a) zur Verhütung oder vorbeugenden Bekämpfung solcher Straftaten ergeben oder
 - b) zur Abwehr einer innerhalb eines absehbaren Zeitraums drohenden Gefahr für mindestens vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte erkennen lassen.

Satz 1 gilt entsprechend für personenbezogene Daten, denen keine Erhebung vorausgegangen ist, mit der Maßgabe, dass für die Weiterverarbeitung der Zweck der Verarbeitung zu berücksichtigen ist. Die §§ 24 und 24a bleiben unberührt. Personenbezogene Daten, die rechtmäßig zu den in § 11 genannten Zwecken erhoben wurden, dürfen nicht zu anderen Zwecken genutzt werden. Für die Weiterverarbeitung von Daten, die aus Maßnahmen nach § 18 erlangt wurden, gilt Absatz 2 Satz 1 Nummer 2 mit der Maßgabe entsprechend, dass im Einzelfall eine Gefahr im Sinne des § 18 Absatz 1 vorliegen muss.

(3) Abweichend von Absatz 2 können die vorhandenen, zur Identifizierung dienenden Daten einer Person, insbesondere Name, Geschlecht, Geburtsdatum, Geburtsort, derzeitige und frühere Staatsangehörigkeit, Anschrift (Grunddaten), auch weiterverarbeitet werden, um diese Person zu identifizieren. Die §§ 24 und 24a und bleiben unberührt.

(4) Abweichend von Absatz 2 können rechtmäßig erhobene personenbezogene Daten allein zum Zwecke der Vorgangsverwaltung oder zu einer zeitlich befristeten Dokumentation weiterverarbeitet werden.

(5) Bei der Weiterverarbeitung von personenbezogenen Daten stellt die Polizei durch technische und organisatorische Vorkehrungen sicher, dass die Absätze 1 bis 4 beachtet werden.

(6) Die Absätze 2 bis 5 gelten auch für die Weiterverarbeitung der im Rahmen der Verfolgung von Straftaten gewonnenen personenbezogenen Daten zum Zwecke der Gefahrenabwehr im Sinne des § 1 Absatz 1. Eine suchfähige Speicherung dieser Daten in Dateisystemen und Akten ist nur über Personen zulässig, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist.“.

20. § 24 wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

**„§ 24
Weiterverarbeitung zu besonderen
Zwecken“**

b) Die Absätze 1 bis 4 werden aufgehoben.

**§ 24
Speicherung, Veränderung
und Nutzung von Daten**

(1) Die Polizei kann rechtmäßig erlangte personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist.

(2) Dabei kann die Polizei auch die im Rahmen der Verfolgung von Straftaten gewonnenen personenbezogenen Daten zum Zwecke der Gefahrenabwehr (§ 1 Abs. 1) speichern, verändern und nutzen. Eine suchfähige Speicherung dieser Daten in Dateien und Akten ist nur über Personen zulässig, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist. Die nach § 22 festzulegenden Prüfungster-

mine dürfen für Daten nach Satz 1 bei Erwachsenen zehn Jahre und bei Jugendlichen fünf Jahre nicht überschreiten. Die Frist beginnt mit dem Tag, an dem das letzte Ereignis eingetreten ist, das zur Speicherung der Daten geführt hat, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. Ist der Verdacht der Straftat gegen die Person entfallen, sind ihre in diesem Zusammenhang in Dateien suchfähig gespeicherten personenbezogenen Daten zu löschen sowie die zu ihrer Person suchfähig angelegten Akten zu vernichten.

(3) Werden personenbezogene Daten von Kindern, die ohne Kenntnis der Sorgeberechtigten erhoben worden sind, gespeichert, sind die Sorgeberechtigten durch die Polizei zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Maßnahme erfolgen kann. Von der Unterrichtung kann abgesehen werden, solange zu besorgen ist, dass die Unterrichtung zu erheblichen Nachteilen für das Kind führt.

(4) Über Kontakt- oder Begleitpersonen einer Person, bei der Tatsachen die Annahme rechtfertigen, dass sie künftig Straftaten begehen wird, sowie über Auskunftspersonen kann die Polizei personenbezogene Daten suchfähig in Dateien speichern, verändern und nutzen, soweit dies zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist. Die Daten dürfen nur für die Dauer eines Jahres gespeichert werden. Die Speicherung für jeweils ein weiteres Jahr ist zulässig, soweit die Voraussetzungen des Satzes 1 weiterhin vorliegen, jedoch darf die Speicherdauer insgesamt drei Jahre nicht überschreiten. Die Entscheidung über die jeweilige Verlängerung trifft die Behördenleiterin oder der Behördenleiter oder ein von ihnen beauftragter Beamter.

- c) Die Absätze 5 bis 7 werden die Absätze 1 bis 3.
- d) Im neuen Absatz 1 wird folgender Satz angefügt:

„Die Verarbeitung von besonderen Kategorien personenbezogener Daten richtet sich nach § 22a.“

- e) Im neuen Absatz 2 wird nach dem Wort „zu“ das Wort „polizeilichen“ eingefügt.

(5) Die Polizei kann Anrufe über Notrufeinrichtungen auf Tonträger aufzeichnen. Eine Aufzeichnung von Anrufen im Übrigen ist nur zulässig, soweit die Aufzeichnung zur polizeilichen Aufgabenerfüllung erforderlich ist. Die Aufzeichnungen sind spätestens nach einem Monat zu löschen, es sei denn, sie werden zur Verfolgung von Straftaten benötigt oder Tatsachen rechtfertigen die Annahme, dass die anrufende Person Straftaten begehen wird, und die Aufbewahrung ist zur vorbeugenden Bekämpfung von Straftaten erforderlich.

(6) Die Polizei kann gespeicherte personenbezogene Daten zu statistischen Zwecken nutzen; die Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren.

(7) Die Polizei kann personenbezogene Daten zur polizeilichen Aus- und Fortbildung nutzen. Die personenbezogenen Daten sind zu anonymisieren. Einer Anonymisierung bedarf es nicht, wenn diese dem Aus- und Fortbildungszweck entgegensteht und die berechtigten Interessen der betroffenen Person an der Geheimhaltung der Daten nicht offensichtlich überwiegen.

21. Nach § 24 wird folgender § 24a eingefügt:

**„§ 24a
Weiterverarbeitung zu wissenschaftlichen Zwecken**

(1) Abweichend von den §§ 17 und 40 des Datenschutzgesetzes Nordrhein-Westfalen ist eine Weiterverarbeitung oder Übermittlung von personenbezogenen Daten, die aus Maßnahmen nach § 18 erlangt wurden, ausgeschlossen. Dies gilt nicht, soweit die Weiterverarbeitung für die polizeiliche Eigenforschung und Evaluierung unerlässlich ist.

(2) Personenbezogene Daten dürfen nur an Amtsträger, für den öffentlichen Dienst besonders Verpflichtete oder

Personen, die zur Geheimhaltung verpflichtet worden sind, übermittelt werden.

(3) Durch geeignete technische und organisatorische Maßnahmen hat die wissenschaftliche Forschung betreibende Stelle zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.“.

22. § 26 wird wie folgt geändert:

a) In der Überschrift werden nach dem Wort „Datenübermittlung“ die Wörter „, Übermittlungsverbote und Verweigerungsgründe“ angefügt.

b) Absatz 1 wird wie folgt gefasst:

„(1) Die Polizei kann personenbezogene Daten unter Beachtung des § 23 auf der Grundlage der nachstehenden Regelungen übermitteln. Personenbezogene Daten von Kontakt- und Begleitpersonen dürfen nur an Polizeibehörden übermittelt werden.“

(1) Personenbezogene Daten dürfen nur zu dem Zweck übermittelt werden, zu dem sie erlangt oder gespeichert worden sind. Abweichend hiervon kann die Polizei personenbezogene Daten übermitteln, soweit dies

1. durch Gesetz zugelassen ist,
2. zur Abwehr einer Gefahr erforderlich ist und der Empfänger die Daten auf andere Weise nicht oder nicht rechtzeitig oder nur mit unverhältnismäßig hohem Aufwand erlangen kann.

Die nach § 24 Abs. 4 gespeicherten Daten dürfen nur an Polizeibehörden übermittelt werden.

(2) Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der Polizei von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist die Datenübermittlung durch die Polizei nur zulässig, wenn der Empfänger die Daten zur Erfüllung des gleichen Zwecks benötigt, zu dem sie die Polizei erlangt hat.

(3) Die Verantwortung für die Übermittlung trägt die übermittelnde Polizeibehörde. Sie prüft die Zulässigkeit der Datenübermittlung. Erfolgt die Datenübermittlung auf Grund eines Ersuchens des Empfängers,

§ 26 Allgemeine Regeln der Datenübermittlung

hat dieser der übermittelnden Polizeibehörde die zur Prüfung erforderlichen Angaben zu machen. Bei Ersuchen von Polizeibehörden sowie anderen öffentlichen Stellen prüft die übermittelnde Polizeibehörde nur, ob das Ersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, im Einzelfall besteht Anlass zur Prüfung der Rechtmäßigkeit des Ersuchens. Erfolgt die Datenübermittlung durch automatisierten Abruf, trägt die Verantwortung für die Rechtmäßigkeit des Abrufs der Empfänger.

- c) Absatz 5 wird Absatz 1 und folgender Satz wird angefügt: „
- d) Absatz 6 wird Absatz 2 und nach den Wörtern „Zeitpunkt zu“ wird das Wort „polizeilichen“ eingefügt.
- e) Nach Absatz 2 werden die folgenden Absätze 3bis 6 eingefügt:

„(3) 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 berechnete Interessen der betroffenen Person oder eines Dritten an der Geheimhaltung offensichtlich überwiegen. Eine Verwendung dieser Daten ist unzulässig. Dies ist dem Empfänger der übermittelten Daten mitzuteilen.

(4) § 54 Absatz 3 Satz 2 des Datenschutzgesetzes Nordrhein-Westfalen bleibt unberührt.

(5) Die Übermittlung unterbleibt, wenn unter Berücksichtigung der Art der Daten und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person das Allgemeininteresse an der Übermittlung überwiegen oder besondere gesetzliche Verwendungsregelungen entgegenstehen. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder besonderer Berufs- oder

Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(6) Eine Datenübermittlung nach den §§ 27 bis 29 unterbleibt darüber hinaus,

1. wenn hierdurch Sicherheitsinteressen des Bundes oder der Länder wesentlich beeinträchtigt würden,
2. wenn hierdurch der Erfolg laufender Ermittlungen oder Leib, Leben oder Freiheit einer Person gefährdet würde,
3. soweit Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde oder
4. 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.“

f) Der bisherige Absatz 4 wird Absatz 7 und wie folgt geändert:

- aa) Satz 2 wird wie folgt gefasst:
„Eine Verarbeitung zu anderen Zwecken ist unter Beachtung des § 23 zulässig.“
- bb) Folgende Sätze werden angefügt:
„Bei personenbezogenen Daten, die aus Maßnahmen nach § 18 stammen, ist dies nur mit ausdrücklicher Zustimmung der übermittelnden Stelle zulässig. Ausländische öffentliche Stellen im Bereich der Europäischen Union und deren Mitgliedstaaten und Drittstaaten und internationale Organisationen sowie

(4) Der Empfänger darf die übermittelten personenbezogenen Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck nutzen, zu dem sie ihm übermittelt worden sind. Ausländische öffentliche Stellen, über- und zwischenstaatliche Stellen sowie Personen und Stellen außerhalb des öffentlichen Bereichs sind bei der Datenübermittlung darauf hinzuweisen.

Personen und Stellen außerhalb des öffentlichen Bereichs sind bei der Datenübermittlung darauf hinzuweisen.“

g) Folgender Absatz 8 wird angefügt:

„(8) Andere Rechtsvorschriften für die Datenübermittlung bleiben unberührt.“

23. § 27 wird wie folgt geändert:

a) In der Überschrift werden die Wörter „zwischen Polizeibehörden“ durch die Wörter „im innerstaatlichen Bereich“ ersetzt.

b) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 werden nach dem Wort „Aufgaben“ die Wörter „oder der des Empfängers“ eingefügt.

bb) In Satz 2 werden die Wörter „zulässig, soweit die Daten auch zu diesem Zweck erhoben werden dürfen“ durch die Wörter „für die nach § 11 erhobenen Daten nicht zulässig“ ersetzt.

cc) Satz 3 wird aufgehoben.

§ 27 Datenübermittlung zwischen Polizeibehörden

(1) Zwischen Polizeibehörden können personenbezogene Daten übermittelt werden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Eine Übermittlung zu einem anderen Zweck als dem, zu dem die Daten erlangt oder gespeichert worden sind, ist zulässig, soweit die Daten auch zu diesem Zweck erhoben werden dürfen. Satz 2 gilt nicht für die nach § 11 erhobenen Daten.

c) Absatz 2 wird wie folgt gefasst:

„(2) Die Polizei kann an andere als die in Absatz 1 genannten Behörden und sonstige öffentliche Stellen personenbezogene Daten übermitteln, soweit dies

1. in anderen Rechtsvorschriften vorgesehen ist oder
 2.
 - a) zur Erfüllung polizeilicher Aufgaben,
 - b) zur Abwehr einer Gefahr durch die empfangende Stelle,
 - c) auf Grund tatsächlicher Anhaltspunkte zur Wahrnehmung einer sonstigen Gefahrenabwehraufgabe durch die empfangende Stelle,
 - d) zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder
 - e) zur Verhütung oder Beseitigung einer schwer wiegenden Beeinträchtigung der Rechte einer Person
- erforderlich ist.“

d) Folgender Absatz 3 wird angefügt:

„(3) Die Polizei kann personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies

1. gemäß Absatz 2 Nummer 2 Buchstabe a, b, d oder e erforderlich ist,
2. die oder der Auskunftsbegehrende ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, dass das Geheimhaltungsinteresse der betroffenen Person überwiegt oder
3. der oder die Auskunftsbegehrende ein berechtigtes Interesse geltend macht und offensichtlich ist, dass die Datenübermittlung im Interesse der betroffenen Person liegt und sie

(2) Das Innenministerium wird ermächtigt, durch Rechtsverordnung zu bestimmen, dass die Datenübermittlung gemäß Absatz 1 an Polizeibehörden bestimmter ausländischer Staaten zulässig ist, wenn dies wegen der internationalen polizeilichen Zusammenarbeit oder der polizeilichen Zusammenarbeit im Grenzgebiet erforderlich ist und kein Grund zu der Annahme besteht, dass die Daten von den ausländischen Polizeibehörden entgegen dem Zweck eines deutschen Gesetzes, insbesondere entgegen den Vorschriften zur Speicherungs-, Nutzungs- oder Übermittlungsbeschränkung oder zur Löschungsverpflichtung verwandt werden. § 28 bleibt unberührt.

in Kenntnis der Sachlage ihre Einwilligung hierzu erteilen würde.“.

24. Die §§ 28 und 29 werden wie folgt gefasst:

**„§ 28
Datenübermittlung im Bereich der
Europäischen Union und deren Mit-
gliedsstaaten**

(1) § 27 gilt entsprechend für die Übermittlung von personenbezogenen Daten an

1. Polizeibehörden,
2. öffentliche und nichtöffentliche Stellen in Mitgliedstaaten der Europäischen Union und
3. zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten, die mit Aufgaben der Gefahrenabwehr sowie Verhütung von Straftaten und deren vorbeugende Bekämpfung befasst sind.

(2) Die Zulässigkeit der Übermittlung personenbezogener Daten durch die Polizei an eine Polizeibehörde oder eine sonstige für die Verhütung von Straftaten oder deren vorbeugende Bekämpfung zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union auf der Grundlage besonderer völkerrechtlicher Vereinbarungen bleibt unberührt.

**§ 28
Datenübermittlung an öffentliche
Stellen, an ausländische öffentliche
Stellen sowie an über- und zwischen-
staatliche Stellen**

(1) Die Polizei kann von sich aus personenbezogene Daten an öffentliche Stellen sowie an ausländische öffentliche und an über- und zwischenstaatliche Stellen übermitteln, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.

(2) Die Polizei kann von sich aus anderen für die Gefahrenabwehr zuständigen öffentlichen Stellen bei ihr vorhandene personenbezogene Daten übermitteln, soweit die Kenntnis dieser Daten zur Aufgabenerfüllung des Empfängers für den Bereich der Gefahrenabwehr erforderlich erscheint.

(3) Die Polizei kann auf Ersuchen personenbezogene Daten an öffentliche Stellen übermitteln, soweit dies

1. zur Abwehr einer Gefahr durch den Empfänger,
2. in besonders gelagerten Einzelfällen zur Wahrnehmung einer sonstigen Gefahrenabwehraufgabe durch den Empfänger,
3. zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer Person

erforderlich ist.

(4) Die Polizei kann personenbezogene Daten auf Ersuchen an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, soweit dies zur Abwehr einer erheblichen Gefahr durch den Empfänger erforderlich ist. Die Datenübermittlung unterbleibt, soweit Grund zu der Annahme besteht, dass dadurch gegen den Zweck eines deutschen Gesetzes, insbesondere gegen die Vorschriften zur Speicherungs-, Nutzungs- oder Übermittlungsbeschränkung oder zur Lösungsverpflichtung verstoßen wird, oder schutzwürdige Belange der betroffenen Person beeinträchtigt werden.

§ 29 Datenübermittlung im internationalen Bereich

(1) Eine Übermittlung personenbezogener Daten an andere als die in § 28 Absatz 1 Nummer 2 genannten Staaten (Drittländer) und andere als in § 28 Absatz 1 Nummer 3 genannte über- und zwischenstaatliche Stellen ist unter Beachtung der §§ 62 bis 65 des Datenschutzgesetzes Nordrhein-Westfalen zulässig, soweit dies zur Erfüllung polizeilicher Aufgaben oder zur Abwehr einer erheblichen Gefahr durch die empfangende Stelle erforderlich ist. Entsprechendes gilt, wenn tatsächliche Anhaltspunkte dafür bestehen, dass Straftaten von erheblicher Bedeutung begangen werden sollen und die Datenübermittlung zur Verhinderung dieser Straftaten erforderlich ist. § 23 gilt auch bei der Datenübermittlung in Drittstaaten. § 28 Absatz 2 gilt entsprechend.

(2) Bei Übermittlungen nach dieser Vorschrift hat die Polizei einen Nachweis zu führen, aus dem der Anlass, der Inhalt, die empfangende Stelle, der Tag der Übermittlung sowie die Aktenfundstelle hervorgehen. Er ist am Ende des Kalenderjahres, das dem Jahr seiner Erstellung

§ 29 Datenübermittlung an Personen oder an Stellen außerhalb des öffentlichen Bereichs

(1) Die Polizei kann von sich aus personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies

1. zur Erfüllung ihrer Aufgaben,
2. zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer Person

erforderlich ist.

(2) Die Polizei kann auf Antrag von Personen oder Stellen außerhalb des öffentlichen Bereichs personenbezogene Daten übermitteln, soweit die oder der Auskunftsbegehrende

1. ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, dass das Geheimhaltungsinteresse der betroffenen Person überwiegt,
2. ein berechtigtes Interesse geltend macht und offensichtlich ist, dass die Datenübermittlung im Interesse der

lung folgt, zu löschen oder zu vernichten. Die Löschung oder Vernichtung unterbleibt, solange der Nachweis noch für eine bereits eingeleitete Datenschutzkontrolle nach § 33c erforderlich ist oder Grund zu der Annahme besteht, dass im Falle einer Löschung schutzwürdige Belange der betroffenen Person beeinträchtigt würden.“.

25. § 30 Absatz 3 wird wie folgt gefasst:

„(3) Die Polizei kann an öffentliche Stellen sowie über- und zwischenstaatliche Stellen der Europäischen Union und deren Mitgliedsstaaten sowie an Drittstaaten und andere als in § 28 Absatz 1 Nummer 3 genannte über- und zwischenstaatliche Stellen Ersuchen auf Übermittlung von personenbezogenen Daten stellen, soweit die Voraussetzungen für eine Datenerhebung vorliegen und gesetzlich nichts anderes bestimmt ist.

„Sollten zu diesem Zweck personenbezogene Daten an öffentliche Stellen eines Drittstaates übermittelt werden, gelten § 26 Absätze 5 und 6 sowie § 29.“.

betroffenen Person liegt und sie in Kenntnis der Sachlage ihre Einwilligung hierzu erteilen würde.

§ 30

Datenübermittlung an die Polizei

(1) Öffentliche Stellen können, soweit gesetzlich nichts anderes bestimmt ist, von sich aus personenbezogene Daten an die Polizei übermitteln, wenn dies zur Erfüllung polizeilicher Aufgaben erforderlich erscheint.

(2) Die Polizei kann an öffentliche Stellen Ersuchen auf Übermittlung von personenbezogenen Daten stellen, soweit die Voraussetzungen für eine Datenerhebung vorliegen. Die ersuchte öffentliche Stelle prüft die Zulässigkeit der Datenübermittlung. Wenn gesetzlich nichts anderes bestimmt ist, prüft sie nur, ob das Ersuchen im Rahmen der Aufgaben der Polizei liegt, es sei denn, im Einzelfall besteht Anlass zur Prüfung der Rechtmäßigkeit des Ersuchens. Die Polizei hat die zur Prüfung erforderlichen Angaben zu machen. Die ersuchte öffentliche Stelle hat die Daten an die Polizei zu übermitteln, soweit gesetzlich nichts anderes bestimmt ist.

(3) Die Polizei kann an ausländische öffentliche Stellen sowie über- und zwischenstaatliche Stellen Ersuchen auf Übermittlung von personenbezogenen Daten stellen, soweit die Voraussetzungen für eine Datenerhebung vorliegen und gesetzlich nichts anderes bestimmt ist.

26. Die §§ 32 und 33 werden wie folgt gefasst:

**„§ 32
Berichtigung, Löschung und Einschränkung der Weiterverarbeitung von Daten**

(1) Personenbezogene Daten sind nach Maßgabe des § 54 in Verbindung mit § 50 Absatz 3 bis 5 des Datenschutzgesetzes Nordrhein-Westfalen zu berichtigen, zu löschen oder in der Verarbeitung einzuschränken. Darüber hinaus sind personenbezogene Daten zu löschen und die dazugehörigen Akten zu vernichten, wenn

1. dies durch dieses Gesetz bestimmt ist,
2. die Speicherung nicht zulässig ist oder
3. bei der zu bestimmten Terminen vorzunehmenden Prüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass die Daten für die Erfüllung der Aufgaben der speichernden Stelle nicht mehr erforderlich sind.

In Bezug auf Nummer 3 sind die in diesem Zusammenhang in Dateien suchfähig gespeicherten personenbezogenen Daten zu löschen sowie die zu der Person suchfähig angelegten Akten zu vernichten. Dies gilt auch, wenn der Verdacht einer Straftat gegen die Person entfallen ist.

Eine nach Satz 2 Nummer 3 vorzunehmende Aktenvernichtung ist nur durchzuführen, wenn die gesamte Akte für die Aufgabenerfüllung nicht mehr erforderlich ist, es sei denn, dass die betroffene Person die Vernichtung von Teilen der Akte verlangt und die weitere Speicherung sie in unangemessener Weise beeinträchtigt. Soweit hiernach eine Vernichtung nicht in Betracht kommt, sind

**§ 32
Berichtigung, Löschung und Sperrung von Daten**

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Sind personenbezogene Daten in Akten zu berichtigen, ist in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten unrichtig waren oder geworden sind.

(2) In Dateien suchfähig gespeicherte personenbezogene Daten und die dazugehörigen zu den Personen suchfähig angelegten Akten sind zu löschen oder zu vernichten, wenn

1. dies durch dieses Gesetz bestimmt ist,
2. die Speicherung nicht zulässig ist,
3. bei der zu bestimmten Terminen vorzunehmenden Prüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass die Daten für die Erfüllung der Aufgaben der speichernden Stelle nicht mehr erforderlich sind.

In Dateien nicht suchfähig gespeicherte Daten sind unter den Voraussetzungen des Satzes 1 zu löschen, soweit die Speicherung festgestellt wird. Die nach Satz 1 Nr. 3 vorzunehmende Aktenvernichtung ist nur durchzuführen, wenn die gesamte Akte für die Aufgabenerfüllung nicht mehr erforderlich ist, es sei denn, dass die betroffene Person die Vernichtung von Teilen der Akte verlangt und die weitere Speicherung sie in unangemessener Weise beeinträchtigt. Soweit hiernach eine Vernichtung nicht in Betracht kommt, sind die Daten zu sperren und mit einem Sperrvermerk zu versehen.

(3) Andere als die in Absatz 2 genannten Akten sind nach Ablauf der jeweiligen Aufbewahrungsfrist zu vernichten.

die Daten in ihrer Verarbeitung einzuschränken und mit einem entsprechenden Vermerk zu versehen.

Andere als die in den Sätzen 2 und 5 genannten Akten sind nach Ablauf der jeweiligen Aufbewahrungsfristen zu vernichten.

(2) Stellt die Polizei fest, dass personenbezogene Daten in Akten unrichtig sind, ist die gemäß § 54 Absatz 1 des Datenschutzgesetzes Nordrhein-Westfalen genannte Berichtigungspflicht dadurch zu erfüllen, dass dies in der Akte vermerkt oder auf sonstige Weise festgehalten wird. Dabei ist in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten unrichtig waren oder geworden sind. Bestreitet die betroffene Person die Richtigkeit sie betreffender personenbezogener Daten und lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, sind die Daten entsprechend zu kennzeichnen, um eine Verarbeitungseinschränkung nach § 50 Absatz 1 Satz 3 des Datenschutzgesetzes Nordrhein-Westfalen zu ermöglichen.

(3) Löschung und Vernichtung unterbleiben in den in § 50 Absatz 3 des Datenschutzgesetzes Nordrhein-Westfalen genannten Fällen. Darüber hinaus unterbleiben Löschung und Vernichtung, wenn

1. Grund zu der Annahme besteht, dass schutzwürdige Belange der betroffenen Person beeinträchtigt werden,
2. die Daten zur Behebung einer bestehenden Beweisnot unerlässlich sind oder
3. die Nutzung der Daten zu wissenschaftlichen Zwecken erforderlich ist; § 24a bleibt unberührt.

In diesen Fällen sind die Daten in ihrer Verarbeitung einzuschränken und mit

(4) Stellt die Polizei fest, dass unrichtige oder nach Absatz 2 Satz 1 Nr. 2 zu löschende personenbezogene Daten übermittelt worden sind, ist dem Empfänger die Berichtigung oder Löschung mitzuteilen, es sei denn, die Mitteilung ist für die Beurteilung der Person oder des Sachverhalts nicht oder nicht mehr von Bedeutung.

(5) Löschung und Vernichtung unterbleiben, wenn

1. Grund zu der Annahme besteht, dass schutzwürdige Belange der betroffenen Person beeinträchtigt werden,
2. die Daten zur Behebung einer bestehenden Beweisnot unerlässlich sind,
3. die Nutzung der Daten zu wissenschaftlichen Zwecken erforderlich ist.

In diesen Fällen sind die Daten zu sperren und mit einem Sperrvermerk zu versehen. Sie dürfen nur zu den in Satz 1 genannten Zwecken oder sonst mit Einwilligung der betroffenen Person genutzt werden. Im Falle des Satzes 1 Nr. 3 gilt § 28 des Datenschutzgesetzes Nordrhein-Westfalen.

(6) Anstelle der Löschung oder Vernichtung sind die Datenträger oder die Akten an ein Staatsarchiv abzugeben, soweit archivrechtliche Regelungen dies vorsehen.

einem entsprechenden Vermerk zu versehen. Sie dürfen nur zu den in Satz 1 genannten Zwecken oder sonst mit Einwilligung der betroffenen Person genutzt werden. Im Falle des Satzes 1 Nummer 3 gilt § 24a.

(4) Vor einer Löschung oder Vernichtung ist ein Anbieten für eine Übernahme durch das Landesarchiv Nordrhein-Westfalen gemäß § 4 Absatz 1 des Archivgesetzes Nordrhein-Westfalen vom 16. März 2010 (GV. NRW. S. 188), das zuletzt durch Gesetz vom 16. September 2014 (GV. NRW. S. 603) geändert worden ist, zu prüfen, soweit archivrechtliche Regelungen dies vorsehen.

§ 33

Benachrichtigung bei verdeckten und eingriffsintensiven Maßnahmen

(1) Über eine Maßnahme gemäß § 16a Absatz 1, §§ 17 bis 21 und 31 sind zu benachrichtigen im Falle

1. des § 16a Absatz 1 und des § 17, die Zielperson und die erheblich mitbetroffenen Personen,
2. des § 18
 - a) die Person, gegen die sich die Maßnahme richtete,
 - b) sonstige überwachte Personen oder
 - c) Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten,
3. der §§ 19 und 20,
 - a) die Zielperson,
 - b) die erheblich mitbetroffenen Personen

§ 33

Errichtung von Dateien, Umfang des Verfahrensverzeichnisses, Freigabe von Programmen, automatisiertes Abrufverfahren

(1) Die Errichtung von Dateien ist auf das erforderliche Maß zu beschränken. In angemessenen Abständen ist die Notwendigkeit ihrer Weiterführung oder Änderung zu prüfen.

(2) In dem nach § 8 des Datenschutzgesetzes Nordrhein-Westfalen zu erstellenden Verfahrensverzeichnis sind die durch dieses Gesetz vorgeschriebenen Löschungs- oder die gemäß den §§ 22 und 24 Abs. 2 festzulegenden Prüfungs- oder Aufbewahrungsfristen aufzuführen.

(3) Ein Verfahrensverzeichnis nach § 8 des Datenschutzgesetzes Nordrhein-Westfalen ist auch zu erstellen, wenn die Polizei personenbezogene Daten in einer automatisierten polizeilichen Verbunddatei speichert, die über das Land hinausgeht.

(4) Über die Freigabe von Programmen zur Verarbeitung personenbezogener Daten auf zentralen oder dezentralen Datenverarbeitungsanlagen entscheidet das Innenministerium oder eine von diesem beauftragte Stelle.

- c) die Personen, deren nicht allgemein zugängliche Wohnung durch die Vertrauensperson oder den verdeckten Ermittler betreten wurde,
- 4. des § 20a Absatz 1 Nummer 2 (Verkehrsdaten) die Beteiligten der betroffenen Telekommunikation,
- 5. des § 20a Absatz 1 Nummer 3 (Nutzungsdaten) der Nutzer,
- 6. des § 20b die Zielperson,
- 7. des § 20c die Beteiligten der überwachten Telekommunikation
- 8. des § 21 die Zielperson und die Personen, deren personenbezogene Daten gemeldet wurden; die Benachrichtigung umfasst auch die Tatsache der Löschung.

(2) Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme möglich ist. Sind die personenbezogenen Daten in ein Strafverfahren eingeführt worden, so ist vor Benachrichtigung an die im Absatz 1 genannten betroffenen Personen die Zustimmung der zuständigen Staatsanwaltschaft einzuholen. Eine Benachrichtigung nach Absatz 1 Nummer 3 erfolgt, sobald dies auch ohne Gefährdung der Möglichkeit der weiteren Verwendung der Vertrauensperson oder verdeckten Ermittlers möglich ist.

(3) Die Benachrichtigung nach Absatz 2 unterbleibt, soweit dies im überwiegenden Interesse der betroffenen Person liegt oder der Benachrichtigung schutzwürdige Belange einer anderen betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung der gemäß Absatz 1 Nummer 4 und 7 genannten Personen, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen sind und anzunehmen ist, dass sie kein Interesse an der

(5) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten aus einer von der Polizei geführten Datei durch Abruf ermöglicht, ist unter den Voraussetzungen des § 9 des Datenschutzgesetzes Nordrhein-Westfalen zulässig; der Abruf darf nur Polizeibehörden gestattet werden.

(6) Das Innenministerium kann zur Erfüllung von Aufgaben der Gefahrenabwehr, die nicht nur von örtlicher Bedeutung sind, mit anderen Ländern und dem Bund eine Verbunddatei der Polizei vereinbaren, die eine automatisierte Datenübermittlung ermöglicht. In der Vereinbarung ist festzulegen, welcher Polizeibehörde die nach diesem Gesetz oder nach anderen Rechtsvorschriften bestehenden Pflichten einer speichernden Stelle obliegen. Die Einrichtung einer Verbunddatei mit automatisierter Abrufmöglichkeit, an der neben der Polizei auch andere Behörden beteiligt sind, ist nur zulässig nach dem Antiterrordateigesetz vom 22. Dezember 2006 (BGBl. I S. 3409), geändert durch Artikel 5 des Gesetzes vom 26. Februar 2008 (BGBl. I S. 215), und nach dem Rechtsextremismus-Datei-Gesetz vom 20. August 2012 (BGBl. I S. 1798). In eine Datei gemäß Satz 3 dürfen nur Daten eingegeben werden, die gemäß § 24 suchfähig in einer Datei gespeichert und den beteiligten Behörden gemäß §§ 26 ff. übermittelt werden können; § 26 Absatz 1 Satz 3 findet keine Anwendung.

Benachrichtigung haben. Nachforschungen zur Feststellung der Identität einer in Satz 2 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. Das Unterbleiben und die Zurückstellung der Benachrichtigung sind zu dokumentieren.

(4) Erfolgt eine Benachrichtigung gemäß Absatz 2 Satz 1 nicht binnen sechs Monaten nach Abschluss der Maßnahme, bedarf die weitere Zurückstellung der richterlichen Zustimmung. Die richterliche Entscheidung ist jeweils nach einem Jahr erneut einzuholen. Über die Zustimmung entscheidet das Gericht, das für die Anordnung der Maßnahme zuständig gewesen ist. Bedurfte die Maßnahme nicht der richterlichen Anordnung, ist für die Zustimmung das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat, zuständig. Nach zweimaliger Verlängerung ist die Zustimmung des für die Einlegung einer Beschwerde zuständigen Gerichts einzuholen. § 68 Absatz 4 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit findet keine Anwendung. Fünf Jahre nach Beendigung der Maßnahme kann mit gerichtlicher Zustimmung endgültig von der Benachrichtigung abgesehen werden, wenn die Voraussetzungen für die Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden, eine weitere Verwendung der Daten gegen den Betroffenen ausgeschlossen ist und die Daten gelöscht wurden. Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, beginnt die in Satz 1 genannte Frist mit der Beendigung der letzten Maßnahme.

(5) Werden personenbezogene Daten von Kindern, die ohne Kenntnis der Sorgeberechtigten erhoben worden sind,

gespeichert, sind die Sorgeberechtigten durch die Polizei zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Maßnahme erfolgen kann. Von der Unterrichtung kann abgesehen werden, solange zu besorgen ist, dass die Unterrichtung zu erheblichen Nachteilen für das Kind führt.

(6) Bei der Benachrichtigung gelten darüber hinaus die Vorgaben des § 48 Absatz 1 und Absatz 3 des Datenschutzgesetzes Nordrhein-Westfalen. Außerdem ist auf die Möglichkeit nachträglichen Rechtsschutzes hinzuweisen. Die Benachrichtigung hat in klarer und einfacher Sprache zu erfolgen.“

27. Nach § 33 werden die folgenden §§ 33a bis 33c eingefügt:

**„§ 33a
Benachrichtigung im Falle der Verletzung des Schutzes personenbezogener Daten**

(1) Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich eine erhebliche Gefahr für Rechtsgüter betroffener Personen zur Folge, so hat die Polizei die betroffenen Personen unverzüglich zu benachrichtigen.

(2) Die Benachrichtigung nach Absatz 1 hat in klarer und einfacher Sprache die Art der Verletzung und ergänzend zumindest folgende Informationen zu enthalten:

1. den Namen und die Kontaktdaten des oder der Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
2. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und
3. eine Beschreibung der von der Polizei ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung

der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls der Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Eine Benachrichtigung gemäß Absatz 1 entfällt, wenn

1. die Polizei geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden. Dies gilt insbesondere für Vorkehrungen wie Verschlüsselungen, durch die die Daten für unbefugte Personen unzugänglich gemacht wurden,
2. die Polizei durch die im Anschluss an die Verletzung getroffenen Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach keine erhebliche Gefahr mehr im Sinne des Absatz 1 besteht, oder
3. dies mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall hat stattdessen durch die Polizei eine öffentliche Bekanntmachung oder ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichsweise wirksam informiert werden.

Die Gründe der Entscheidung sind zu dokumentieren.

(4) Die Polizei kann eine Benachrichtigung unter den in § 48 Absatz 2 des Datenschutzgesetzes Nordrhein-Westfalen genannten Voraussetzungen aufschieben, einschränken oder unterlassen, soweit nicht die Interessen der betroffenen Personen aufgrund der von der Verletzung ausgehenden erheblichen Gefahr im Sinne des Absatz 1 überwiegen. Die Gründe der Entscheidung sind zu dokumentieren.

(5) Wenn der Verantwortliche die betroffene Person über eine Verletzung des Schutzes personenbezogener Daten nicht benachrichtigt hat, kann die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit verlangen, dies nachzuholen oder verbindlich feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind. Hierbei hat sie oder er die Wahrscheinlichkeit zu berücksichtigen, mit der die Verletzung des Schutzes personenbezogener Daten zu einer erheblichen Gefahr im Sinne des Absatzes 1 führt. § 59 des Datenschutzgesetzes Nordrhein-Westfalen bleibt unberührt.

§ 33b

Protokollierung bei verdeckten oder eingriffsintensiven Maßnahmen

(1) Bei einer Erhebung personenbezogener Daten gemäß § 16a Absatz 1, §§ 17 bis 21 und 31 sind zu protokollieren

1. das zur Datenerhebung eingesetzte Mittel,
2. der Zeitpunkt des Einsatzes,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen und
4. die Organisationseinheit, die die Maßnahme durchführt.

(2) Zudem sind je nach Durchführung der konkreten Maßnahme die betroffenen Personen im Sinne des § 33 Absatz 1 Nummer 1 bis 8 zu dokumentieren.

(3) Nachforschungen zur Feststellung der Identität einer in § 33 Absatz 1 Nummer 4 und 7 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. Die Zahl der Personen, deren Protokollierung unterblieben ist, ist im Protokoll anzugeben.

(4) Die Protokolldaten dürfen nur verwendet werden für Zwecke der Benachrichtigung nach § 33 und um der betroffenen Person oder der oder dem Landesbeauftragten für Datenschutz und Informationsfreiheit die Prüfung zu ermöglichen, ob die Maßnahmen rechtmäßig durchgeführt worden sind. Sie sind bis zum Abschluss der Kontrolle nach § 33c aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 1 genannten Zweck noch erforderlich sind.

(5) § 55 des Datenschutzgesetzes Nordrhein-Westfalen bleibt unberührt.

§ 33c Datenschutzkontrolle

Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit führt unbeschadet ihrer oder seiner sonstigen Aufgaben und Kontrollen mindestens alle zwei Jahre zumindest stichprobenartige Überprüfungen bezüglich der Datenverarbeitung bei nach § 33b zu protokollierenden Maßnahmen und von Übermittlungen an Drittstaaten gemäß des § 29 durch. Zu diesem Zwecke sind durch technische und organisatorische Maßnahmen in geeigneter auswertbarer Form die Protokollierungen gemäß § 29 und § 33b zur Verfügung zu stellen.“

28. § 34c Absatz 5 wird wie folgt geändert:

(Gesetz zur Stärkung der Sicherheit in Nordrhein-Westfalen - Sechstes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen)

§ 34c

Elektronische Aufenthaltsüberwachung

(...)

- a) In Satz 1 werden nach dem Wort „ist“ die Wörter „unter Beachtung des § 55 des Datenschutzgesetzes Nordrhein-Westfalen“ eingefügt.
- b) Satz 2 wird aufgehoben.

(5) Jeder Abruf der Daten ist zu protokollieren. Die Protokollierung muss den landesrechtlichen Vorschriften, die Artikel 25 der 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 (ABl. L 119 vom 4.5.2016, S. 89) umsetzen, entsprechen. Die Protokolldaten sind spätestens nach vierundzwanzig Monaten zu löschen.

(...)

29. Folgender § 68 wird angefügt:

**„§ 68
Berichtspflichten gegenüber dem
Landtag**

Die Landesregierung berichtet dem Landtag alle zwei Jahre über die nach den §§ 16a, 17 bis 20 und 21 getroffenen Maßnahmen und über Übermittlungen nach § 29. Bei Maßnahmen nach § 16a entfällt die Berichtspflicht, wenn die Observation offen durchgeführt wurde. Abweichend von Satz 1 ist dem Landtag über die nach § 20a bis 20c getroffenen Maßnahmen jährlich zu berichten. In den Berichten wird insbesondere dargestellt, in welchem Umfang von welchen Befugnissen, aus Anlass welcher Verdachtslagen Gebrauch gemacht wurde und inwieweit die betroffenen Personen

hierüber benachrichtigt wurden. Der Landtag macht die Berichte in anonymisierter Form öffentlich.“.

Artikel 2
Änderung des Ordnungsbehörden-
gesetzes

Das Ordnungsbehördengesetz in der Fassung der Bekanntmachung vom 13. Mai 1980 (GV. NRW. S. 528), das zuletzt durch Gesetz vom 6. Dezember 2016 (GV. NRW. S. 1062) geändert worden ist, wird wie folgt geändert:

1. Im Inhaltsverzeichnis wird in der Angabe zu § 24 nach dem Wort „Polizeigesetzes“ das Wort „, Datenschutz“ eingefügt.
2. § 24 wird wie folgt geändert:
 - a) In der Überschrift wird nach dem Wort „Polizeigesetzes“ das Wort „, Datenschutz“ eingefügt.
 - b) Der Wortlaut wird Absatz 1 und wie folgt geändert:
 - aa) In Nummer 1 werden nach der Angabe „§ 9“ die Wörter „mit Ausnahme des Absatzes 1“ eingefügt.
 - bb) In Nummer 6 werden nach der Angabe „§ 15“ die Wörter „mit Ausnahme des Absatzes 2“ eingefügt.
 - cc) Die Nummern 7 und 8 werden wie folgt gefasst:
 - „7. § 22 mit Ausnahme des Absatzes 2 Sätze 5 bis 7 sowie der Absätze 3 und 5,

Gesetzes über Aufbau und Befugnisse
der Ordnungsbehörden
- Ordnungsbehördengesetz (OBG) -

§ 24 Geltung des Polizeigesetzes

§ 24
Geltung des Polizeigesetzes

Folgende Vorschriften des Polizeigesetzes des Landes Nordrhein-Westfalen gelten entsprechend für die Ordnungsbehörden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist:

1. § 9,
2. § 10 mit Ausnahme des Absatzes 1 Nr. 2 und des Absatzes 3 Satz 1 Nr. 2,
3. § 11,
4. § 12 mit Ausnahme des Absatzes 1 Nr. 4,
5. § 13,
6. § 15,
7. §§ 22 und 23,

- | | |
|--|--|
| <p>8. § 23 mit Ausnahme des Absatzes 1 Satz 3, des Absatzes 2 Satz 3 und 5, des Absatzes 3 Satz 2 und des Absatzes 6, “</p> | <p>8. § 24 mit Ausnahme der Absätze 2, 4 und 5,</p> |
| <p>dd) In Nummer 9 wird die Angabe „Satz 3“ durch die Wörter „Satz 2, des Absatzes 4, des Absatzes 6, soweit die Datenübermittlung nach § 29 betroffen ist, und des Absatzes 7“ ersetzt.</p> | <p>9. § 26 mit Ausnahme des Absatzes 1 Satz 3,</p> |
| <p>ee) Die Nummern 10 und 11 werden wie folgt gefasst:</p> <p>„10. §§ 27 und 28,</p> <p>11. § 30 mit Ausnahme des Absatzes 3 Satz 2 und“</p> | <p>10. § 27 mit Ausnahme des Absatzes 2,</p> <p>11. §§ 28 bis 30,</p> |
| <p>ff) Nummer 12 wird aufgehoben.</p> | <p>12. § 32,</p> |
| <p>gg) Nummer 13 wird Nummer 12.</p> | <p>13. § 34 mit Ausnahme von Absatz 2, § 35 mit Ausnahme von Absatz 1 Nr. 4, §§ 36 bis 46.</p> |
- d) Folgender Absatz 2 wird angefügt:
- „(2) Für die Verarbeitung personenbezogener Daten durch die Ordnungsbehörden zur Erfüllung ihrer Aufgaben nach diesem Gesetz gilt im Übrigen 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 (ABl. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72) und ergänzend Teil 1 und Teil 2 des Datenschutzgesetzes Nordrhein-Westfalen vom [einsetzen: Ausfertigungsdatum und Fundstelle des neuen Datenschutzgesetzes]in der jeweils geltenden Fassung.“

Artikel 3

Durch diese Gesetze wird das Grundrecht aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes (Recht auf informationelle Selbstbestimmung) eingeschränkt.

Artikel 4

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

BEGRÜNDUNG

A. Allgemeiner Teil

I. Zielsetzung

Die EU-Datenschutzreform, bestehend aus der sog. Datenschutz-Grundverordnung (DSGVO, Fn. 4) und der sog. Datenschutz-Richtlinie für Justiz und Inneres (JI-Richtlinie, Fn. 5) ist zum 25. Mai 2016 in Kraft getreten. Die JI-Richtlinie ist bis zum 6. Mai 2018 in nationales Recht umzusetzen. Die DSGVO gilt unmittelbar in den Mitgliedstaaten. Sie wird ab dem 25. Mai 2018 europaweit unmittelbar anwendbar sein.

Der Bund hat mit der Neufassung des Bundesdatenschutzgesetzes (BDSG) vom 30. Juni 2017 bereits den allgemeinen Teil des Datenschutzrechts angepasst. Weitere besondere Bereiche werden noch folgen. Auf Landesebene werden bereichsübergreifende Regelungen mit dem vom Ministerium des Innern vorgelegten Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Nordrhein-Westfälisches Datenschutz-Anpassungs- und Umsetzungs-gesetz EU - NRWDSAnpUG-EU - LT-Drs. 17/1981) umgesetzt.

Darauf aufbauend besteht auch im Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW) sowie im Gesetz über Aufbau und Befugnisse der Ordnungsbehörden des Landes Nordrhein-Westfalen (OBG) ein datenschutzrechtlicher Anpassungsbedarf. Systematisch gilt das neugefasste Datenschutzgesetz Nordrhein-Westfalen (DSG NRW-Neu) grundsätzlich für den gesamten Anwendungsbereich des PolG NRW und OBG. Bereichsspezifische Regelungen gehen jedoch solchen des DSG NRW-Neu vor.

Neben dem EU-Gesetzgeber hat auch das Bundesverfassungsgericht (BVerfG) in seinem sog. BKA-Urteil vom 20. April 2016, Fn. 6, grundsätzliche Aussagen zum polizeilichen Datenschutz getroffen. Wenngleich sich das Urteil formal lediglich auf das bestehende Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) bezieht, gelten die Vorgaben mittelbar auch für die vergleichbaren Regelungen in den Polizeigesetzen der Länder und müssen dementsprechend auch dort umgesetzt werden. Dies ist auch Bestandteil des Koalitionsvertrages.

Vor dem Hintergrund der ohnehin anstehenden Umsetzung des EU-Datenschutzpaketes werden mit diesem Gesetzentwurf die o.g. vom BVerfG vorgegebenen Datenschutzgrundsätze gleichzeitig im PolG NRW angepasst. Die gemeinsame Umsetzung ist aufgrund des überschneidenden Sachzusammenhangs zwingend notwendig. Die Erforderlichkeit der Umsetzung der weiteren Vorgaben des BVerfG in Bezug auf die Verhältnismäßigkeit der einzelnen polizeilichen Eingriffsbefugnisse wird demgegenüber parallel überprüft und in einer separaten Novelle eingebracht.

⁴ 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72)

⁵ 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

⁶ Vgl. Urteil des BVerfG vom 20.04.2016, 1 BvR 966/09 und 1 BvR 1140/09.

§ 24 OBG wird an die Änderungen des PolG NRW im Artikel 1 unter Berücksichtigung der europäischen Datenschutzreform und der hieraus folgenden Novellierung des DSG NRW angepasst. Um die für die nichtpolizeiliche Gefahrenabwehr notwendigen Regelungen des PolG NRW auch künftig anwendbar zu machen, werden die einschlägigen Verweisungen als Folgeänderungen angepasst.

Die nichtpolizeiliche Gefahrenabwehr nach dem Ordnungsbehördengesetz unterfällt unmittelbar und vorrangig dem Geltungsbereich der DSGVO. Dies bedeutet für die Praxis, dass zunächst die DSGVO anzuwenden ist. Ergänzt werden die Regelungen der DSGVO durch das Datenschutzgesetz Nordrhein-Westfalen, insbesondere durch die Durchführungsbestimmungen zur Verordnung (EU) 2016/679 im Teil 2 des DSG NRW.

Soweit wegen der besonderen Sachmaterie spezielle Regelungen zum Datenschutz im PolG NRW getroffen wurden, wird auf diese verwiesen. Da - anders als die nicht straftatenbezogene Gefahrenabwehr der Ordnungsbehörden - das Handeln der Polizeibehörden zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung dem Geltungsbereich der JI-Richtlinie unterfällt, können die Verweise in das PolG NRW nur eingeschränkt erfolgen. Eine Verweisung auf das PolG NRW entfällt, soweit die Regelung im PolG NRW auf die JI-Richtlinie bzw. auf Teil 3 DSG NRW-Neu, der die JI-Richtlinie ins nationale Recht umsetzt, Bezug nimmt. Gleiches gilt, wenn die Materie bereits in der DSGVO unmittelbar geregelt ist, so z.B. die Datenübermittlung an Drittländer oder internationale Organisationen im Kapitel V, Art. 44 ff. DSGVO.

Die Verfolgung und Ahndung von Ordnungswidrigkeiten durch die Ordnungsbehörden unterfällt dagegen der Geltung der JI-Richtlinie und gem. § 35 Abs. 2 DSG NRW-Neu den richtlinienbezogenen Regelungen des Teils 3 des DSG NRW-Neu und ist von dieser Gesetzesanpassung nicht betroffen.

II. Wesentlicher Inhalt

Der datenschutzrechtliche Änderungsbedarf, der sich zum einen aus der EU-Datenschutzreform und zum anderen aus den Datenschutz-Vorgaben des BVerfG ergibt, soll einheitlich durch diesen Gesetzentwurf im PolG NRW umgesetzt werden, da diese Regelungsmaterien in engem systematischen und sachlichen Zusammenhang stehen.

Der Gesetzentwurf sieht im Wesentlichen folgende Regelungen vor:

1. Einführung einer allgemeinen Rechtsgrundlage für die Erhebung von personenbezogenen Daten durch die Polizei
2. Einführung der Einwilligung als Zulässigkeitsgrund für Datenerhebungen durch die Polizei
3. Anpassungen im Bereich der Erhebung besonderer Kategorien von Daten
4. Umsetzung des vom BVerfG in seinem sog. BKA-Urteil konkretisierten Grundsatzes der hypothetischen Datenenerhebung
5. Einführung einer Kennzeichnungspflicht für Daten entsprechend § 14 BKAG-Neu

6. Bündelung von Benachrichtigungs-, Protokollierungs- und Berichtspflichten an den Landtag.

Im Artikel 2 des Gesetzentwurfs werden die Verweisungen in § 24 OBG an die Änderungen des PolG NRW unter Berücksichtigung der europäischen Datenschutzreform angepasst.

B. Besonderer Teil

Zu Artikel 1

Nr. 1 (Inhaltsübersicht):

Durch den Gesetzesentwurf werden die §§ 22a, 23a, 24a, 33a, 33b, 33c und 68 neu eingefügt. Die Angaben zu den §§ 9, 22, 23, 24, 27, 28, 29, 33 und dem zweiten Titel werden neu gefasst. Zudem wird dem § 26 eine Angabe angefügt und in § 32 eine Angabe ersetzt. Die Inhaltsüberschrift wird entsprechend angepasst.

Nr. 2 (§ 9):

Allgemeines

Durch Einfügung eines neuen Absatz 1 werden u.a. systematische Anpassungen an das neu gefasste Datenschutzgesetz Nordrhein-Westfalen getroffen. In § 4 Absatz 1 Buchstabe b) DSGVO NRW-Neu in der bisherigen Fassung war vorgesehen, dass die Verarbeitung personenbezogener Daten auch auf Grundlage einer Einwilligung einer betroffenen Person zulässig war. Im neuen Datenschutzgesetz Nordrhein-Westfalen existiert eine entsprechende allgemeine Bestimmung nicht, so dass diese nun spezialgesetzlich geschaffen werden muss. Der Vollständigkeit halber wird neben der Aufnahme der Einwilligung auch die in § 3 Absatz 1 DSGVO NRW-Neu vorhandene allgemeine Rechtsgrundlage für die Datenerhebung durch öffentliche Stellen spezialgesetzlich für die Polizei aufgenommen.

Absatz 1

Nummer 1

Die Vorschrift stellt eine Rechtsgrundlage gemäß Art. 8 der JI-Richtlinie dar.

Erster Halbsatz

Hier ist die allgemeine Rechtsgrundlage für die Erhebung personenbezogener Daten durch die Polizei zwecks polizeilicher Aufgabenwahrnehmung verankert.

Nummer 1, zweiter Halbsatz

Durch die Regelung wird klargestellt, dass die Polizei auch personenbezogene Daten erheben darf, die die betroffene Person offensichtlich öffentlich gemacht hat, zum Beispiel in sozialen Netzwerken. Zwecks einheitlicher Rechtsanwendung werden die Voraussetzungen des Art. 10 Buchstabe c) JI-Richtlinie für eine rechtmäßige Verarbeitung besonderer Kategorien von Daten auf die Erhebung aller personenbezogenen Daten übertragen.

Nummer 2

Im Zuge des Wegfalls der in § 4 Absatz 1 Buchstabe b) des Datenschutzgesetzes Nordrhein-Westfalen in der bisherigen Fassung geregelten Einwilligung, normiert die Vorschrift nun die Einwilligung spezialgesetzlich als Zulässigkeitsgrund der Erhebung personenbezogener Daten. Die Voraussetzungen einer wirksamen Einwilligung ergeben sich aus § 38 DSGVO NRW-Neu, auf den die Vorschrift daher Bezug nimmt.

Absatz 2

Inhalt des bisherigen Absatzes 1, der nach der Einfügung des neuen Absatzes 1 hierher verschoben wurde.

Absatz 3

Entspricht bisherigem Absatz 2, der redaktionell durch Bezug auf den neuen Absatz 2 angepasst wurde.

Absatz 4

Inhalt des bisherigen Absatzes 3.

Absatz 5

Inhalt des Absatzes 4 des Datenschutzgesetzes Nordrhein-Westfalen in der bisherigen Fassung. Der bisherige Absatz 5 wurde ersatzlos gestrichen. Für Satz 1 der bisherigen Fassung erfolgte dies, da sich eine entsprechende Vorgabe nun als allgemeine Bestimmung zur Zulässigkeit der Verarbeitung personenbezogener Daten in § 37 Nummer 2 DSG NRW-Neu findet. Satz 2 der bisherigen Fassung wurde gestrichen, da der Anwendungsbereich nun von § 22a abgedeckt ist. Nach der Einführung des neuen Begriffes der besonderen Kategorien von Daten und entsprechender Verarbeitungsvoraussetzungen in Art. 10 JI-Richtlinie, umgesetzt durch §§ 36 Nummer 18,45 DSG NRW-Neu, muss das Verhältnis dieser Daten zu sonstigen nicht tat- und gefahrenbezogenen Merkmalen im Sinne der bisherigen Fassung festgelegt werden. Grund hierfür ist, dass es Daten geben kann, die unter beide Kategorien fallen, jedoch bei unterschiedlichen Regelungsregimen unterschiedlichen Verarbeitungsvoraussetzungen unterliegen würden. Beispiele wären politische oder weltanschauliche bzw. religiöse Überzeugungen oder Daten zum Sexualleben. Laut Erwägungsgrund 37 zur JI-Richtlinie hat der europäische Gesetzgeber einen besonderen Schutz für alle Daten intendiert, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind. Auch der Landesgesetzgeber hat aufgrund der besonderen Rechtfertigungsbedürftigkeit der Erhebung von nicht tat- oder gefahrenbezogenen Merkmalen für diese einen besonderen Schutz vorgesehen. Daher erscheint es sachgerecht, im Sinne einer praktikablen Lösung, beide Datengruppen unter die besonderen Datenkategorien i.S.d. § 36 Nummer 18 i.V.m. § 45 DSG NRW-Neu zu fassen und den einheitlichen Voraussetzungen des § 22a zu unterwerfen.

Absatz 6

Absatz 6 bleibt unverändert

Absatz 7

In Absatz 7 wird der vormalige Absatz 5 Satz 1 aufgenommen.

Nr. 3 (§ 14):

Erkennungsdienstliche Maßnahmen stellen eine Verarbeitung besonderer Kategorien von Daten im Sinne des § 36 Nummer 18 DSG NRW-Neu dar und unterfallen damit den Voraussetzungen des § 45 DSG NRW-Neu. Die Verarbeitung muss daher „unbedingt erforderlich“ statt wie bisher einfach „erforderlich“ sein.

Nr. 4 (§ 14a):

Das Abstellen auf das neue Merkmal der „unbedingten Erforderlichkeit“ in Absatz 1 Satz 1 ist der Tatsache geschuldet, dass es sich bei den regelungsgegenständlichen molekulargenetischen Untersuchungen um die Verarbeitung besonderer Daten i.S.d. § 36 Ziff. 18 DSG NRW-Neu handelt und die entsprechende Datenverarbeitung damit den Voraussetzungen des § 45 Abs. 1 DSG NRW-Neu unterfallen.

Nr. 5 (§ 15):

In Absatz 2 erfolgt eine redaktionelle Anpassung der Verweise auf die Weiterverarbeitung zu besonderen Zwecken in § 24 Absatz 2 und 3 und auf die Berichtigung, Löschung und Einschränkung der Weiterverarbeitung von Daten in § 32 Absatz 3 und 4.

Nr. 6 (§ 15c):

Die bisher in Absatz 8 Satz 3 vorgesehene jährliche Berichtspflicht wurde ersatzlos gestrichen. Hintergrund ist das o.g. Urteil des BVerfG vom 20. April 2016, das eine entsprechende Berichtspflicht nur über verdeckte Überwachungsmaßnahmen fordert (a.a.O., Rz. 142, 143, 268, 340, 354). Diese wird in § 68 nunmehr einheitlich geregelt. Bei Maßnahmen nach § 15c handelt es sich jedoch um offen durchgeführte Maßnahmen. Eine hier durchzuführende jährliche Berichtspflicht würde dem in § 68 auf der Grundlage des vom BVerfG gesetzten Maßstabs widersprechen.

In Absatz 4 erfolgt eine redaktionelle Anpassung des Verweises auf die Berichtigung, Löschung und Einschränkung der Weiterverarbeitung von Daten in § 32 Absatz 3.

In Absatz 7 erfolgt eine redaktionelle Anpassung des Verweises auf die Nutzung personenbezogener Daten zu statistischen Zwecken und zu Zwecken der Aus- und Fortbildung in § 24 Absatz 2 und 3.

Nr. 7 (§ 16a):**Absatz 2**

Die Streichung der Kennzeichnungspflicht aus Satz 2 und der Pflicht zur Aufrechterhaltung der Kennzeichnung bei Übermittlungen an andere Stellen aus Satz 3 erfolgt vor dem Hintergrund der nun in § 23a Absatz 1 eingeführten allgemeinen Pflicht zur Kennzeichnung personenbezogener Daten bei Speicherung in polizeilichen Dateisystemen. § 23a Absatz 3 sieht vor, dass die Kennzeichnung nach einer Übermittlung an eine andere Stelle durch diese aufrechtzuerhalten ist. Durch die allgemeine Kennzeichnungspflicht in § 23 a wird die Pflicht zur (Aufrechterhaltung der) Kennzeichnung (bei Übermittlungen) in einzelnen Befugnissen obsolet.

Absatz 3

Hier ist der Regelungsinhalt des Absatzes 4 in der bisherigen Fassung enthalten. Die Verschiebung und redaktionelle Anpassung an Satz 1 ist durch den Wegfall des Absatzes 3 in der bisherigen Fassung bedingt. Die in Satz 1 in der bisherigen Fassung geregelte Pflicht zur Benachrichtigung ist nun in der zentralen Vorschrift des § 33 Absatz 1 enthalten. Eine Regelung in einzelnen Befugnissen ist damit obsolet. Daher war Satz 1 in der bisherigen Fassung zu streichen. Beim Wegfall von Satz 2 in der bisherigen Fassung handelt es sich um eine Folgeänderung zum Wegfall des § 17 Absatz 5 und 6 in der bisherigen Fassung.

Nr. 8 (§ 17):

Im Zuge der Normierung einer zentralen Vorschrift über Benachrichtigungen in § 33, sind die in den Absätzen 5 und 6 enthaltenen Regelungen zur Unterrichtung obsolet geworden und wurden daher gestrichen.

Absatz 3

Im Zuge des Wegfalls der Regelungen des § 16a Absatz 2 Satz 2 und Satz 3 war auch die Verweisvorschrift des Absatz 3 in der bisherigen Fassung zu streichen. Dies führt zu einer Verschiebung der Nummerierung des nachfolgenden Absatzes. Der Regelungsinhalt des neu gefassten Absatzes 3 entspricht dabei dem des Absatzes 4 in der bisherigen Fassung. Zudem

erfolgt eine redaktionelle Anpassung des Verweises auf die Weiterverarbeitung zu besonderen Zwecken in § 24 Absatz 3 und auf die Berichtigung, Löschung und Einschränkung der Weiterverarbeitung von Daten in § 32 Absatz 3.

Absatz 4

Hier ist der Regelungsinhalt des bisherigen Absatzes 7 unverändert enthalten. Die Neuverortung ist dem Wegfall der Absätze 3, 5 und 6 geschuldet.

Nr. 9 (§ 18):**Absatz 5**

In Satz 4 erfolgt eine redaktionelle Anpassung des Verweises auf die nun in § 24 Absatz 3 geregelte Nutzung personenbezogener Daten zu Zwecken der Aus- und Fortbildung und auf die nun in § 32 Absatz 3 Nummer 1 und 2 geregelten Fälle, in denen die Löschung und Vernichtung unterbleiben können.

Absatz 6

Entspricht, mit einer redaktionellen Anpassung an den Wegfall des § 17 Absatz 5 und 6, dem bisherigen Absatz 7. Absatz 6 in der bisherigen Fassung ist wegen der zentralen Vorschrift des § 23a obsolet geworden und daher entfallen.

Nr. 10 (§ 19):**Absatz 1**

Hier erfolgt eine redaktionelle Anpassung an die Verschiebung des bisherigen Regelungsinhaltes des § 17 Absatz 7 nach Absatz 4 der Vorschrift.

Absatz 2

Mit dem Wegfall des Satz 2 erfolgt eine redaktionelle Anpassung an den Wegfall der in Bezug genommenen Regelungen zur Kennzeichnung des § 16a Absatz 2 Satz 2 und 3.

Absatz 3

Mit dem Wegfall des Absatzes 3 erfolgt eine redaktionelle Anpassung an den Wegfall der in Bezug genommenen Regelungen zur Unterrichtung des § 17 Absatz 5 und 6. Die in der bisherigen Regelung enthaltene Schutzvorschrift für Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist und für verdeckte Ermittler, findet sich nun in der Vorschrift des § 33 Absatz 2 Satz 3.

Nr. 11 (§ 20):**Absatz 4**

Hier erfolgt eine redaktionelle Anpassung an den Wegfall der in Bezug genommenen Regelungen zur Kennzeichnung des § 16a Absatz 2 Satz 2 und 3 der Verschiebung des Inhaltes des § 17 Absatz 7 in der bisherigen Fassung nach § 17 Absatz 4. Absatz 5 der bisherigen Fassung entfällt im Zuge des Wegfalls der Regelungen zur Unterrichtung in § 17 Absatz 5 und 6.

Nr. 12 (§ 20a):**Absatz 4**

Hier ist der Regelungsinhalt des bisherigen Absatzes 5 unverändert enthalten. Die Neuverortung ist dem Wegfall des Absatzes 6 der bisherigen Fassung geschuldet. Mit der Einführung

einer zentralen Vorschrift zu Berichtspflichten an den Landtag in § 68 ist die Regelung entsprechender Berichtspflichten in einzelnen Vorschriften obsolet geworden. Die Berichtspflicht bleibt also über § 68 erhalten.

Absatz 5

Hier ist der Regelungsinhalt des bisherigen Absatzes 7 unverändert enthalten. Die Neuverortung ist dem Wegfall des Absatzes 6 der bisherigen Fassung geschuldet.

Nr. 13 (§ 20b):

In Satz 4 erfolgt eine redaktionelle Anpassung an die Streichung der Berichtspflicht an den Landtag in § 20a Absatz 6 der bisherigen Fassung und an die dadurch bedingte Neuverortung des Absatzes 5 der bisherigen Fassung in § 20a Absatz 4.

Nr. 14 (§ 20c):

Absatz 8

In Satz 5 erfolgt ein Verweis auf die nunmehr in § 33 c geregelte Datenschutzkontrolle. In Satz 6 erfolgt eine redaktionelle Anpassung der bisherigen Unterrichtung an die zentrale Regelung zu Benachrichtigungen in § 33.

Absatz 9

Mit dem Wegfall des Absatzes 9 der bisherigen Fassung erfolgt eine redaktionelle Anpassung an den Wegfall der in Bezug genommenen Regelungen zur Unterrichtung des § 17 Absatz 5 und 6. Der Regelungsinhalt des bisherigen Absatzes 10 ist in veränderter Form nun im neuen Absatz 9 enthalten. Im Zuge der Einführung der zentralen Vorschrift zu Protokollierungen in § 33b sind hier nur noch über § 33 b hinaus gehende Protokollierungspflichten enthalten. Die übrigen Voraussetzungen ergeben sich nunmehr direkt aus § 33 b, auf den die Vorschrift verweist.

Nr. 15 (§ 21):

Mit dem Wegfall des Absatzes 4 der bisherigen Fassung erfolgt eine redaktionelle Anpassung an den Wegfall der in Bezug genommenen Regelungen zur Unterrichtung des § 17 Absatz 5 und 6 und zur Kennzeichnung von Daten in § 16a Absatz 2 Satz 2 und 3 der bisherigen Fassung.

Nr. 16 (Zweiter Titel Weiterverarbeitung von personenbezogenen Daten):

Allgemeines

Der Titel war neu zu fassen, da die Begriffe der Datenspeicherung, Datenveränderung und Datennutzung nunmehr einheitlich unter den Begriff der Verarbeitung im Sinne des Art. 3 Nummer 2 (umgesetzt durch § 36 Nummer 2 DSG NRW-Neu) fallen. Der Begriff der Verarbeitung in diesem Sinne umfasst jedoch auch die Erhebungsebene. Die Übernahme des Begriffs der Verarbeitung ist im PolG NRW indes nicht möglich, da dieses durch die Normierung einzelner Befugnisnormen einerseits und allgemeiner Regeln zur weiteren Verarbeitung der Daten andererseits, strukturell zwischen der Erhebungsebene und der nachfolgenden Verarbeitung unterscheidet. An dieser Stelle wurde daher der Begriff der Weiterverarbeitung gewählt, der alle Verarbeitungsvorgänge i.S.d. § 36 Nummer 2 DSG NRW-Neu, mit Ausnahme des Erhebens, umfasst. Für die Übermittlung personenbezogener Daten gelten weiterhin die speziellen Vorschriften des Dritten Titels.

Nr. 17 (§ 22):**Absatz 1**

Absatz 1 entspricht dem aktuellen § 24 Absatz 1. Der Begriff des Dateisystems entstammt § 36 Nummer 7 des Datenschutzgesetzes NRW.

Absatz 2

Satz 1 bis 3 entspricht § 22 Satz 1bis 3der bisherigen Fassung. Die Sätze 4 und 5 entsprechen § 24 Absatz 2 Satz 3 und 4 in der bisherigen Fassung. Die Einfügung des Satz 6 dient dazu, den Fristbeginn zu in den Sätzen 2 und 3 festgelegten Fristen auf alle zu einer Person gespeicherten Daten einheitlich anzuwenden. Dies folgt vergleichbaren Regelungen in der Strafprozessordnung (§ 489 Absatz 6 StPO) und den Polizeigesetzen einzelner Länder (z.B. Art. 38 Absatz 2 Satz 6 des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei, § 33 Absatz 6 Satz 2 Polizei- und Ordnungsbehördengesetz des Landes Rheinland-Pfalz und § 27 Absatz 4 Satz 4 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung). So soll verhindert werden, dass innerhalb der Frist zu einer Person hinzugespeicherte Daten aufgrund unterschiedlicher Fristabläufe ausgesondert werden müssen und so die polizeifachlich erforderliche Abbildung der Entwicklung einer betroffenen Person in kriminalistischer Hinsicht über aussagekräftige Zeiträume hinweg erschwert wird. Satz 7 sichert die Einhaltung der in den Sätzen 2 und 3 genannten Fristen durch die Vorgabe technischer oder organisatorischer Regelungen.

Absatz 3

Absatz 3 regelt die Besonderheiten im Falle eines Freispruchs sowie im Falle eines Restverdachts einer Straftat (BVerfG NJW 2022, 3231).

Absatz 4

Absatz 4 entspricht dem aktuellen § 22 Satz 5. Der Begriff des Dateisystems entstammt § 36 Nummer 7 DSG NRW-Neu.

Absatz 5

Absatz 5 entspricht dem bisherigen § 24 Absatz 4. Die Sätze 2 und 3 werden lediglich hinsichtlich des neuen Begriffes der Weiterverarbeitung von Daten redaktionell angepasst.

Absatz 6

entspricht dem bisherigen § 23 Absatz 2.

Nr. 18 (§ 22a):

Die Vorschrift konkretisiert die Vorgaben des § 45 i. V. m. § 16 DSG NRW-Neu für die Weiterverarbeitung sog. besonderer Kategorien personenbezogener Daten für die polizeiliche Aufgabenerfüllung. Besondere Kategorien von Daten sind beispielsweise Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten und Daten zum Sexualleben oder zur sexuellen Orientierung. Nach Art. 10 der JI-Richtlinie (umgesetzt in § 42 DSG NRW-Neu) muss die Verarbeitung besonderer Kategorien von Daten unbedingt erforderlich sein. Dies ist anzunehmen, wenn keine zumutbaren Alternativ- und Ausgleichsmaßnahmen zur Verfügung stehen, um das angestrebte Ziel zu erreichen und wenn die Aufgabenerfüllung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist.

Nr. 19 (§ 22b):

§ 22b regelt die Kennzeichnungspflicht bei der Speicherung in polizeilichen Datensystemen. Es handelt sich dabei um eine technisch-organisatorische Folgeregulierung aufgrund der Einführung der hypothetischen Datenneuerhebung. Damit werden auch die Vorgaben aus § 29 Absatz 4 BKAG-Neu umgesetzt. Diese Norm gibt den Verbundteilnehmern des polizeilichen Informationsverbundes beim BKA vor, eine Speicherung personenbezogener Daten nur unter Beachtung der Kennzeichnungsregelungen aus § 14 BKAG-Neu (als Ausfluss der hypothetischen Datenneuerhebung) vornehmen zu dürfen. Wegen der grundsätzlichen datenschutzrechtlichen Bedeutung der hypothetischen Datenneuerhebung ist eine Implementierung auch in den darüber hinausgehenden weiteren polizeilichen Anwendungen angezeigt.

Absatz 4 wurde für die Fälle technischer Unmöglichkeit oder des unverhältnismäßigen Aufwandes weitere Ausnahmen von der Kennzeichnungspflicht getroffen. Er gilt ausschließlich für besondere Einzelfälle.

Absatz 5 beinhaltet eine Übergangsvorschrift zur Weiterverarbeitung oder Übermittlung personenbezogener Daten auch ohne eine Kennzeichnung zum Stichtag des 23. Mai 2018, dem Tag vor Inkrafttreten des neuen Datenschutzgesetzes Nordrhein-Westfalen.

Nr. 20 (§ 23):**Allgemeines**

Mit § 23 wird der Grundsatz der hypothetischen Datenneuerhebung (abgekürzt hyDaNe) aus dem Urteil des BVerfG vom 20. April 2016 (s.o.) im PolG NRW verankert. Danach richten sich die Anforderungen an die Weiterverarbeitung zu anderen Zwecken als dem Erhebungszweck nach den Grundsätzen der Zweckbindung und -änderung, wobei sich die Reichweite der Zweckbindung nach der jeweiligen Ermächtigungsnorm für die Datenerhebung richtet. Die Verhältnismäßigkeitsanforderungen für eine Zweckänderung haben sich am Grundsatz der hypothetischen Datenneuerhebung zu orientieren. Hierbei bemisst sich das Gewicht, das einer solchen Regelung im Rahmen der Abwägung zukommt, am Gewicht des Eingriffs der Datenerhebung. Das bedeutet, dass Informationen, die durch besonders eingriffsintensive Maßnahmen erlangt wurden, auch nur zu besonders gewichtigen Zwecken benutzt werden. Die neue Nutzung der Daten muss dem Schutz von Rechtsgütern eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen können (vgl. BVerfG a.a.O., Rz. 287f. m.w.N.).

In Anlehnung an die Parallelvorschrift des § 12 BKAG-Neu wird in Absatz 1 die weitere Nutzung innerhalb derselben Zwecke und in Absatz 2 die zweckändernde Nutzung geregelt. Um einen Gleichlauf mit § 12 Absatz 2 BKAG-Neu zu gewährleisten, wird die hypothetische Datenneuerhebung in § 23 Absatz 2 als allgemeiner Grundsatz formuliert, der bei jeder Datenverarbeitung zu beachten ist auch wenn sich das BVerfG in o.g. Urteil nur mit (besonders) eingriffsintensiven und verdeckten Maßnahmen auseinandergesetzt hat.

Absatz 1

Absatz 1 regelt die Verarbeitung von personenbezogenen Daten zur Erfüllung derselben Aufgabe und zum Schutz derselben Rechtsgüter oder sonstigen Rechte oder zur auf dieselben Straftaten bezogenen Gefahrenabwehr. Dabei handelt es sich um Datennutzungen über das der Datenerhebung zu Grunde liegende Verfahren hinaus, die sich im Rahmen der ursprünglichen Zwecke halten und durch dieselbe Behörde durchgeführt werden. Das BVerfG hat in seinem o.g. Urteil vom 20. April 2016 (siehe oben Fn. 6; Rz. 278ff.) klargestellt, dass solche Datennutzungen als weitere Nutzungen zulässig sind und nicht dem Grundsatz der hypothetischen Datenneuerhebung unterliegen.

Satz 2 regelt die entsprechende Anwendung von Satz 1 für personenbezogene Daten, denen keine Erhebung vorausgegangen ist - dazu gehören beispielsweise auch unaufgefordert durch Dritte erlangte Daten. Danach soll Satz 1 mit der Maßgabe gelten, dass aufgrund der fehlenden Datenerhebungsvorschrift für die Bestimmung derselben Aufgabe und derselben Rechtsgüter etc. der Zweck der Verarbeitung heranzuziehen ist. Diese Systematik folgt dem bisherigen Verständnis bei der Behandlung solcher Daten.

Absatz 2

Absatz 2 setzt die Vorgaben des BVerfG in seinem o.g. Urteil vom 20. April 2016 an die zweckändernde Verarbeitung von personenbezogenen Daten um und führt damit den Grundsatz der hypothetischen Datenenerhebung in das PoIG NRW ein.

Zu Satz 2 siehe Begründung zu Absatz 1 Satz 2.

Absatz 3

Die Regelung sieht ebenso wie § 12 Absatz 4 BKAG-Neu vor, dass die Vorgaben zu Zweckbindung und der Grundsatz der hypothetischen Datenenerhebung nicht gelten, wenn Grunddaten zwecks Identifizierung einer Person erhoben werden. Hierbei handelt es sich um folgende Daten:

- Familiennamen
- Vornamen
- Geschlecht
- Geburtsnamen
- Geburtsdatum
- Geburtsort einschließlich des Geburtsstaates
- Wohnanschrift
- derzeitige Staatsangehörigkeit und frühere Staatsangehörigkeiten.

Für eine derartige Ausnahme besteht evident ein hohes polizeifachliches Erfordernis. Im Übrigen wird auf die Begründung zur Parallelvorschrift des § 12 Absatz 4 BKAG-Neu (BT-Drs. 18/11163, S. 95) verwiesen. Hier heißt es u.a.: „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“.

Absatz 4

Der Absatz enthält eine Sonderregelung für Daten, die ausschließlich zum Zwecke der Vorgangsverwaltung oder zur zeitlich befristeten Dokumentation (bspw. für einen Untersuchungsausschuss des Landtags NRW) erhoben worden sind. Mit der Regelung wird klargestellt, dass es sich in diesen Fällen nicht um zweckändernde Weiterverarbeitungen im Sinne des § 23 Absatz 2 handelt.

Absatz 5

Mit der Regelung soll die Beachtung der Absätze 1 bis 4 durch organisatorische und technische Maßnahmen nach dem Vorbild des § 12 Abs. 5 BKAG-Neu sichergestellt werden.

Absatz 6

Absatz 6 entspricht inhaltlich dem bisherigen § 24 Absatz 2 Satz 1 und 2. Er wurde lediglich hinsichtlich des neuen Begriffes der Weiterverarbeitung von Daten redaktionell angepasst.

Nr. 21 (§ 24):

§ 24 Absätze 1 bis 3 enthalten die bisherigen Regelungen des § 24 Absatz 5 -bis 7 (Weiterverarbeitung zu besonderen Zwecken). Absatz 1 wurde um einen Hinweis auf § 22a ergänzt (z.B. Stimmauswertung).

Nr. 22 (§ 24a):

Bisher war die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken Stellen bis auf eine Regelung in Bezug auf die Löschung (§ 32 Absatz 5 Satz 1 Nummer 3) hauptsächlich in § 28 DSG NRW-Neu geregelt. Nunmehr erfolgt eine zentrale Regelung im Sinne der § 17 und § 40 DSG NRW-Neu. Es bedarf aber einer Präzisierung/Einschränkung der allgemeinen Vorgaben, welche u.a. durch die Bezugnahme auf die polizeiliche Eigenforschung und Evaluierung erfolgt.

Allgemeines

Das BVerfG hat in seinem o.g. Urteil vom 20. April 2016 ausgeführt, dass sich auch die Anforderungen an die Übermittlung staatlich erhobener Daten an den Grundsätzen der Zweckbindung und Zweckänderung ausrichten und damit dem Grundsatz der hypothetischen Datenneuerhebung unterliegen. Dieser wurde nun in den Übermittlungsvorschriften verankert. Die bisher in den §§ 27 und 29 getrennt geregelten Übermittlungen zwischen Polizeibehörden und Übermittlungen an Personen oder Stellen außerhalb des öffentlichen Bereiches wurden aus systematischen Gründen nun einheitlich als Übermittlungen im innerstaatlichen Bereich in § 27 geregelt. Die bisher nicht explizit geregelten Datenübermittlungen im Bereich der Europäischen Union und deren Mitgliedstaaten sind nun in § 28 verankert. Inhaltlich wurden die bestehenden Übermittlungsvorschriften mit Ausnahme der Einführung des Grundsatzes der hypothetischen Datenneuerhebung weitestgehend erhalten. Die Neuverortung und entsprechende Neubezeichnung der Vorschriften gewährt die Übersichtlichkeit des Abschnitts und macht die Unterteilung durch weitere Aufzählungszeichen innerhalb des Abschnitts obsolet. Die bestehende Unterteilung in die Abschnitte I. bis III. wurde daher aufgehoben.

Nr. 23 (§ 26):

§ 26 regelt grundsätzliche Vorgaben der Datenübermittlung. Die speziellen Voraussetzungen zur Datenübermittlungen im innerstaatlichen Bereich, auf EU-Ebene und im internationalen Bereich finden sich nunmehr in den §§ 27-29.

Absatz 1

In Satz 1 wird der vom BVerfG in seinem Urteil vom 20. April 2016 (siehe oben Fn. 6) aufgestellte Grundsatz der hypothetischen Datenneuerhebung wie von Gericht gefordert (s. BVerfG a.a.O., Rz. 307ff.) auch im Hinblick auf die Datenübermittlung (Rn. 307 ff.) umgesetzt. Satz 2 entspricht dem aktuellen § 26 Absatz 1 Satz 3.

Absatz 2

Absatz 2 entspricht dem bisherigen § 26 Absatz 3.

Absatz 3

In Abs. 3 wird in Anlehnung an § 4 Absatz 2 Satz 2 DSG NRW-Neu 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. Wie auch im Bereich des § 2 Absatz 2 DSG-NRW-Neu, gilt die Vorschrift auch hier unterschiedslos für alle Daten, unabhängig davon, ob sie aus Akten oder anderen Dateisystemen stammen.

Absatz 4

Den Verweis auf § 54 Absatz 2 Satz 2 DSGVO NRW-Neu stellt klar, dass die Polizeibehörden verpflichtet sind, den Empfänger im Falle unrichtiger oder unrechtmäßig übermittelter Daten zu unterrichten.

Absatz 5

In Satz 2 wird ein Übermittlungsverbot eingeführt. Das Verbot gilt als allgemeine Vorschrift für sämtliche Übermittlungen nach den §§ 27 bis 29.

Absatz 6

Die Vorschrift enthält spezielle Übermittlungs- und Verweigerungsgründe für eine Datenübermittlung nach den §§ 27 - 29. Die genannten Gründe sind als Prüfungsmaßstab für Datenübermittlungen an Stellen in Mitgliedstaaten der Europäischen Union und an Stellen im internationalen Ausland zugrunde zu legen. Unter Bezugnahme auf die diesbezüglichen Ausführungen des BVerfG in seinem Urteil vom 20. April 2016 (Rz. 328), wird die Besorgnis einer Verletzung von elementaren Rechtsgrundsätzen und Menschenrechten als Beispiel in Nr. 4 aufgenommen.

Absatz 7

Satz 1 entspricht dem bisherigen § 26 Absatz 4 Satz 1. In Satz 2 erster Halbsatz wird 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. Satz 2 zweiter Halbsatz und Satz 3 macht die zweckändernde Nutzung von Daten, die aus Maßnahmen nach § 18 stammen, von der ausdrücklichen Zustimmung der übermittelnden Stelle abhängig. So wird der Tatsache Rechnung getragen, dass das BVerfG Maßnahmen der Wohnraumüberwachung als besonders eingriffsintensiv bewertet (vgl. BVerfG a.a.O Rz. 105). Satz 3 statuiert eine Hinweispflicht für das Zustimmungsbedürfnis auch bei Datenübermittlungen nach den §§ 28 und 29.

Absatz 8

Die Regelung stellt klar, dass besondere Übermittlungsregelungen beispielsweise im Bereich von Sicherheits- und Zuverlässigkeitsüberprüfungen über OSIP und der Schnittstelle SIPOL unberührt bleiben.

Nr. 24 (§ 27):

Die Vorschrift regelt die Datenübermittlung im innerstaatlichen Bereich. Absatz 1 entspricht dem bisherigen § 27 Absatz 1 und wurde hinsichtlich der neuen Systematik, die keine Sonderregelungen für Datenübermittlungen zwischen Polizeibehörden vorsieht, angepasst. Die Absätze 2 und 3 fassen die Übermittlungsregelungen der bisherigen §§ 28 Absatz 2 und 3, 29 Absatz 1 und 2 zusammen und verzichten auf eine Unterscheidung hinsichtlich einer Übermittlung auf Veranlassung der Polizei bzw. auf Ersuchen einer anderen Stelle nach Absatz 2 und 3.

Die bisher in § 27 Absatz 2 enthaltene Verordnungsermächtigung wird gestrichen, da nach der Neufassung der §§ 28 und 29 hierfür kein praktischer Anwendungsbereich mehr besteht.

Nr. 25 - § 28 - § 29:**§ 28**

Die Vorschrift regelt die Datenübermittlung im Bereich der Europäischen Union und deren Mitgliedsstaaten und stellt sie innerstaatlichen Übermittlungen gleich. Durch den Verweis auf § 27 gilt der Grundsatz der hypothetischen Datenneuerhebung auch für die innereuropäische

Datenübermittlung. Durch Regelung in einer Einzelsvorschrift wird der hohen Bedeutung eines effektiven Informationsaustausches zwischen Sicherheitsbehörden der Mitgliedstaaten der Europäischen Union Rechnung getragen. Eine intensive grenzübergreifende Zusammenarbeit der europäischen Sicherheitsbehörden insbesondere bei der Abwehr von Gefahren des internationalen Terrorismus stellt eine herausragend wichtige Voraussetzung für die europaweite Verhinderung terroristischer Anschläge und Straftaten dar. Ebenso wie im BKAG-Neu, werden daher auch im PolG NRW Datenübermittlungen ins europäische Ausland innerstaatlichen Datenübermittlungen gleichgestellt.

§ 29

Die Absätze 1 und 2 konkretisieren die Vorgaben der §§ 62 - 65 DSGVO NRW-Neu für Datenübermittlungen an Drittstaaten und an internationale Organisationen. In Satz 3 wird zusätzlich zu § 26 Abs. 1 auf das Erfordernis des Vorliegens der Voraussetzungen der sog. hypothetischen Datenneuerhebung im jeweiligen Einzelfall gemäß § 23 hingewiesen, insbesondere der dortige Absatz 2, der für die Datenübermittlung an eine andere Stelle einschlägig ist. Satz 4 verweist auf bi- oder internationale Vereinbarungen, die im Bereich der Datenübermittlung unberührt bleiben.

Absatz 2 regelt den für die datenschutzrechtliche Kontrolle notwendigen Übermittlungsnachweis und die dazugehörige Aussonderungsregelung.

Nr. 26 (§ 30):

Absatz 1 und 2 entsprechen dem bisherigen § 30 Absatz 1 und 2.

Absatz 3 wurde aufgrund der neuen Systematik redaktionell und inhaltlich angepasst.

Nr. 27 - § 32 - § 33:

§ 32

Allgemeines

Das Datenschutzgesetz Nordrhein-Westfalen führt in § 36 Nummer 3 den neuen Begriff der „Einschränkung der Weiterverarbeitung“ ein, welcher das bisherige Konzept der „Sperrung von Daten“ im Sinne des § 3 Absatz 2 Nummer 5 des bisherigen Datenschutzgesetzes Nordrhein-Westfalen sprachlich ersetzt. Dementsprechend wurde der Titel der Vorschrift angepasst und das Instrument des Sperrvermerks durch einen der Einschränkung der Verarbeitung entsprechenden Vermerk ersetzt. Da der gesamte Anwendungsbereich der Vorschrift vom Datenschutzgesetz Nordrhein-Westfalen abgedeckt wird, mussten Bezüge zu den einschlägigen Vorschriften der §§ 50 und 54 DSGVO NRW-Neu hergestellt werden. Dabei wurde der Inhalt der Vorschrift in der bisherigen Fassung im Wesentlichen beibehalten und durch Verweise auf das DSGVO NRW-Neu ergänzt.

Absatz 1

Die Vorschrift beinhaltet die Grundverweismorm auf die Vorschriften der §§ 50, 54 DSGVO NRW-Neu zur Berichtigung, Löschung sowie Einschränkung der Weiterverarbeitung personenbezogener Daten und enthält darüber hinausgehende Fälle der Löschung. Darüber hinaus werden die Voraussetzungen der Aktenvernichtung an das Konzept der §§ 50, 54 DSGVO NRW-Neu angepasst.

Satz 3 erfolgt in Anlehnung an den bisherigen § 24 Absatz 2 Satz 5. Neben des hier geregelten Falles des Wegfalls des Straftatverdachtes nach Einleitung eines strafrechtlichen Ermittlungsverfahrens, wurde aus Gründen der Vollständigkeit auch eine Löschpflicht für den Fall des Wegfalls des Straftatverdachtes bei reiner Vorgangsverwaltung aufgenommen.

Absatz 2

Die Vorschrift legt unter Bezug zu § 50 DSGVO NRW-Neu Regeln zum Umgang mit unrichtigen Daten fest.

Absatz 3

Die Vorschrift legt unter Bezug zu § 50 DSGVO NRW-Neu fest, in welchen Fällen Löschung und Vernichtung unterbleiben können. Wegen des Wegfalls des Begriffs des Sperrvermerks siehe Erläuterung unter Allgemeines.

Absatz 4

Hier ist die bisher in Absatz 6 geregelte Pflicht zur Zusammenarbeit mit einem Staatsarchiv in Bezug auf das Landesarchiv Nordrhein-Westfalen konkretisiert worden.

§ 33**Allgemeines**

In der Vorschrift werden die bisher in Einzelbefugnissen vorhandenen Unterrichtungspflichten nach § 17 Absatz 5 und 6 in einer zentralen Vorschrift zusammengeführt und in Umsetzung der diesbezüglichen Vorgaben des BVerfG im Urteil vom 20. April 2016 auf alle verdeckten Maßnahmen ausgedehnt (vgl. BVerfG a.a.O., Rz. 136). Der Begriff der „Unterrichtung“ wird in Einklang mit der Terminologie des BVerfG (a.a.O., Rz. 136) durch den Begriff der „Benachrichtigung“ ersetzt.

Absatz 1

Die Vorschrift zählt die Maßnahmen auf, bei denen eine Benachrichtigung der dort genannten Betroffenen erfolgen muss und ersetzt somit die bisherigen dezentral aufgeführten Unterrichtungspflichten in den Einzelbefugnissen. Bei Maßnahmen nach § 21 umfasst die Pflicht zur Benachrichtigung auch die Tatsache der Löschung. Dies entspricht der Regelung des § 21 Absatz 4 Satz 2 der bisherigen Fassung.

Absatz 2 bis 4

Die Absätze 2 bis 4 beinhalten Ausnahme- und Rückstellungsregelungen für eine Benachrichtigung des Betroffenen. Die entsprechen inhaltlich im Wesentlichen den bisherigen Regelungen des § 17 Absatz 5 und 6. Die endgültige Zurückstellung einer Benachrichtigung nach Absatz 4 Satz 7 und 8 dient einem effektiveren Schutz von V-Personen und Verdeckten Ermittlern i.S.d. §§ 19 und 20.

Absatz 5

Dieser entspricht dem bisherigen § 24 Absatz 3.

Absatz 6

Absatz 6 enthält einen Verweis auf die Vorgaben des § 48 Absatz 1 und Absatz 3 des Datenschutzgesetzes Nordrhein-Westfalen. Außerdem gibt er vor, auf die Möglichkeit nachträglichen Rechtsschutzes hinzuweisen. Schließlich ist die Benachrichtigung in klarer und einfacher Sprache zu formulieren.

Nr. 28 - § 33a - § 33b - § 33c:**§ 33a****Allgemeines**

§ 33a setzt die in Art. 31 der JI-Richtlinie vorgesehene Pflicht zur Benachrichtigung im Fall der Verletzung des Schutzes personenbezogener Daten um.

Absatz 1

Satz 1 konstituiert die grundsätzliche Benachrichtigungspflicht aus § 31 Absatz 1 JI-Richtlinie. Diese ist gegeben, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einer erheblichen Gefahr für Rechtsgüter der betroffenen Personen führt. Als Anwendungshilfe können hier die Gedanken aus Erwägungsgrund 52 der JI-Richtlinie herangezogen werden. Danach sollten Eintrittswahrscheinlichkeit und Schwere des Risikos nach der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein hohes Risiko birgt.

Absatz 2

Hier werden die formalen Anforderungen an die Benachrichtigung aus Art. 31 Absatz 2 i.V.m. Art. 30 Absatz 3 JI-Richtlinie umgesetzt.

Absatz 3

Die Vorschrift setzt die in Art. 31 Absatz 3 vorgesehenen Ausnahmen von der Benachrichtigungspflicht um.

Absatz 4

In Ausnutzung des durch Art. 31 Absatz 5 i.V.m. Art. 13 Absatz 3 JI-Richtlinie eröffneten mitgliedstaatlichen Gestaltungsspielraumes, werden in dieser Vorschrift ergänzend Ausnahmeregelungen von der unverzüglichen Pflicht zur Benachrichtigung getroffen. Um einen Gleichlauf mit dem bereichsübergreifenden Landesdatenschutzrecht zu gewährleisten, werden hierbei die Vorgaben des § 48 Absatz 2 DSGVO NRW-Neu über die allgemeine Benachrichtigung der betroffenen Person berücksichtigt.

Absatz 5

Die Vorschrift setzt das in Art. 31 Absatz 4 der JI-Richtlinie enthaltene Recht der Aufsichtsbehörde (hier: Landesbeauftragter für Datenschutz und Informationsfreiheit) um.

§ 33b

Der an dieser Stelle neu aufgenommene Regelungsinhalt setzt die Anforderungen aus dem o.g. Urteil des BVerfG vom 20. April 2016 an eine Protokollierungspflicht bei verdeckten und sonstigen eingriffsintensiven Maßnahmen (BVerfG a.a.O., Rz. 141) um. Damit wird unabhängig von der Protokollierungsvorschrift aus § 55 DSGVO NRW-Neu eine eigenständige Vorschrift zur Protokollierung geschaffen.

Absatz 1

Abs. 1 konstituiert die Pflicht zur vollständigen Protokollierung bei verdeckten und eingriffsintensiven Maßnahmen. Die aufgezählten Maßnahmen entsprechen dem Maßnahmenkatalog aus § 33 Absatz 1.

Absatz 2

Ergänzend sind bei den in § 33 Absatz 1 genannten Maßnahmen die Daten der dort genannten betroffenen Personen zu protokollieren.

Absatz 3

Nachforschungen zur Feststellung der Identität der in Absatz 1 bezeichneten Personen sind nur vorzunehmen, wenn dies unter Abwägung der Eingriffsintensität der Maßnahme, des Aufwands für die Identitätsfeststellung und der daraus folgenden Beeinträchtigungen für die betroffenen Personen geboten ist. Die Einschränkung der Benachrichtigung wird entsprechend § 33 Absatz 3 Satz 2 und 3 auf die dort genannten Personen beschränkt.

Absatz 4

Die Vorschrift enthält eine Nutzungsbeschränkung der Protokolldaten für Benachrichtigungszwecke sowie Zwecke der Datenschutz- und Rechtmäßigkeitskontrolle.

Absatz 5

Die Vorschrift gibt an, dass § 55 des Datenschutzgesetzes Nordrhein-Westfalen unberührt bleibt.

§ 33c**Allgemeines**

Die Vorgaben des BVerfG zum BKAG (a.a.O., Rz. 141 ff.) sehen für die in § 33 angeführten und in § 33b zu protokollierenden Maßnahmen sowie für Datenübermittlungen gemäß § 29 eine turnusmäßige Kontrolle des/der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW vor. Ergänzend ist durch technische und organisatorische Maßnahmen im Sinne des o. g. Urteils des BVerfG vom 20. April 2016 sicherzustellen, dass die Daten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält. (a.a.O., Rz. 141 ff. i. V. m. Urteil des BVerfG vom 24.04.2013, 1 BvR 1215/07, Rz. 215).

Nr. 29 (§ 34c):

Die Änderung des Absatzes 5 trägt der Tatsache Rechnung, dass die in Bezug genommene Vorschrift des Art. 25 der JI-Richtlinie mittlerweile durch § 55 DSGVO NRW-Neu umgesetzt wurde.

Nr. 30 (§ 68):

Die Vorschrift setzt die Forderung des Urteils des Bundesverfassungsgerichts vom 20. April 2016 (a.a.O., Rz. 142, 143, 268, 340, 354) nach einer Pflicht zur Benachrichtigung des Parlaments und der Öffentlichkeit über verdeckte Überwachungsmaßnahmen um. Die bisher in den §§ 20a Absatz 6 und 20b Satz 5 enthaltenen Berichtspflichten werden hierher überführt.

Zu Artikel 2**Nr. 1 (Inhaltsübersicht):**

Die Änderung der Inhaltsübersicht ist aufgrund der Änderung der Überschrift des § 24 OBG erforderlich.

Nr. 2 (§ 24):

Die Überschrift des § 24 OBG wird aufgrund der Anpassung an die europäische Datenschutzreform und des neu hinzugekommenen Absatzes 2 geändert. Der Gesetzestext wurde in zwei Absätze unterteilt. Die Verweisung auf § 9 Abs. 1 PolG NRW entfällt.

Absatz 1**Nummer 1**

Die Verweisung auf § 9 Abs. 1 PolG NRW entfällt. Die Rechtmäßigkeit der Datenverarbeitung im Rahmen der Erfüllung der Aufgaben nach dem OBG richtet sich nach Art. 6 DSGVO und ergänzend nach § 3 DSGVO NRW-Neu. Die Einwilligung als zulässige Rechtsgrundlage für die Datenerhebung ist im Art. 6 Abs. 1 a) und Art. 7 DSGVO ausdrücklich geregelt. Die Erhebung besonderer Kategorien personenbezogener Daten ist unmittelbar geregelt im Art. 9 DSGVO und ergänzend im § 16 DSGVO NRW-Neu.

Nummer 6

Die Verweisung auf § 15 Abs. 2 PolG NRW entfällt. Der neu gefasste § 15 Abs. 2 PolG NRW verweist auf die Regelungen des § 24 und des § 32 PolG NRW. Eine Verweisung auf § 24 PolG NRW für die Ordnungsbehörden findet nicht statt, da entsprechende Regelungen im Art. 89 DSGVO und ergänzend in § 9 und § 17 DSG NRW-Neu bereits enthalten sind. Ebenso findet eine Verweisung auf den neugefassten § 32 PolG NRW nicht statt, da die Berichtigung, Löschung und Einschränkung der Weiterverarbeitung von Daten im Art. 16 DSGVO Recht auf Berichtigung, Art. 17 DSGVO Recht auf Löschung und Art. 18 DSGVO Recht auf Einschränkung der Verarbeitung sowie ergänzend im § 10 DSG NRW-Neu Löschung personenbezogener Daten geregelt ist.

Nummer 7

Der neugefasste § 22 PolG NRW trifft Regelungen zur Datenspeicherung und zur Festlegung von Prüfungsterminen. Eine Verweisung entfällt soweit die Regelungen straftatenbezogen sind.

Die Verweisung auf den neugefassten § 23 PolG NRW erfolgt nunmehr in § 24 Abs. 1 Nr. 8.

Nummer 8

Nach dem Erwägungsgrund 50 der DSGVO ist die Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, zulässig, wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, so können im Unionsrecht oder im Recht der Mitgliedstaaten die Aufgaben und Zwecke bestimmt und konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird. Im neugefassten § 23 PolG NRW werden fachspezifische Rahmenbedingungen für die Weiterverarbeitung von personenbezogenen Daten und für die Zweckänderung gesetzt. Es handelt sich hierbei um eine ergänzende spezialgesetzliche Regelung zum Art. 6 Abs. 4 DSGVO und § 9 DSG NRW-Neu zum Schutz der öffentlichen Sicherheit.

Soweit § 23 PolG NRW die Weiterverarbeitung von personenbezogenen Daten aus dem verdeckten Einsatz technischer Mittel oder aus Wohnungen nach § 18 PolG NRW regelt, entfällt eine Verweisung, da den Ordnungsbehörden die Befugnis zur Datenerhebung durch den verdeckten Einsatz technischer Mittel oder aus Wohnungen nach § 18 PolG NRW nicht zusteht.

Die frühere Verweisung auf § 24 PolG NRW entfällt. Entsprechende Regelungen finden sich unmittelbar im Art. 89 DSGVO sowie im § 9 und § 17 DSG NRW-Neu.

Nummer 9

§ 26 PolG NRW wurde teilweise neu gefasst. Die Verweisung auf § 26 Abs. 1 S. 2 PolG NRW entfällt, mangels Befugnis der Ordnungsbehörden zur Verarbeitung von Daten nach § 22 a Abs. 5 PolG NRW.

Da für die Aufgabenerfüllung nach dem OBG der Teil III des Datenschutzgesetzes NRW nicht anwendbar ist, entfällt die Verweisung auf § 26 Abs. 4 PolG NRW.

Die Verweisung auf § 26 Abs. 6 PolG NRW erfolgt nur eingeschränkt, da die Datenübermittlung an Drittländer oder internationale Organisationen unmittelbar in den Art. 44 ff DSGVO geregelt ist. Auf § 29 PolG NRW wird daher nicht verwiesen.

Im Einklang mit § 9 DSGVO NRW-Neu dürfen die übermittelten personenbezogenen Daten nur für die Zwecke verarbeitet werden, zu denen sie übermittelt wurden. Eine Verweisung auf § 26 Abs. 7 PolG NRW entfällt daher.

Nummer 10

Die Datenübermittlungsvorschriften der §§ 27 und 28 PolG NRW im innerstaatlichen Bereich und im Bereich der Europäischen Union und deren Mitgliedsstaaten stellen eine fachbereichsspezifische Konkretisierung der datenschutzrechtlichen Vorgaben dar. Dabei wurden § 27 Abs. 2 und Abs. 3 PolG NRW neu gefasst, was eine uneingeschränkte Verweisung erlaubt.

Die Verweisung auf § 28 PolG NRW war früher im § 24 Abs. 1 Nr. 11 OBG geregelt. Insofern handelt es sich hier um eine redaktionelle Änderung.

Nummer 11

Eine Verweisung auf den § 30 PolG NRW erfolgt, soweit dieser Ersuchen auf Übermittlung personenbezogener Daten regelt. Eine Verweisung auf § 30 Abs. 3 Satz 2 PolG NRW, der die Übermittlung von Daten an Drittstaaten betrifft, unterbleibt. Die Datenübermittlung durch die Ordnungsbehörden an Drittländer oder internationale Organisationen richtet sich unmittelbar nach Kapitel V, Art. 44 ff DSGVO. Auf § 30 Abs. 3 Satz 2 PolG NRW und die Regelungen zur Übermittlung von Daten an Drittstaaten im § 29 PolG NRW wird daher nicht verwiesen.

Nummer 12

Es handelt sich um eine redaktionelle Folgeänderung. Die Verweisung war früher im § 24 Abs. 1 Nr. 13 OBG geregelt.

Zum Wegfall der Verweisung auf den neugefassten § 32 PolG NRW s. oben Begründung zu § 24 Abs. 1 Nr. 6 OBG.

Absatz 2

Die Regelung erfolgt zur Anpassung an die ab dem 25. Mai 2018 unmittelbar geltende DSGVO und das novellierte DSGVO NRW-Neu. Mit Anwendbarkeit der DSGVO unmittelbar im nationalen Recht gilt der Vorrang der DSGVO gegenüber dem nationalen Recht. Das DSGVO NRW-Neu und die fachbereichsspezifischen Regelungen zum Datenschutz im PolG NRW ergänzen und konkretisieren fachbereichsspezifisch die Regelungen DSGVO.

Zu Artikel 3

Die einzuführenden Änderungen ermöglichen Maßnahmen, durch die das Grundrecht Recht auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 des Grundgesetzes) eingeschränkt werden können.

Daher ist durch diese Regelung dem Zitiergebot Rechnung zu tragen.

Zu Artikel 4

Die Vorschrift regelt das In-Kraft-Treten.