Referentenentwurf

Gesetz
zur Änderung polizeirechtlicher Vorschriften

Vom …

Der Sächsische Landtag hat am … das folgende Gesetz beschlossen:

Inhaltsübersicht

Artikel 1 Änderung des Sächsischen Polizeivollzugsdienstgesetzes

Artikel 2 Änderung des Sächsischen Polizeibehördengesetzes

Artikel 3 Änderung des Sächsischen Kontrollgesetzes

Artikel 4 Änderung des Sächsischen Gesetzes zur Regelung polizeilicher Zuverlässigkeitsüberprüfungen

Artikel 5 Folgeänderung im Sächsischen Besoldungsgesetz

Artikel 6 Folgeänderung im Sächsischen Verwaltungsorganisationsgesetz

Artikel 7 Folgeänderung im Sächsischen Personalvertretungsgesetz

Artikel 8 Folgeänderungen im Sächsischen Straßenverkehrsrechtsgesetz

Artikel 9 Folgeänderungen in der Sächsischen Polizeiorganisationsverordnung

Artikel 10 Folgeänderung in der Sächsischen Waffengesetzdurchführungsverordnung

Artikel 11 Folgeänderung in der Sächsischen Vertretungsverordnung

Artikel 12 Folgeänderungen in der Sächsischen Heilfürsorgeverordnung

Artikel 13 Folgeänderungen in der Sächsischen Straßenverkehrsrechtsverordnung

Artikel 14 Inkrafttreten

Artikel 1

Änderung des Sächsischen Polizeivollzugsdienstgesetzes

Das Sächsische Polizeivollzugsdienstgesetz vom 11. Mai 2019 (SächsGVBl. S. 358), das durch das Gesetz vom 5. Juli 2024 (SächsGVBl. S. 595) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angabe zu § 3 wird durch die folgende Angabe ersetzt:

      „§ 3 Tätigwerden der Polizei für die Polizeibehörden oder andere Stellen“.

b) Nach der Angabe zu § 12 wird folgende Angabe eingefügt:

„§ 12a Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme“.

c) Die Angabe zu § 19 wird durch die folgende Angabe ersetzt:

„§ 19 Maßnahmen zum Schutz vor häuslicher Gewalt und sonstigen Nachstellungen“.

d) Nach der Angabe zu § 57 wird folgende Angabe eingefügt:

„§ 57a Anwendungen zur automatisierten Verarbeitung von an öffentlichen Orten und besonders gefährdeten öffentlichen Einrichtungen offen erhobenen personenbezogenen Daten“.

e) Die Angabe zu § 59 wird durch die folgende Angabe ersetzt:

„§ 59 (weggefallen)“.

f) Die Angabe zu § 60 wird durch die folgende Angabe ersetzt:

„§ 60 Ausschreibung von Personen und Sachen“.

g) Nach der Angabe zu § 62 wird die folgende Angabe eingefügt:

„§ 62a Anlassbezogene Anwendung zur automatisierten Datenanalyse

§ 62b Anlassbezogener nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet“.

h) Nach der Angabe zu § 64 wird folgende Angabe eingefügt:

„§ 64 Einsatz einer V-Person, Verdeckte Ermitterin und Verdeckter Ermittler“.

i) Nach der Angabe zu § 66 wird folgende Angabe eingefügt:

„§ 66a Unterbrechung oder Verhinderung der Telekommunikation“.

j) Die Angabe zu § 69 wird durch folgende Angabe ersetzt:

„§ 69 (weggefallen)“.

k) Die Angabe zu § 71 wird durch folgende Angabe ersetzt:

„§ 71 Einsatz von unbemannten Luftfahrtsystemen“.

l) Die Angabe zu § 72 wird durch die folgende Angabe ersetzt:

„§ 72 (weggefallen)“.

m) Die Angabe zu § 79 wird durch folgende Angabe ersetzt:

„§ 79 Befugnis zur Datenverarbeitung“.

n) Nach der Angabe zu § 79 wird folgende Angabe eingefügt:

„§ 79a Zweckbindung, Zweckänderung, Hypothetische Datenneuerhebung

§ 79b Weiterverarbeitung zu Aus- und Fortbildungszwecken, zu statistischen, archivarischen oder wissenschaftlichen Zwecken, Weiterverarbeitung von Vorgangsverwaltungs- und Protokolldaten

§ 79c Training und Test von lernenden IT-Systemen“.

o) Die Angabe zu § 80 wird durch folgende Angabe ersetzt:

„§ 80 Vorsorgende Speicherung von personenbezogenen Daten zu Verurteilten, Beschuldigten, Verdächtigen und Anlasspersonen“.

p) Nach der Angabe zu § 80 wird die folgende Angabe eingefügt:

„§ 80a Vorsorgende Speicherung von personenbezogenen Daten zu Zeuginnen und Zeugen, Opfern, Hinweisgeberinnen und -gebern, Kontakt- und Begleitpersonen

§ 80b Vorsorgende Speicherung von zu Gefahrenabwehrzwecken erhobenen Daten

§ 80c Vorsorgende Speicherung von personenbezogenen Daten zu sonstigen Personen

§ 80d Dauer der Speicherung, Aussonderungsprüffristen, Höchstspeicherfristen“.

q) Nach der Angabe zu § 84 wird folgende Angabe eingefügt:

„§ 84a Öffentlichkeitsfahndung“.

r) Die Angabe zu § 88 wird durch folgende Angabe ersetzt:

„§ 88 Zuverlässigkeitsüberprüfung zum Schutz von besonders gefährdeten Veranstaltungen“.

s) Nach der Angabe zu § 106 wird folgende Angabe eingefügt:

„§ 106a Ordnungswidrigkeiten“.

2. § 3 wird durch folgenden § 3 ersetzt:

„§ 3

Tätigwerden der Polizei für die Polizeibehörden oder andere Stellen

Wird die Polizei gemäß § 2 Absatz 3 tätig, trifft sie die erforderlichen Maßnahmen in eigener Zuständigkeit. Ist zur Wahrnehmung einer polizeilichen Aufgabe im Sinne des § 2 Absatz 1 nach gesetzlicher Vorschrift eine andere Stelle zuständig und erscheint deren rechtzeitiges Tätigwerden bei Gefahr im Verzug nicht erreichbar, hat die Polizei die notwendigen vorläufigen Maßnahmen zu treffen. Die zuständige Stelle ist unverzüglich zu unterrichten.“

3. § 4 Nummer 5 bis 8 wird durch folgende Nummern 5 bis 9 ersetzt:

„5. terroristische Straftat: die in § 129a Absatz 1 und 2 Nummer 2 bis 5 des Strafgesetzbuches bezeichneten Straftaten, sofern die Begehung der Straftat dazu bestimmt ist,

a) die Bevölkerung auf erhebliche Weise einzuschüchtern,

b) eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder

c) die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates, eines Landes oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen;

die Straftat muss durch die Art ihrer Begehung oder durch ihre Auswirkungen einen Staat, ein Land oder eine internationale Organisation erheblich schädigen können;

6. Vorfeldstraftat: Straftatbestand, der Verhaltensweisen erfasst, die vom Gesetzgeber als generell gefährlich für Individualrechtsgüter oder Kollektivrechtsgüter bewertet werden, aber als einzelne Handlungen in räumlicher oder zeitlicher Hinsicht noch vor einer konkreten oder konkretisierten Gefährdung oder gar Verletzung solcher Rechtsgüter liegen können und damit strafbewehrte Vorbereitungshandlungen darstellen;

7. Ordnungswidrigkeiten von erheblicher Bedeutung: Ordnungswidrigkeiten, bei deren Begehung ein Schaden für ein bedeutsames Rechtsgut, wie Bestand oder Sicherheit des Bundes oder eines Landes, Leben, Gesundheit, Freiheit einer Person oder bedeutende Sach- und Vermögenswerte, zu befürchten ist oder wenn die Vorschrift ein sonst bedeutsames Interesse der Allgemeinheit schützt;

8. Informationssystem: ein Verarbeitungssystem, in dem die Polizei zur Erfüllung von Aufgaben personenbezogene Daten ganz oder teilweise automatisiert verarbeitet oder nicht automatisiert verarbeitet, soweit die Daten in einem Dateisystem gespeichert sind;

9. Kontakt- und Begleitperson: eine Person, die mit einer anderen Person, bei der Tatsachen die Annahme rechtfertigen, dass sie Straftaten von erheblicher Bedeutung begehen wird, nicht nur flüchtig oder in zufälligem Kontakt steht und Tatsachen die Annahme rechtfertigen, dass

   a) sie von der Vorbereitung einer solchen Straftat Kenntnis hat,

   b) sie aus der Tat Vorteile zieht oder

   c) die andere Person sich ihrer zur Begehung der Straftat bedienen könnte.“

4. Nach § 12 wird der folgende § 12a eingefügt:

„§ 12a

Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme

Die Polizei kann zur Abwehr einer Gefahr, die von unbemannten Fahrzeugsystemen ausgeht, die an Land, in der Luft oder zu Wasser betrieben werden, technische Mittel gegen das System, dessen Steuerungseinheit oder Steuerungsverbindung einsetzen, soweit die Abwehr der Gefahr auf andere Weise aussichtslos ist oder wesentlich erschwert wäre. Zur Abwehr der in Satz 1 bezeichneten Gefahren kann die Polizei technische Mittel auch zur Erkennung einer Gefahr einsetzen.“

5. § 15 Absatz 1 Satz 1 Nummer 5 bis 8 wird durch folgende Nummern 5 bis 9 ersetzt:

„5. wenn sie sich in einem Fahrzeug befindet, das zur gezielten Kontrolle ausgeschrieben ist und tatsächliche Anhaltpunkte dafür vorliegen, dass die Maßnahme zur Abwehr einer Gefahr erforderlich ist;

6. wenn sie an einer Kontrollstelle angetroffen wird, die von der Polizei eingerichtet worden ist, um Straftaten von erheblicher Bedeutung, gemäß § 24 Absatz 1 Nummer 3, Nummer 4 oder Absatz 2 Nummer 4 des Sächsischen Versammlungsgesetzes oder gemäß § 31a des Sächsischen Polizeibehördengesetzes zu verhindern;

7. wenn sie sich innerhalb eines Kontrollbereichs aufhält, der von der Polizei bestimmt worden ist, um Straftaten im Sinne des § 100a der Strafprozessordnung

oder nach § 24 Absatz 1 Nummer 3, Nummer 4 oder Absatz 2 Nummer 4 des Sächsischen Versammlungsgesetzes oder nach § 31a des Sächsischen Polizeibehördengesetzes zu verhindern, da Tatsachen die Annahme rechtfertigen, dass dann dort Straftaten dieser Art bevorstehen; die Bestimmung eines Kontrollbereichs darf längstens für sieben Tage erfolgen sowie bedarf der Zustimmung des Staatsministeriums des Innern und der öffentlichen Bekanntgabe durch die anordnende Dienststelle; die öffentliche Bekanntgabe kann unterbleiben, wenn der Kontrollbereich nicht für länger als 48 Stunden bestimmt wird, sonst die Wahrnehmung der polizeilichen Aufgabe gefährdet wäre und besondere gebietsbezogene Maßnahmen zu dieser Abgrenzung vorgenommen werden;

8. wenn sie sich an Orten aufhält, für die durch Rechtsverordnung nach § 42 des Waffengesetzes das Führen von Waffen im Sinne des § 1 Absatz 2 des Waffengesetzes verboten oder beschränkt worden ist, oder

9. zum Schutz privater Rechte.“

6. § 19 wird durch den folgenden § 19 ersetzt:

„§ 19

Maßnahmen zum Schutz vor häuslicher Gewalt und sonstigen Nachstellungen

(1) Die Polizei kann, soweit es zur Abwehr einer Gefahr für Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer anderen Person, insbesondere in engen sozialen Beziehungen, erforderlich ist,

1. die Person, von der die Gefahr ausgeht, aus einer gemeinsam mit der gefährdeten Person genutzten Wohnung und dem unmittelbar angrenzenden Bereich verweisen und ihr die Rückkehr dorthin untersagen, sowie

2. der Person, von der die Gefahr ausgeht, verbieten,

   a) sich in einem bestimmten Umkreis der Wohnung der betroffenen Person aufzuhalten,

   b) Orte zu betreten, an denen sich die gefährdete Person oder bestimmte ihr nahestehende Personen regelmäßig aufhalten werden,

   c) Verbindung zur gefährdeten Person auch unter Verwendung von Fernkommunikationsmitteln aufzunehmen und

   d) ein Zusammentreffen mit der gefährdeten Person herbeizuführen.

Die Anordnungen sind zu befristen; die Frist kann verlängert werden. Maßnahmen nach Satz 1 enden mit dem Ablauf des 14. Tages nach ihrer Anordnung, soweit nicht die Polizei im Einzelfall eine kürzere Frist festlegt. Stellt die gefährdete Person während der nach Satz 3 bestimmten Dauer der Maßnahmen einen Antrag nach dem Gewaltschutzgesetz, enden die Maßnahmen mit dem Tag der gerichtlichen Entscheidung oder des gerichtlichen Vergleichs, spätestens jedoch mit Ablauf des 14. Kalendertages nach dem Ende der nach Satz 3 bestimmten Dauer.

(2) Die Polizei unterrichtet die gefährdete Person unverzüglich über die Dauer und den Umfang einer Maßnahme nach Absatz 1 sowie über Beratungsangebote und die Möglichkeit, Schutz nach dem Gewaltschutzgesetz zu beantragen.“

7. § 21 wird durch den folgenden § 21 ersetzt:

„§ 21

Aufenthaltsanordnung und Kontaktverbot

(1) Die Polizei kann zum Zweck der Verhütung von Straftaten einer Person untersagen, einen bestimmten Ort, ein bestimmtes Gebiet innerhalb einer Gemeinde oder ein Gemeindegebiet zu betreten oder sich dort aufzuhalten, soweit Tatsachen die Annahme rechtfertigen, dass die Person dort eine Straftat begehen wird (Aufenthaltsverbot). Das Aufenthaltsverbot ist zeitlich und örtlich auf den zur Verhütung der Straftat erforderlichen Umfang zu beschränken und darf räumlich nicht den Zugang zur Wohnung der betroffenen Person oder die Wahrnehmung anderer berechtigter Interessen beschränken. Die Vorschriften des Versammlungsrechts bleiben unberührt.

(2) Die Polizei kann einer Person verbieten, sich ohne Erlaubnis der Polizei von ihrem Wohn- oder Aufenthaltsort oder aus einem bestimmten anderen Bereich zu entfernen (Aufenthaltsgebot) oder sich in bestimmten Bereichen aufzuhalten (Aufenthaltsverbot), wenn

1. Tatsachen die Annahme rechtfertigen, dass die betroffene Person innerhalb absehbarer Zeit eine ihrer Art nach konkretisierte Straftat gegen den Bestand oder die Sicherheit des Bundes oder eines Landes, Leben, Gesundheit oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, begehen wird, oder

2. das Verhalten der betroffenen Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen wird.

Soweit es sich bei der in Satz 1 Nummer 1 oder 2 in Bezug genommenen Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen. Unter den Voraussetzungen der Sätze 1 und 2 kann die Polizei auch den Kontakt mit bestimmten Personen oder Personen einer bestimmten Gruppe untersagen, wenn Tatsachen die Annahme rechtfertigen, dass diese von der Vorbereitung der drohenden Straftat Kenntnis haben, diese aus der Tat Vorteile ziehen werden oder die Person sich ihrer zur Begehung bedienen wird (Kontaktverbot). Anordnungen nach den Sätzen 1 bis 3 sind auf höchstens zwei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als zwei Monate ist zulässig, soweit die Voraussetzungen weiterhin vorliegen. Für Maßnahmen nach Absatz 2 gilt im Übrigen Absatz 1 Satz 2 und 3.

(3) Maßnahmen nach Absatz 2 bedürfen der Anordnung durch das Amtsgericht auf Antrag der Polizei. Die Anordnung ist sofort vollziehbar. Bei Gefahr im Verzug kann die Anordnung durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion oder durch von diesen hierzu beauftragte Bedienstete getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. Die Maßnahme ist zu beenden, wenn die Bestätigung durch das Gericht abgelehnt wird.

(4) Im Antrag nach Absatz 3 Satz 1 sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Name und Anschrift,

2. Art, Umfang und Dauer der Maßnahme sowie

a) im Fall des Aufenthaltsgebots nach Absatz 2 Satz 1 eine Bezeichnung der Bereiche, von denen sich die Person ohne Erlaubnis der zuständigen Polizeidienststelle nicht entfernen, oder im Fall des Aufenthaltsverbots nach Absatz 2 Satz 1 eine Bezeichnung der Bereiche, an denen sich die Person ohne Erlaubnis der zuständigen Polizeidienststelle nicht aufhalten darf, und

b) im Fall des Kontaktverbots nach Absatz 2 Satz 3 eine Bezeichnung der Personen oder der Gruppe, mit denen oder mit der der betroffenen Person der Kontakt untersagt ist, soweit möglich mit Name und Anschrift,

3. der Sachverhalt sowie

4. die Begründung.

(5) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Name und Anschrift,

2. Art, Umfang und Dauer der Maßnahme, sowie

a) im Fall des Aufenthaltsgebots nach Absatz 2 Satz 1 eine Bezeichnung der Bereiche, von denen sich die Person ohne Erlaubnis der zuständigen Polizeidienststelle nicht entfernen, oder im Fall des Aufenthaltsverbots nach Absatz 2 Satz 1 eine Bezeichnung der Bereiche, an denen sich die Person ohne Erlaubnis der zuständigen Polizeidienststelle nicht aufhalten darf, und

b) im Fall des Kontaktverbots nach Absatz 2 Satz 3 eine Bezeichnung der Personen oder der Gruppe, mit denen oder mit der der betroffenen Person der Kontakt untersagt ist, soweit möglich mit Name und Anschrift, sowie

3. die wesentlichen Gründe.

(6) Die Erforderlichkeit, die praktische Anwendung und die Auswirkungen der Maßnahmen nach Absatz 2 werden nach einem Erfahrungszeitraum von drei Jahren, spätestens jedoch zum 31. Dezember 2029, durch die Staatsregierung geprüft. Die Staatsregierung berichtet dem Landtag über das Ergebnis der Evaluierung.“

8. § 28 Nummer 6 und 7 wird durch folgende Nummern 6 bis 8 ersetzt:

„6. es sich um ein Land-, Wasser- oder Luftfahrzeug handelt, in dem sich eine Person befindet, deren Identität nach § 15 Absatz 1 Satz 1 Nummer 4, 6 oder 7 festgestellt werden darf oder die zur gezielten Kontrolle ausgeschrieben ist; die Durchsuchung kann sich auch auf die in diesem Fahrzeug enthaltenen oder mit dem Fahrzeug verbundenen Sachen erstrecken,

7. sie von einer Person mitgeführt wird, deren Identität nach § 15 Absatz 1 Satz 1 Nummer 4, 5, 6 oder 7 festgestellt werden darf, oder

8. es sich um ein Fahrzeug handelt, das zur gezielten Kontrolle ausgeschrieben ist und tatsächliche Anhaltspunkte dafür vorliegen, dass die Durchsuchung zur Abwehr einer Gefahr erforderlich ist“.

9. § 29 Absatz 3 wird durch folgenden Absatz 3 ersetzt:

„(3) Während der Nachtzeit (§ 104 Absatz 3 der Strafprozessordnung) darf eine Wohnung nur in den Fällen des Absatzes 1 Satz 1 Nummer 2 betreten und durchsucht werden. Diese Einschränkung gilt nicht, wenn von der Wohnung eine erhebliche, die Gesundheit Dritter beeinträchtigende Störung ausgeht.“

10. § 40 wird wie folgt geändert:

a) In Absatz 4 Satz 2 wird die Angabe „von Spezialeinheiten“ gestrichen.

b) Nach Absatz 4 wird der folgende Absatz 5 eingefügt:

„(5) Die Erforderlichkeit, die praktische Anwendung und die Auswirkungen des Einsatzes von Vorrichtungen für den Abschuss besonderer Formen von Projektilen durch Polizeibedienstete, die außerhalb von Spezialeinheiten zum Einsatz kommen, werden nach einem Erfahrungszeitraum von 3 Jahren, spätestens jedoch zum 31. Dezember 2029, durch die Staatsregierung geprüft. Die Staatsregierung berichtet dem Landtag über das Ergebnis der Evaluierung.“

11. § 41 Absatz 1 Satz 3 wird durch folgenden Satz 3 ersetzt:

„Das angewendete Mittel muss nach Art und Maß den jeweiligen Umständen, insbesondere dem Verhalten, dem Alter und dem Zustand der oder des Betroffenen angemessen sein.“

12. In § 48 Absatz 3 Satz 2 wird die Angabe „Erwerbstätigkeit“ durch die Angabe „Erwerbsfähigkeit“ ersetzt.

13. Die §§ 57 und 58 werden durch die folgenden §§ 57, 57a und 58 ersetzt:

„§ 57

Offener Einsatz technischer Mittel zur Bild- und Tonaufnahme und -aufzeichnung

(1) Die Polizei kann bei abstrakten Gefahren im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen unter freiem Himmel, die nicht dem Sächsischen Versammlungsgesetz unterliegen, offen Übersichtsbildübertragungen anfertigen, wenn und soweit dies wegen der Größe der Veranstaltung oder Ansammlung oder der Unübersichtlichkeit der Lage zur Lenkung und Leitung eines Polizeieinsatzes im Einzelfall erforderlich ist. Eine Identifikation von Personen oder Aufzeichnung der Übertragung findet hierbei nicht statt.

(2) Die Polizei kann bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen unter freiem Himmel, die nicht dem Sächsischen Versammlungsgesetz unterliegen, personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen von Personen erheben, bei denen Tatsachen die Annahme rechtfertigen, dass sie innerhalb absehbarer Zeit eine ihrer Art nach konkretisierte Straftat begehen werden, durch die Personen, Sach- oder Vermögenswerte gefährdet werden, oder dass von ihnen sonstige erhebliche Gefahren für die öffentliche Sicherheit ausgehen.

(3) Die Polizei kann

1. an oder in den Objekten im Sinne des § 15 Absatz 1 Satz 1 Nummer 3 oder in deren unmittelbarer Nähe und

2. auf öffentlichen Straßen, Wegen oder Plätzen, wenn nach polizeilich dokumentierten Tatsachen die Kriminalitätsbelastung dort gegenüber der des Gemeindegebiets deutlich erhöht ist (Kriminalitätsschwerpunkte),

personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen von Personen erheben, soweit Tatsachen die Annahme rechtfertigen, dass dort künftig Straftaten begangen werden, durch die Personen, Sach- oder Vermögenswerte gefährdet werden.

(4) Die Polizei kann bei der Durchführung von Maßnahmen zur Gefahrenabwehr durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen personenbezogene Daten kurzzeitig in einem Zwischenspeicher für 60 Sekunden erfassen, soweit und solange dies mit hinreichender Wahrscheinlichkeit zum Schutz der eigenen oder einer dritten Person gegen eine Gefahr für Leib oder Leben erforderlich ist. In Wohnungen ist eine Maßnahme nach Satz 1 nur zulässig, wenn dies mit hinreichender Wahrscheinlichkeit zur Abwehr einer dringenden Gefahr für Leib oder Leben der eigenen oder einer dritten Person erforderlich ist. Satz 2 gilt nicht für Arbeits-, Betriebs- oder Geschäftsräume während der Öffnungszeiten und wenn die Maßnahme während der Öffnungszeiten durchgeführt wird.

(5) Die Speicherung der nach Absatz 4 Satz 1 erlangten Daten über 60 Sekunden hinaus ist nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz der eigenen oder einer dritten Person gegen eine Gefahr für Leib oder Leben erforderlich ist. Die Speicherung der nach Absatz 4 Satz 2 erlangten Daten ist nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz der eigenen oder einer dritten Person gegen eine dringende Gefahr für Leib oder Leben erforderlich ist. Nach den Sätzen 1 und 2 erlangte Daten sind automatisiert nach höchstens 60 Sekunden zu löschen, soweit die Voraussetzungen für eine Aufzeichnung nicht vorliegen.

(6) In Bereichen, die der Ausübung von Tätigkeiten von Berufsgeheimnisträgern nach den §§ 53 und 53a der Strafprozessordnung dienen, sind Maßnahmen nach Absatz 4 und 5 unzulässig. Ergeben sich während der Durchführung einer Maßnahme nach Absatz 5 Satz 2 tatsächliche Anhaltspunkte dafür, dass der Kernbereich privater Lebensgestaltung betroffen ist, ist die Maßnahme zu unterbrechen. Die Maßnahme darf fortgeführt werden, wenn keine Anhaltspunkte mehr dafür vorliegen, dass der Kernbereich privater Lebensgestaltung betroffen ist. Soweit Erkenntnisse aus dem Kernbereich privater Lebensgestaltung durch eine Maßnahme nach Satz 2 erlangt worden sind, dürfen diese nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsache der Erfassung der Daten und der Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden.

(7) Der Einsatz des technischen Mittels nach den Absätzen 4 und 5 ist durch einen optischen oder akustischen Warnhinweis besonders erkennbar zu machen und der Beginn der Aufzeichnung nach Absatz 5 der betroffenen Person mitzuteilen. Bei Gefahr im Verzug kann die Mitteilung unterbleiben. Der Einsatz des technischen Mittels und die Aufzeichnungen sind zum Zweck einer nachträglichen Überprüfung der Rechtsmäßigkeit zu dokumentieren.

(8) Die Aufzeichnungen nach den Absätzen 4 und 5 durch körpernah getragene Geräte sind verschlüsselt sowie manipulationsgesichert zu fertigen und aufzubewahren. Die angefertigten Bild- und Tonaufnahmen sind nach Ablauf von einem Monat zu löschen sowie daraus gefertigte Unterlagen zu vernichten, soweit sie nicht für Zwecke der Strafverfolgung oder für die Überprüfung der Rechtmäßigkeit einer aufgezeichneten Maßnahme oder der Aufzeichnung benötigt werden. Auf Antrag erhalten betroffene Personen Einsicht in die Aufzeichnung. Die betroffenen Personen sind über das Bestehen des Rechts auf Einsichtnahme zu informieren. Näheres zum Verfahren regelt das Staatsministerium des Innern durch Verwaltungsvorschrift. Die weitere Verarbeitung der nach Absatz 5 Satz 2 erlangten Daten ist nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt wurde. Für das Verfahren gelten die

Vorschriften des Buches 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.

(9) Die Polizei darf im öffentlichen Verkehrsraum personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Bildübertragung und -aufzeichnung zur Verhütung von Verstößen gegen die Verkehrsvorschrift des § 23 Absatz 1a der Straßenverkehrs-Ordnung erheben, sofern tatsächliche Anhaltspunkte bestehen, dass an bestimmten Streckenabschnitten oder Verkehrsknotenpunkten in regelmäßiger Weise gegen die genannte Vorschrift verstoßen wird oder es sich in sonstiger Weise um einen Bereich mit besonderer Unfallträchtigkeit handelt. Die Bildaufzeichnungen dürfen das Fahrzeug, das Kraftfahrzeugkennzeichen sowie Informationen über Ort, Zeit, Fahrtrichtung und die fahrzeugführende Person erfassen. Ergibt sich kein Hinweis auf einen Verkehrsverstoß, sind die Bilddaten unverzüglich, spätestens jedoch mit der Beendigung der Maßnahme zu löschen. Aufgezeichnete Daten, die nicht unverzüglich zu löschen sind, dürfen ausschließlich zum Zweck der Verfolgung und Ahndung von Verstößen gegen die in Satz 1 bezeichneten Verkehrsvorschriften verarbeitet werden.

(10) Maßnahmen nach den Absätzen 2 bis 5 und 9 dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(11) Maßnahmen nach Absatz 4 Satz 2 und Absatz 5 Satz 2, die praktische Anwendung und die Auswirkungen dieser Vorschrift werden nach einem Erfahrungszeitraum von drei Jahren, spätestens jedoch zum 31. Dezember 2029, durch die Staatsregierung evaluiert. Die Staatsregierung berichtet dem Landtag über das Ergebnis der Evaluierung.

(12) Nach den Absätzen 2 und 3 erhobene Daten und daraus gefertigte Unterlagen sind spätestens nach zwei Monaten zu löschen oder zu vernichten, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten zur Geltendmachung von öffentlich-rechtlichen Ansprüchen oder nach Maßgabe des § 2 Absatz 2 zum Schutz privater Rechte, insbesondere zur Behebung einer bestehenden Beweisnot erforderlich sind.

§ 57a

Anwendungen zur automatisierten Verarbeitung von an öffentlichen Orten und besonders gefährdeten öffentlichen Einrichtungen offen erhobenen personenbezogenen Daten

(1) Die Polizei kann bei Maßnahmen nach § 57 Absatz 2 und 3 Anwendungen zur automatisierten Datenverarbeitung verwenden zur Erkennung und Auswertung von

1. Bewegungsmustern, die auf die Begehung einer Straftat hindeuten, oder

2. Mustern bezogen auf Waffen im Sinne des § 1 Absatz 2 des Waffengesetzes, Messer und gefährliche Gegenstände.

Sofern Muster nach Satz 1 erkannt werden, prüft die Polizei unverzüglich, ob mit Straftaten von erheblicher Bedeutung in absehbarer Zeit mit hinreichender Wahrscheinlichkeit gerechnet werden kann. Liegen die Voraussetzungen nach Satz 2 vor, kann die Polizei eine automatisierte Nachverfolgung der für das Vorliegen der Voraussetzungen nach Satz 2 verantwortlichen Personen durch ihre Kennzeichnung in den vorliegenden Bildübertragungen und -aufzeichnungen vornehmen. Die Polizei kann in Bezug auf die jeweils nachverfolgten Personen nach Satz 3 eine biometrische Echtzeit-Fernidentifizierung von in öffentlich zugänglichen Bereichen erhobenen personenbezogenen Daten anhand des Datenbestandes der polizeilichen Auskunfts- und Fahndungssysteme

durchführen, wenn eine erhebliche gegenwärtige Gefahr für Leib oder Leben einer Person vorliegt, sofern die Abwehr dieser Gefahr auf diese Weise unbedingt erforderlich ist.

(2) Die Polizei kann durch Maßnahmen nach § 57 Absatz 2 und 3 in öffentlich zugänglichen Bereichen erhobene personenbezogene Daten zu Zwecken der biometrischen Echtzeit-Fernidentifizierung verarbeiten, sofern dies unbedingt erforderlich ist

1. zur Abwehr einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr durch die Begehung einer terroristischen Straftat, soweit es die Daten der Personen betrifft, die diese Gefahr verursachen, oder

2. zur Suche nach im Datenbestand der polizeilichen Auskunfts- und Fahndungssysteme gespeicherten

   a) Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung oder

   b) vermissten Personen.

Soweit es sich bei der terroristischen Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen. Die biometrische Echtzeit-Fernidentifizierung ist zeitlich und örtlich auf das unbedingt erforderliche Maß zu begrenzen.

(3) Maßnahmen nach Absatz 1 Satz 4 und Absatz 2 Satz 1 bedürfen einer richterlichen Anordnung auf Antrag der Präsidentin oder des Präsidenten des Landeskriminalamtes oder einer Polizeidirektion oder durch von diesen beauftragte Bedienstete. In dem Antrag sind anzugeben:

1. der Sachverhalt, insbesondere die einzelfallbezogenen bestimmten Tatsachen, die das Vorliegen der Voraussetzungen nach Absatz 1 Satz 4 oder Absatz 2 Satz 1 begründen, und

2. die Begründung, insbesondere die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme.

Bei Gefahr im Verzug dürfen die Maßnahmen nach Absatz 1 Satz 4 und Absatz 2 Satz 1 nur durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion oder durch von diesen hierzu beauftragte Bedienstete angeordnet werden.

(4) Für die Protokollierung einer Maßnahme nach Absatz 1 Satz 4 oder Absatz 2 gilt § 75 Absatz 1 mit der Maßgabe, dass die Datenverarbeitung vollständig zu protokollieren ist. Die oder der Sächsische Datenschutz- und Transparenzbeauftragte ist unverzüglich über abgeschlossene Maßnahmen nach Absatz 1 Satz 4 und Absatz 2 zu informieren. Das Staatsministerium des Innern hat das Nähere zum Verfahren nach Anhörung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten in einer zu veröffentlichenden Verwaltungsvorschrift zu regeln und insbesondere zu bestimmen

1. die Anforderungen an die in den Abgleich einzubeziehenden biometrischen Daten,

2. den technischen Verfahrensablauf sowie

3. die Anforderungen an die Qualitätsstandards des einzusetzenden Erkennungssystems.

§ 58

Anlassbezogene automatisierte Kennzeichenerkennung

(1) Die Polizei kann durch den Einsatz technischer Mittel ohne Wissen der Person Kennzeichen von Kraftfahrzeugen sowie Informationen über Ort, Zeit und Fahrtrichtung automatisiert erheben mit dem Ziel des unmittelbar anschließenden automatisierten Abgleichs mit polizeilichen Datenbeständen

1. zur Abwehr einer erheblichen Gefahr, soweit dokumentierte Erkenntnisse eine solche Gefahr begründen,

2. zur Verhütung von Straftaten von erheblicher Bedeutung unter den Voraussetzungen des § 15 Absatz 1 Nummer 3 in unmittelbarer Nähe zu den in § 15 Absatz 1 Nummer 3 genannten Anlagen, Einrichtungen, Gebäuden oder Objekten, soweit Tatsachen die Annahme rechtfertigen, dass dort Straftaten von erheblicher Bedeutung begangen werden sollen,

3. zur Verhütung von Straftaten von erheblicher Bedeutung auf Bundesfernstraßen, soweit Tatsachen die Annahme rechtfertigen, dass im Umfeld des Kontrollorts gewerbs- oder gewohnheitsmäßig Straftaten von erheblicher Bedeutung durch überregional agierende Täter begangen werden sollen,

4. zur Verhütung von Straftaten von erheblicher Bedeutung in der Nähe von Orten gemäß § 57 Absatz 3 Nummer 2, soweit Tatsachen die Annahme rechtfertigen, dass dort Straftaten von erheblicher Bedeutung begangen werden sollen, oder

5. in der unmittelbaren Nähe zu öffentlichen Einrichtungen des internationalen Verkehrs oder im Grenzgebiet zur Republik Polen und zur Tschechischen Republik bis zu einer Tiefe von 30 Kilometern, wenn Tatsachen die Annahme rechtfertigen, dass dort zum Zeitpunkt der Kontrolle Straftaten von erheblicher Bedeutung begangen werden sollen.

Maßnahmen nach § 60 sind unzulässig.

(2) Ein automatisierter unverzüglicher Abgleich nach Absatz 1 ist nur zulässig mit anlassabhängig bestimmten Fahndungsbeständen über Kennzeichen von Fahrzeugen, die

1. nach § 60 oder einer vergleichbaren Vorschrift eines anderen Landes, den §§ 163e und 463a der Strafprozessordnung, Artikel 36 der Verordnung (EU) 2018/1862 und § 47 des Bundeskriminalamtgesetzes,

2. auf Grund einer Gefahr für Zwecke der Gefahrenabwehr,

3. auf Grund des Verdachts einer Straftat für Zwecke der Strafverfolgung oder

4. aus Gründen der Strafvollstreckung

in den Sachfahndungsbeständen der Informationssysteme der Polizei und im Schengener Informationssystem ausgeschrieben sind. In den Fällen des Absatzes 1 Nummer 1 darf ein Abgleich nur mit den zu diesen Zwecken gespeicherten personenbezogenen Daten erfolgen. Im Übrigen sind die einzubeziehenden Fahndungsbestände auf solche Kennzeichendaten zu beschränken, die für die jeweiligen Zwecke Bedeutung haben können. Der Abgleich darf nur mit vollständigen erfassten Kennzeichen des Fahndungsbestandes erfolgen.

(3) Der Einsatz technischer Mittel im Sinne des Absatzes 1 ist zeitlich und örtlich zu begrenzen. Durch technisch-organisatorische Maßnahmen ist sicherzustellen, dass der Einsatz solcher Mittel weder einzeln noch in der Kombination flächendeckend oder im Dauerbetrieb erfolgt. Liegt im Ergebnis des automatisierten Abgleichs nach Absatz 2 eine Datenübereinstimmung vor, ist sie unverzüglich durch Inaugenscheinnahme zu verifizieren. Liegt für das vollständig nach Absatz 1 erhobene Kraftfahrzeugkennzeichen keine Datenübereinstimmung vor, sind die erhobenen Daten sofort, technisch spurenlos und automatisiert zu löschen. Gleiches gilt, wenn im Ergebnis der Prüfung nach Satz 3 keine Übereinstimmung der Daten festgestellt wurde. Einzelerfassungen dürfen nicht zu einem Bewegungsbild zusammengeführt werden. Bei Datenübereinstimmung können die Daten nach Maßgabe des § 79a weiterverarbeitet werden. Datenerhebungen und Datenabgleiche dürfen nicht protokolliert werden.

(4) Bei Datenübereinstimmung kann das betreffende Kraftfahrzeug angehalten und die Identität der in diesem angetroffenen Personen festgestellt werden. § 15 Absatz 2 und 3 gilt entsprechend.

(5) Maßnahmen nach Absatz 1 dürfen nur durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion oder durch von diesen hierzu beauftragte Bedienstete angeordnet werden. Die Erkenntnisse, die der Maßnahme zugrunde liegen und die Fahndungsbestände, die zum Abgleich einbezogen werden, sind in der Anordnung zu dokumentieren.

(6) Die Erforderlichkeit, die praktische Anwendung und die Auswirkungen des stationären Technikeinsatzes werden nach einem Erfahrungszeitraum von 3 Jahren, spätestens jedoch zum 31. Dezember 2029, durch die Staatsregierung geprüft. Die Staatsregierung berichtet dem Landtag über das Ergebnis der Evaluierung.“

14. § 59 wird gestrichen.

15. § Die §§ 60 und 61 werden durch die folgenden §§ 60 und 61 ersetzt:

„§ 60

Ausschreibung von Personen und Sachen

(1) Die Polizei kann die Personalien einer Person, das amtliche Kennzeichen eines von ihr benutzten oder eingesetzten Kraftfahrzeugs oder die Identifizierungsnummer oder äußere Kennzeichnung eines von ihr eingesetzten Wasserfahrzeugs, Luftfahrzeugs oder Containers in Fahndungssystemen zur verdeckten Kontrolle, Ermittlungsanfrage oder gezielten Kontrolle ausschreiben, wenn die Maßnahme zur Verhütung der Straftat erforderlich ist und

1. Tatsachen die Annahme rechtfertigen, dass die Person in absehbarer Zeit eine zumindest der Art nach konkretisierte Straftat von erheblicher Bedeutung begehen wird, oder

2. das Verhalten der Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen wird.

Soweit es sich bei der in Satz 1 Nummer 1 oder 2 in Bezug genommenen Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen.

(2) Wird eine nach Absatz 1 ausgeschriebene Person oder ein ausgeschriebenes amtliches Kraftfahrzeugkennzeichen bei einer polizeilichen Kontrolle festgestellt, dürfen an die ausschreibende Polizeidienststelle übermittelt werden

1. im Fall der Ausschreibung zur verdeckten Kontrolle Erkenntnisse über das Antreffen, die erlangten Erkenntnisse über Ort und Zeit des Antreffens der Person, Anlass der Überprüfung, Reiseweg und Reiseziel, gemeinsam mit der ausgeschriebenen Person angetroffene Personen oder Insassen des Fahrzeugs und mitgeführte Sachen,

2. im Fall der gezielten Kontrolle, zusätzlich zu den Erkenntnissen nach Nummer 1, solche aus § 27 Absatz 1 Nummer 6 und § 28 Absatz 1 Nummer 6 bis 8 sowie

3. im Fall der Ermittlungsanfrage die durch die Befragung der Person erlangten Erkenntnisse.

(3) Ausschreibungen nach Absatz 1 dürfen für höchstens ein Jahr angeordnet werden. Eine Verlängerung um höchstens ein Jahr ist zulässig, soweit die Voraussetzungen weiterhin vorliegen. Die Verlängerung von Ausschreibungen zur verdeckten Kontrolle bedarf der gerichtlichen Anordnung nach Maßgabe von Absatz 4 Satz 2. Spätestens nach jeweils sechs Monaten hat die ausschreibende Polizeidienststelle zu prüfen, ob die Voraussetzungen für die Ausschreibung noch vorliegen. Das Ergebnis der Prüfung ist zu dokumentieren. Liegen die Voraussetzungen für die Ausschreibung nicht mehr vor, ist der Zweck der Ausschreibung erreicht oder kann er nicht erreicht werden, ist die Ausschreibung unverzüglich zu löschen.

(4) Maßnahmen nach Absatz 1 dürfen nur durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion oder durch von diesen hierzu beauftragte Bedienstete angeordnet werden. In der schriftlichen Anordnung sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,

2. Art, Umfang und Dauer der Maßnahme,

3. der Sachverhalt sowie

4. die Begründung.

§ 61

Elektronische Aufenthaltsüberwachung

(1) Die Polizei kann eine Person dazu verpflichten, ein technisches Mittel, mit dem der Aufenthaltsort dieser Person elektronisch überwacht werden kann, ständig in betriebsbereitem Zustand am Körper bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen, wenn

1. dies zum Schutz einer bestimmten anderen gefährdeten Person erforderlich ist, weil Tatsachen die Annahme rechtfertigen, dass dann, wenn die überwachte Person bestimmte Orte betritt, aufsucht oder sich dort aufhält oder mit der gefährdeten Person zusammentrifft, Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung, soweit sie durch Straftatbestände geschützt ist, die im Mindestmaß mit wenigstens drei Monaten Freiheitsstrafe bedroht sind, der gefährdeten Person innerhalb eines

absehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise durch einen Angriff von erheblicher Intensität oder Auswirkung gefährdet sind,

2. gegen die Person eine Maßnahme nach § 21 Absatz 2 angeordnet wird und Tatsachen die Annahme begründen, dass die elektronische Aufenthaltsüberwachung erforderlich ist, um diese Person durch die Überwachung und die Datenverarbeitung von der Begehung der anlassgebenden Straftaten abzuhalten und Verstöße gegen Aufenthaltsanordnungen oder Kontaktverbote nach § 21 Absatz 2 zu verhüten,

3. das Verhalten dieser Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen wird und die Maßnahme sie von deren Begehung abhalten soll.

Soweit es sich bei der in Satz 1 Nummer 3 in Bezug genommenen Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen.

(2) Die Polizei kann mit Hilfe des von der Person mitgeführten technischen Mittels automatisiert Daten über deren Aufenthaltsort sowie über etwaige Beeinträchtigungen der Datenerhebung verarbeiten. Soweit dies zur Erfüllung des Überwachungszwecks nach Absatz 1 erforderlich ist, dürfen die erhobenen Daten zu einem Bewegungsbild verbunden werden. Es ist, soweit dies technisch möglich ist, sicherzustellen, dass innerhalb der Wohnung der betroffenen Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden; dennoch erhobene Daten dürfen nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsache ihrer Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich zum Zweck der Datenschutzkontrolle verwendet werden. Sie ist nach Abschluss der Datenschutzkontrolle nach § 94 zu löschen. Daten nach den Sätzen 1 und 2 dürfen nur verarbeitet werden, wenn dies zu folgenden Zwecken erforderlich ist:

1. zur Abwehr einer Gefahr für Leib, Leben, Freiheit oder die sexuelle Selbstbestimmung, soweit sie durch Straftatbestände geschützt ist, die im Mindestmaß mit wenigstens drei Monaten Freiheitsstrafe bedroht sind,

2. zur Verhütung oder zur Verfolgung von terroristischen Straftaten sowie von Straftaten gegen die in Nummer 1 genannten Rechtsgüter,

3. zur Feststellung von Verstößen gegen Anordnungen nach § 19 Absatz 1 Nummer 1, Nummer 2 Buchstabe a, Nummer 2 Buchstabe b und Nummer 2 Buchstabe d oder nach § 21 Absatz 2 Satz 1 oder Absatz 3,

4. zur Verfolgung einer Straftat nach § 106,

5. zur Aufrechterhaltung der Funktionsfähigkeit des technischen Mittels.

Soweit es sich bei den in Satz 7 Nummer 2 in Bezug genommenen Straftaten um Vorfeldstraftaten handelt, kann die Datenverarbeitung nur erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt. Zur Einhaltung der Zweckbindung nach Satz 7 hat die Verarbeitung der Standortdaten automatisiert zu erfolgen. Die Daten sind gegen unbefugte Kenntnisnahme und Verarbeitung besonders zu sichern. Die in Satz 1 und Satz 2 genannten Daten sind spätestens zwei Monate nach Beendigung der Maßnahme zu löschen, soweit sie nicht zu Zwecken nach Satz 7 weiterverarbeitet werden. Jeder Abruf der Daten ist gemäß § 32 des Sächsischen Datenschutz-Umsetzungsgesetzes zu protokollieren. Die Protokolldaten sind nach Abschluss der Datenschutzkontrolle nach § 94 zu löschen.

(3) Maßnahmen nach Absatz 1 bedürfen einer richterlichen Anordnung auf Antrag der Polizei. Bei Gefahr im Verzug kann die Anordnung durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion oder durch von diesen hierzu beauftragte Bedienstete getroffen werden. In diesem Fall ist eine gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nicht innerhalb von drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. Die Maßnahme ist zu beenden, wenn sie durch das Gericht abgelehnt wird.

(4) In dem Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Name und Anschrift,

2. Art, Umfang und Dauer der Maßnahme, die Angabe, ob gegenüber der Person, gegen die sich die Maßnahme richtet, Maßnahmen nach § 19 Absatz 1 oder § 21 Absatz 2 angeordnet worden sind,

3. der Sachverhalt sowie

4. die Begründung.

(5) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Name und Anschrift,

2. Art, Umfang und Dauer der Maßnahme sowie

3. die wesentlichen Gründe.

(6) Im Rahmen von Maßnahmen nach Absatz 1 Nummer 1 oder 2 ist die Erstellung eines Bewegungsbildes nur zulässig, soweit dies durch richterliche Anordnung auf Antrag der Polizei ausdrücklich gestattet wird. Die Anordnung ist sofort vollziehbar. Sie ist auf höchstens zwei Monate zu befristen; eine Verlängerung um jeweils nicht mehr als zwei Monate ist zulässig, sofern die Voraussetzungen für die Anordnung noch vorliegen. Die Maßnahme ist unverzüglich zu beenden, wenn die Voraussetzungen nicht mehr vorliegen.

(7) Die Erforderlichkeit, die praktische Anwendung und die Auswirkungen dieser Vorschrift werden nach einem Erfahrungszeitraum von drei Jahren, spätestens jedoch zum 31. Dezember 2029, durch die Staatsregierung geprüft. Die Staatsregierung berichtet dem Landtag über das Ergebnis der Evaluierung.“

16. Nach § 62 werden die folgenden §§ 62a und 62b eingefügt:

„§ 62a

Anlassbezogene Anwendung zur automatisierten Datenanalyse

(1) Die Polizei kann unter den Voraussetzungen des § 79a zur Gewinnung neuer Erkenntnisse gespeicherte personenbezogene Daten anlassbezogen automatisiert zusammenführen und mit weiteren nach diesem Gesetz oder anderen Rechtsgrundlagen gespeicherten personenbezogenen Daten automatisiert verknüpfen, aufbereiten und auswerten (automatisierte Datenanalyse), soweit

1. dies erforderlich ist zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder der Länder, Leib, Leben, Gesundheit oder Freiheit einer Person

oder für Sachen von besonderem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,

2. Tatsachen die Annahme rechtfertigen, dass in absehbarer Zeit eine zumindest ihrer Art nach konkretisierte Straftat von erheblicher Bedeutung begangen wird und die automatisierte Datenanalyse zur Verhinderung dieser Straftat erforderlich ist, oder

3. Tatsachen die Annahme rechtfertigen, dass Straftaten nach § 100a Absatz 2 oder § 100b Absatz 2 der Strafprozessordnung begangen werden sollen und die automatisierte Datenanalyse zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist.

Soweit es sich bei der in Satz 1 Nummer 2 und 3 in Bezug genommenen Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen. Im Fall einer Straftat nach § 100a Absatz 2 der Strafprozessordnung muss die zu verhütende Straftat auch im Einzelfall vorliegen.

(2) Die Polizei hat die durch die automatisierte Datenanalyse bereitgestellten Informationen abschließend zu bewerten und die erforderlichen weiteren Entscheidungen zu treffen. Bei der automatisierten Datenanalyse ist sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Die automatisierte Datenanalyse wird manuell ausgelöst und erfolgt auf der Grundlage von anlassbezogenen Suchbegriffen, die sich aus einem konkreten Sachverhalt bezogen auf einen Anlassfall im Sinne des Absatzes 1 Satz 1 ergeben. Bei Maßnahmen nach Absatz 1 Nummer 2 und 3 ist der Suchvorgang auf die nach den §§ 6 und 7 Verantwortlichen auszurichten. Eine direkte Anbindung der Analyseplattform an Internetdienste ist unzulässig.

(3) Zum Zweck einer automatisierten Datenanalyse können eigene Vorgangsdaten, Falldaten, Daten aus polizeilichen Auskunftssystemen, Verkehrsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch zusammengeführt werden. Datensätze aus gezielten Abfragen in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen können ergänzend einbezogen werden, soweit dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. Personenbezogene Vorgangsdaten zu Unbeteiligten sind von der automatisierten Datenanalyse ausgenommen. Verkehrsdaten dürfen bei einer Maßnahme nach Absatz 1 Nummer 3 nicht in die Datenanalyse einbezogen werden. Zur Datenanalyse gespeicherte personenbezogene Verkehrsdaten sind nach Ablauf von zwei Jahren zu löschen, soweit nicht die weitere Speicherung der Daten für die Fallbearbeitung ausnahmsweise erforderlich ist. Die Entscheidung, die Daten nicht zu löschen, ist zu begründen. Personenbezogene Daten, die aus einer Wohnraumüberwachung gewonnen wurden, dürfen nicht in die automatisierte Datenanalyse einbezogen werden.

(4) Das Staatsministerium des Innern hat nach Anhörung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten das Nähere zum Verfahren in einer zu veröffentlichenden Verwaltungsvorschrift zu regeln und insbesondere zu bestimmen

1. Art und Umfang der Daten, die zur automatisierten Datenanalyse zusammengeführt werden unter Berücksichtigung des Eingriffsgewichts der automatisierten Datenanalyse im Hinblick auf die Kategorie der betroffenen Personen nach § 28 des Sächsischen Datenschutz-Umsetzungsgesetzes,

2. die Erteilung von Zugriffsberechtigungen durch ein Rollen- und Rechtekonzept,

3. erforderliche Kennzeichnungen zur Sicherstellung der Einhaltung der Zweckbindung,

4. die Durchführung von Zugriffskontrollen,

5. die Anforderungen an die Protokollierung, die Dauer der Aufbewahrung der Protokolldaten und die Dokumentation von Maßnahmen,

6. die Methoden und Techniken, die zur automatisierten Datenanalyse eingesetzt werden dürfen, sowie

7. verfahrensrechtliche Maßnahmen zum Zweck der Erkennung und Korrektur fehlerhafter Datenauswertung.

Im Hinblick auf das gemäß Satz 1 Nummer 1 zu erstellende Konzept ist sicherzustellen, dass das Gewicht des Grundrechtseingriffs der Erhebung der Daten und der Veranlassungszusammenhang bei der Bestimmung des Umfangs der in die Datenanalyse einzubeziehenden Daten Berücksichtigung findet. Unter Veranlassungszusammenhang ist der sachliche Bezug der von der Analyse betroffenen Person zum jeweiligen Phänomenbereich zu verstehen. Bei dem gemäß Satz 1 Nummer 2 zu erstellenden Konzept ist sicherzustellen, dass die Zugriffsrechte eingeschränkt nach Phänomenbereichen, Funktion und spezifischer Qualifikation der Zugriffsberechtigten gestaltet werden. Bei der Ausgestaltung der Zugriffsrechte ist zudem der Umfang und die Sensibilität der von der Zugriffsberechtigung umfassten Daten zu berücksichtigen.

(5) Der Zugang zur Anwendung der automatisierten Datenanalyse ist durch eine Zugriffskontrolle zu reglementieren. Die Zugriffe unterliegen hierbei der ständigen Protokollierung. Jeder Fall der automatisierten Datenanwendung ist von der Anwenderin oder dem Anwender zu begründen.

(6) Die Einrichtung, wesentliche Änderung und Anwendung einer automatisierten Datenanalyse erfolgt durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion oder durch von diesen hierzu beauftragte Bedienstete. Die oder der Sächsische Datenschutz- und Transparenzbeauftragte ist vor der Einrichtung, wesentlichen Änderung oder Anwendung anzuhören. Bei Gefahr im Verzug ist die Anhörung nachzuholen. § 94 bleibt unberührt.

§ 62b

Anlassbezogener nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

(1) Die Polizei kann biometrische Daten im Sinne von § 2 Nummer 13 des Sächsischen Datenschutz-Umsetzungsgesetzes zu Gesichtern und Stimmen, die sie zur Erfüllung ihrer Aufgaben verarbeiten darf oder für die sie eine Berechtigung zum Abruf hat, mit öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung nachträglich zur Datenverarbeitung biometrisch abgleichen, sofern

1. dies erforderlich ist zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse erforderlich ist, oder

2. die Identifizierung oder die Ermittlung des Aufenthaltsorts der Zielperson, von der die Gefahr ausgeht, auf andere Weise aussichtslos ist oder wesentlich erschwert wäre.

Die Maßnahme nach Satz 1 ist auch zulässig, sofern

1. Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat gemäß § 100a Absatz 2 der Strafprozessordnung begehen wird, oder

2. das Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraums eine terroristische Straftat begehen wird, und die Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Ein Abgleich der biometrischen Daten nach Satz 1 mit im Internet öffentlich zugänglichen Echtzeit-Lichtbild- und Echtzeit-Videodateien darf nicht erfolgen. Soweit es sich bei der in Satz 2 Nummer 1 oder 2 in Bezug genommenen Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen.

(2) Liegt im Ergebnis des automatisierten Abgleichs nach Absatz 1 eine Datenübereinstimmung vor, ist sie unverzüglich durch Inaugenscheinnahme zu verifizieren. Weitere Maßnahmen dürfen erst nach erfolgreicher Verifizierung erfolgen. Liegt im Ergebnis eines automatisierten Abgleichs nach Absatz 1 oder einer Prüfung nach Satz 1 keine Datenübereinstimmung vor, sind die erhobenen Daten sofort technisch spurenlos und automatisiert zu löschen. Im Fall von Satz 3 darf die Datenverarbeitung nicht protokolliert werden.

(3) Maßnahmen nach Absatz 1 Satz 1 bedürfen einer richterlichen Anordnung auf Antrag der Polizei. In dem schriftlichen Antrag sind anzugeben:

1. die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird,

2. die biometrischen Daten, die dieser Person zuzuordnen sind, und die Daten, die zum Abgleich herangezogen werden sollen,

3. der Sachverhalt sowie

4. die Begründung.

(4) Die oder der Sächsische Datenschutz- und Transparenzbeauftragte ist unverzüglich über abgeschlossene Maßnahmen nach Absatz 3 Satz 2 zu informieren. § 94 bleibt unberührt.

(5) Das Staatsministerium des Innern hat nach Anhörung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten das Nähere zum Verfahren in einer zu veröffentlichenden Verwaltungsvorschrift zu regeln und insbesondere zu bestimmen

1. die Anforderungen an die in den Abgleich einzubeziehenden biometrischen Daten,

2. den technischen Verfahrensablauf und

3. die Anforderungen an die Qualitätsstandards des einzusetzenden Erkennungssystems.“

17. § 63 Absatz 2 wird durch folgenden § 63 Absatz 2 ersetzt:

„(2) Personenbezogene Daten dürfen durch Maßnahmen nach Absatz 1 nur erhoben werden über:

1. die für eine Gefahr nach den §§ 6 oder 7 Verantwortlichen oder unter den Voraussetzungen des § 9 über Personen, die für die Gefahr nicht verantwortlich sind, wenn dies erforderlich ist zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leben, Gesundheit oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist,

2. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie in absehbarer Zeit eine zumindest ihrer Art nach konkretisierte Straftat von erheblicher Bedeutung begehen werden,

3. Personen, bei denen das Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen werden, oder

4. Kontakt- und Begleitpersonen der Personen nach den Nummern 2 und 3.

Soweit es sich bei der in Satz 1 Nummer 2 oder 3 in Bezug genommenen Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen. Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind.“

18. § 64 wird durch folgenden § 64 ersetzt:

„§ 64

Einsatz einer V-Person, Verdeckte Ermittlerin und Verdeckter Ermittler

(1) Die Polizei kann unter den Voraussetzungen des § 63 Absatz 2 Satz 1 und 2 personenbezogene Daten erheben durch den Einsatz:

1. von Polizeibediensteten, die unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität (Legende) ermitteln (Verdeckte Ermittlerin, Verdeckter Ermittler), oder

2. einer Person, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist (V-Person).

(2) Soweit es für den Aufbau und zur Aufrechterhaltung der Legende von Verdeckten Ermittlerinnen und Ermittlern unerlässlich ist, dürfen Urkunden hergestellt, verändert und gebraucht werden. Verdeckte Ermittlerinnen und Ermittler dürfen unter ihrer Legende zur Erfüllung ihres Auftrages am Rechtsverkehr teilnehmen.

(3) Verdeckte Ermittlerinnen und Ermittler dürfen unter Verwendung ihrer Legende eine Wohnung mit dem Einverständnis der berechtigten Person betreten. Das Einverständnis darf nicht durch ein über die Benutzung der Legende hinausgehendes Vortäuschen eines Zutrittsrechts herbeigeführt werden.

(4) Liegen tatsächliche Anhaltspunkte dafür vor, dass durch eine Maßnahme ausschließlich Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Ergeben sich bei der Durchführung einer Maßnahme tatsächliche Anhaltspunkte dafür, dass der Kernbereich privater Lebensgestaltung betroffen ist, ist der Einsatz zu unterbrechen, sobald dies ohne Gefährdung für Leib, Leben oder die weitere Verwendung als Verdeckte Ermittlerin, verdeckter Ermittler oder als V-Person möglich ist. Unterbleibt die Unterbrechung, sind die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und die Umstände des Fortsetzens der Maßnahme zu dokumentieren. Die Maßnahme darf fortgeführt werden, sobald zu erwarten ist, dass die Gründe, die zur Unterbrechung geführt haben, nicht mehr vorliegen. Vor der Weitergabe von Informationen hat die Verdeckte Ermittlerin, der Verdeckte Ermittler oder die V-Person sowie deren polizeiliche Kontaktperson zu prüfen, ob durch die Information oder die Art und Weise, in der sie erlangt wurde, Erkenntnisse aus dem Kernbereich privater Lebensgestaltung betroffen sind. Bestehen Zweifel, ob Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen worden sind, entscheidet die oder der behördliche Datenschutzbeauftragte über die Verwendbarkeit und Löschung der Daten. Im Übrigen gilt § 76 Absatz 5. Gleiches gilt, wenn der Verdeckten Ermittlerin, dem Verdeckten Ermittler oder der V-Person Erkenntnisse aus dem Kernbereich privater Lebensgestaltung bekannt werden.

(5) Als V-Person darf nicht eingesetzt werden, wer

1. minderjährig ist oder unter Betreuung steht (§ 1896 des Bürgerlichen Gesetzbuches) oder

2. nach § 53 oder § 53a der Strafprozessordnung zur Verweigerung des Zeugnisses berechtigt ist, soweit Sachverhalte betroffen sind, auf die sich das Zeugnisverweigerungsrecht bezieht.

(6) Die Zusammenarbeit mit einer V-Person ist zu beenden, wenn

1. der Einsatz nicht mehr erforderlich ist,

2. die Person sich als ungeeignet erweist,

3. die Person eine Straftat von erheblicher Bedeutung begeht oder

4. nachträglich ein Ausschlussgrund im Sinne des Absatzes 5 Nummer 2 eintritt.

(7) Maßnahmen nach Absatz 1 bedürfen einer richterlichen Anordnung auf Antrag der Polizei. Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,

2. Art, Umfang und Dauer der Maßnahme,

3. der Sachverhalt und

4. die Begründung.

Die Anordnung ist auf höchstens sechs Monate zu befristen.“

19. Die §§ 66 bis 68 werden durch die folgenden §§ 66 bis 68 ersetzt:

„§ 66

Überwachung der Telekommunikation

(1) Die Polizei kann ohne Wissen der betroffenen Person deren Telekommunikation überwachen und aufzeichnen sowie deren noch innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegte Inhalte erheben. Die Maßnahme kann sich richten gegen eine Person

1. die nach den §§ 6 oder 7 verantwortlich ist und wenn die Maßnahme erforderlich ist zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt,

2. bei der Tatsachen die Annahme rechtfertigen, dass sie in absehbarer Zeit eine zumindest ihrer Art nach konkretisierte Straftat gemäß § 100a Absatz 2 der Strafprozessordnung, die sich gegen die Rechtsgüter nach Nummer 1 richtet, begehen wird und im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für ein solches Rechtsgut vorliegen,

3. deren Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen wird,

4. bei der Tatsachen die Annahme rechtfertigen, dass eine Person nach den Nummern 1 bis 3 deren Telekommunikationsanschluss oder Endgerät benutzt, oder

5. bei der Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach den Nummern 1 bis 3 bestimmte Mitteilungen entgegennimmt oder von dieser herrührende Mitteilungen weitergibt.

Soweit es sich bei der in Satz 2 Nummer 2 und 3 in Bezug genommenen Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen. Die Datenerhebung ist nur zulässig, wenn die Abwehr der Gefahr oder die Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Die Überwachung und Aufzeichnung der Telekommunikation kann unter den Voraussetzungen des Absatzes 2a auch in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und

2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

(2a) Die Überwachung und Aufzeichnung der Telekommunikation nach Absatz 2 darf sich nur gegen eine Person richten,

1. die nach den §§ 6 oder 7 verantwortlich ist und wenn die Maßnahme erforderlich ist zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Existenz der Menschen berührt,

2. bei der Tatsachen die Annahme rechtfertigen, dass sie in absehbarer Zeit eine zumindest ihrer Art nach konkretisierte Straftat gemäß § 100a Absatz 2 der Strafprozessordnung, die sich gegen die Rechtsgüter nach Nummer 1 richtet, begehen wird und im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für ein solches Rechtsgut vorliegen,

3. deren Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen wird,

4. bei der Tatsachen die Annahme rechtfertigen, dass eine Person nach den Nummern 1 bis 3 deren Telekommunikationsanschluss oder Endgerät benutzt, oder

5. bei der Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach den Nummern 1 bis 3 bestimmte Mitteilungen entgegennimmt oder von dieser herrührende Mitteilungen weitergibt.

Soweit es sich bei der in Satz 1 Nummer 3 in Bezug genommenen Straftat um eine Vorfeldstraftat handelt, ist die Maßnahme nur zulässig, wenn im Einzelfall auch tatsächliche Anhaltspunkte für eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegen. Die Datenerhebung ist nur zulässig, wenn die Abwehr der Gefahr oder die Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(3) Bei Eingriffen nach Absatz 2 ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

(4) Maßnahmen nach Absatz 1 und 2 bedürfen einer richterlichen Anordnung auf Antrag der Polizei. Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,

2. die Rufnummer oder eine andere spezifische Kennung des zu überwachenden Telekommunikationsanschlusses oder des Endgerätes, sofern sich nicht aus Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zuzuordnen ist,

3. im Fall des Absatzes 2 möglichst genau das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, und das technische Mittel,

4. Art, Umfang und Dauer der Maßnahme,

5. der Sachverhalt sowie

6. die Begründung.

(5) Auf Grund einer Anordnung nach Absatz 1 hat jeder Anbieter gemäß § 3 Nummer 1 des Telekommunikationsgesetzes (Diensteanbieter) nach Maßgabe der Regelungen des Telekommunikationsgesetzes und der darauf beruhenden Rechtsverord-

nung zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen der Polizei die Überwachung und Aufzeichnung von Telekommunikationsverbindungen zu ermöglichen. Für die Entschädigung gilt § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend.

(6) Maßnahmen nach Absatz 2, die praktische Anwendung und die Auswirkungen dieser Vorschrift werden nach einem Erfahrungszeitraum von drei Jahren, spätestens jedoch zum 31. Dezember 2029, durch die Staatsregierung geprüft. Die Staatsregierung berichtet dem Landtag über das Ergebnis der Evaluierung.

§ 66a

Unterbrechung oder Verhinderung der Telekommunikation

(1) Für die Unterbrechung oder Verhinderung von Telekommunikationsverbindungen durch die Polizei gilt § 66 Absatz 1 entsprechend.

(2) Telekommunikationsverbindungen Dritter dürfen nur unterbrochen oder verhindert werden, wenn dies aus technischen Gründen zur Durchführung der Maßnahme unvermeidbar ist und zum Zweck der Maßnahme nicht außer Verhältnis steht.

(3) Zur Abwehr einer unmittelbar bevorstehenden erheblichen Gefahr für Leib oder Leben einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, kann die Telekommunikationsverbindung auch ohne Kenntnis der Rufnummer oder einer anderen Kennung des betreffenden Anschlusses oder des Endgerätes unterbrochen oder verhindert werden, indem ein räumlicher Bereich, insbesondere eine Funkzelle, technisch blockiert wird.

(4) Über die Unterbrechung oder Verhinderung von Telekommunikationsverbindungen nach den Absätzen 1 und 3 sind die betroffenen Diensteanbieter zu informieren.

(5) Die Unterbrechung oder Verhinderung von Telekommunikationsverbindungen nach den Absätzen 1 und 3 bedürfen einer richterlichen Anordnung auf Antrag der Polizei. Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,

2. soweit bekannt, die Rufnummer oder eine andere Kennung des zu blockierenden Anschlusses oder des Endgerätes,

3. im Fall des Absatzes 4 die Bezeichnung der Funkzelle oder des räumlichen Bereichs, in dem sich das zu blockierende Endgerät befinden soll,

4. Art, Umfang und Dauer der Maßnahme,

5. der Sachverhalt sowie

6. die Begründung.

Die Anordnung ist auf höchstens drei Tage zu befristen.

(6) Auf Grund einer Anordnung nach Absatz 5 ist jeder Diensteanbieter verpflichtet, unverzüglich

1. bestehende Telekommunikationsverbindungen bekannter, zur Telekommunikation nutzbarer Endgeräte zu unterbrechen oder dies von Beginn an zu verhindern, oder

2. jede Telekommunikationsverbindung in einem bestimmten räumlichen Bereich technisch zu blockieren.

Für die Entschädigung der Diensteanbieter gilt § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend.

§ 67

Erhebung von Verkehrs- und Nutzungsdaten

(1) Für die Erhebung von Verkehrsdaten im Sinne des § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten im Sinne des § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes durch die Polizei gilt § 66 Absatz 1 entsprechend. Die Erhebung von Verkehrsdaten und Nutzungsdaten kann sich auch auf Zeiträume vor deren Anordnung erstrecken. Maßnahmen nach Satz 1 dürfen auch durchgeführt werden, wenn unbeteiligte Dritte unvermeidbar betroffen werden.

(2) Maßnahmen nach Absatz 1 Satz 1 bedürfen einer richterlichen Anordnung auf Antrag der Polizei. Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,

2. die Rufnummer oder eine andere spezifische Kennung des zu ermittelnden Telekommunikationsanschlusses oder des Endgerätes; eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation oder des Endgerätes ist ausreichend, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre,

3. Art, Umfang und Dauer der Maßnahme,

4. der Sachverhalt sowie

5. die Begründung.

(3) Auf Grund der Anordnung einer Datenerhebung nach Absatz 1 ist jeder Diensteanbieter und jeder Anbieter nach § 2 Absatz 1 Satz 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes verpflichtet, der Polizei die zu beauskunftenden Verkehrs- und Nutzungsdaten zu übermitteln. Die Daten sind unverzüglich auf dem von der Polizei bestimmten Weg zu übermitteln. Für die Entschädigung gilt § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend.

§ 68

Identifizierung und Lokalisierung von Telekommunikationsgeräten

(1) Für den verdeckten Einsatz technischer Mittel zur Ermittlung

1. spezifischer Kennungen, insbesondere der Geräte- und Kartennummer von zur Telekommunikation nutzbaren Endgeräten oder

2. des Standortes eines zur Telekommunikation nutzbaren Endgerätes

gilt § 66 Absatz 1 entsprechend.

(2) Die Polizei kann, soweit dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer vermissten, hilflosen oder suizidgefährdeten Person oder einer gefährdeten Person, die einen Notruf über eine öffentlich bekannt gegebene Telefonnummer der Polizei ausgelöst hat, den Standort eines ihr zuzuordnenden mobilen Endgerätes ermitteln, wenn die Ermittlung des Aufenthaltsortes auf andere Weise weniger Erfolg versprechend oder erschwert wäre. Unter den Voraussetzungen des Satzes 1 kann die Polizei von jedem Diensteanbieter jederzeit Auskunft über die für die Ermittlung des Standortes des Endgerätes erforderlichen Daten sowie dessen netzseitige Teilnehmerkennung und Gerätenummer verlangen. Für die Entschädigung gilt § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend.

(3) Personenbezogene Daten Dritter dürfen nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. Daten nach Absatz 1 dürfen nur zum Zweck des Datenabgleichs zur Ermittlung der spezifischen Kennung oder des Standortes des mobilen Endgerätes verwendet werden. Daten nach Absatz 2 dürfen nur zum Zweck des Datenabgleichs zur Ermittlung des Standortes des mobilen Endgerätes verwendet werden. Nach Beendigung der Maßnahme sind die Daten unverzüglich zu löschen.

(4) Maßnahmen nach Absatz 1 bedürfen einer richterlichen Anordnung auf Antrag der Polizei. Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,

2. soweit bekannt, die Rufnummer oder eine andere Kennung des zu ermittelnden Anschlusses oder des zu ortenden Endgerätes,

3. Art, Umfang und Dauer der Maßnahme,

4. der Sachverhalt sowie

5. die Begründung.

Maßnahmen nach Absatz 2 ordnen die Präsidentin oder der Präsident des Landeskriminalamtes oder einer Polizeidirektion oder von diesen hierzu beauftragte Bedienstete an. Die Maßnahmen sind schriftlich anzuordnen und zu begründen. In der Anordnung sind insbesondere die zur Identifizierung der gefährdeten Person erforderlichen Daten und die Rufnummer oder eine andere spezifische Kennung des zu ortenden Endgerätes anzugeben, soweit diese Daten vorliegen.“

20. § 69 wird gestrichen.

21. Die §§ 70 und 71 werden durch die folgenden §§ 70 und 71 ersetzt:

„§ 70

Erhebung von Bestandsdaten

(1) Die Polizei kann von einem Diensteanbieter oder einem Anbieter nach § 2 Absatz 1 Satz 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes Auskunft über Bestandsdaten verlangen gemäß

1. § 3 Nummer 6 des Telekommunikationsgesetzes (§ 174 Absatz 1 Satz 1 des Telekommunikationsgesetzes) sowie

2. § 2 Absatz 2 Nummer 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (§ 22 Absatz 1 Satz 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes),

sofern dies zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist. Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder Speichereinrichtungen geschützt wird, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, darf die Auskunft nur verlangt werden, wenn in den Fällen

1. gemäß § 174 Absatz 1 Satz 2 des Telekommunikationsgesetzes auch die gesetzlichen Voraussetzungen zur Nutzung dieser Daten vorliegen,

2. gemäß § 23 Absatz 2 Nummer 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes im Einzelfall die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen und dies erforderlich ist zur Abwehr einer konkreten Gefahr für

   a) Leib, Leben oder Freiheit einer Person,

   b) die sexuelle Selbstbestimmung,

   c) den Bestand des Bundes oder eines Landes,

   d) die freiheitlich demokratische Grundordnung oder

   e) Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 174 Absatz 1 Satz 3 des Telekommunikationsgesetzes, § 22 Absatz 1 Satz 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes), soweit dies erforderlich ist für den Bestand oder die Sicherheit des Bundes oder eines Landes, zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder für Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt oder deren Erhaltung im öffentlichen Interesse geboten istt.

(3) Maßnahmen nach Absatz 1 Satz 2 bedürfen einer richterlichen Anordnung auf Antrag der Polizei. Einer richterlichen Anordnung bedarf es nicht soweit die betroffene Person von dem Auskunftsverlangen bereits Kenntnis hat oder haben muss und im Fall des Absatzes 1 Satz 2 die Nutzung der Daten bereits durch eine richterliche Anordnung gestattet wird oder ohne richterliche Anordnung erfolgen kann; das Vorliegen der Voraussetzungen hierfür ist zu dokumentieren.

(4) Auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 hat der Diensteanbieter oder jeder Anbieter nach § 2 Absatz 1 Satz 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes die zur Auskunftserteilung erforderlichen Daten unverzüglich und vollständig zu übermitteln. Für die Entschädigung gilt § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend.

§ 71

Einsatz von unbemannten Luftfahrtsystemen

(1) Die Polizei kann bei den nachfolgenden Maßnahmen Daten unter den dort genannten Voraussetzungen auch durch den Einsatz unbemannter Luftfahrtsysteme erheben:

1. Datenerhebung nach § 56,

2. offene Beobachtung und Aufzeichnung mittels Bildübertragung nach § 57 Absatz 1 bis 3 und Absatz 9,

3. Datenerhebung durch Observation und Einsatz technischer Mittel nach § 63 Absatz 1 und 2,

4. Datenerhebung durch Einsatz technischer Mittel in Wohnungen nach § 65 Absatz 1,

5. Datenerhebung durch Telekommunikationsüberwachung nach § 66 Absatz 1 und 2 sowie

6. Datenerhebung durch den verdeckten Einsatz technischer Mittel zur Standorterhebung nach § 68 Absatz 2.

In den Fällen des Satzes 1 Nummer 1 dürfen unbemannte Luftfahrtsysteme nur dann eingesetzt werden, wenn die Offenheit der Maßnahme gewahrt bleibt. In diesen Fällen soll auf die Verwendung unbemannter Luftfahrtsysteme gesondert hingewiesen werden.

(2) Soweit in den Fällen des Absatz 1 eine richterliche Anordnung erforderlich ist, muss diese auch den Einsatz von unbemannten Luftfahrtsystemen umfassen. Unbemannte Luftfahrtsysteme dürfen nicht bewaffnet werden.“

22. § 72 wird gestrichen.

23. Die §§ 73 bis 75 werden durch die folgenden §§ 73 bis 75 ersetzt:

„§ 73

Anordnung, gerichtliche Zuständigkeit

(1) Für gerichtliche Entscheidungen nach diesem Gesetz gelten die folgenden Absätze.

(2) Zuständig ist das Amtsgericht, in dessen Bezirk die zuständige Polizeidienststelle ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Buches 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.

(3) Anordnungen zu den Befugnissen nach § 57a Absatz 1 Satz 4 und Absatz 2, § 60 Absatz 3 Satz 3, § 62 sowie § 62b Absatz 1 Satz 4 und Absatz 2 ergehen schriftlich und müssen den zugrunde liegenden Sachverhalt und die wesentlichen Gründe enthalten. Sie haben die von der Maßnahme betroffenen Personen oder Gegenstände sowie Art, Dauer und Umfang der Maßnahme zu bestimmen. Die Maßnahmen sind auf höchstens drei Monate zu befristen; eine Verlängerung durch das zuständige Gericht

um jeweils nicht mehr als den Anordnungszeitraum ist zulässig, sofern die Voraussetzungen für die Maßnahme noch vorliegen. Die Regelungen in § 21 Absatz 2 Satz 4 und 5, § 57a Absatz 2 Satz 3, § 60 Absatz 3 Satz 1 bis 3 sowie § 65 Absatz 4 Satz 3 und 4 bleiben unberührt.

(4) Anordnungen nach Absatz 3 Satz 1 können bei Gefahr im Verzug durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion getroffen werden; mit Ausnahme der Befugnis nach § 65 Absatz 4 auch durch von diesen hierzu beauftragte Bedienstete. Im Fall einer solchen Anordnung ist die richterliche Bestätigung unverzüglich nachzuholen. Bei Maßnahmen nach § 57a Absatz 1 Satz 4 und Absatz 2 ist die richterliche Bestätigung innerhalb von 24 Stunden nachzuholen. Die Maßnahme ist zu beenden und die bereits gespeicherten personenbezogenen Daten sind unverzüglich zu löschen, wenn die richterliche Bestätigung abgelehnt wird oder nicht innerhalb von drei Tagen erfolgt.

(5) Für polizeiliche Anordnungen nach den § 21 Absatz 2 sowie den §§ 57a, 61, und 62b bis 68 gilt Absatz 3 entsprechend.

§ 74

Benachrichtigungspflichten

(1) Über eine Maßnahme sind nach deren Abschluss unverzüglich zu benachrichtigen:

1. im Fall des § 57a Absatz 1 Satz 4 oder Absatz 2 die Zielperson,

2. im Fall des § 58 die Personen, gegen die im Trefferfall gemäß § 58 Absatz 3 Satz 3 weitere Maßnahmen angeordnet wurden,

3. im Fall des § 60

   a) die zur verdeckten Kontrolle, zur Ermittlungsanfrage und zur gezielten Kontrolle ausgeschriebenen Personen sowie

   b) die Personen, deren personenbezogene Daten infolge einer auf der Ausschreibung beruhenden Maßnahme übermittelt wurden,

4. im Fall des § 62 die Personen, gegen die nach Auswertung der durch die Rasterfahndung erlangten Daten weitere Maßnahmen getroffen wurden,

5. im Fall des § 62b die Zielperson,

6. im Fall des § 63

   a) die Zielperson und

   b) die erheblich mitbetroffenen Personen,

7. im Fall des § 64

   a) die Zielperson,

   b) die erheblich mitbetroffenen Personen und

   c) die Personen, deren nicht allgemein zugängliche Wohnung die Verdeckte Ermittlerin, der Verdeckte Ermittler oder die V-Person betreten hat,

8. im Fall des § 65

   a) die Zielperson,

   b) die erheblich mitbetroffenen Personen sowie

   c) die Eigentümer und Bewohner der überwachten Wohnung,

9. im Fall des § 66 die Beteiligten der überwachten Telekommunikation,

10. im Fall des § 66a die Zielperson,

11. im Fall der Erhebung von Verkehrsdaten nach § 67 Absatz 1 Satz 2 die Beteiligten der betroffenen Telekommunikation,

12. im Fall der Erhebung von Nutzungsdaten nach § 67 Absatz 1 Satz 2 der Nutzer,

13. im Fall des § 68 die Zielperson, soweit sie nicht von der Maßnahme Kenntnis erlangt hat sowie

14. im Fall des § 70 die Zielperson, sofern eine richterliche Anordnung der Bestandsdatenerhebung nach § 70 Absatz 3 erforderlich ist.

Die Benachrichtigung hat die Angaben nach § 12 Absatz 1 des Sächsischen Datenschutz-Umsetzungsgesetzes zu enthalten.

(2) Die Benachrichtigung einer Person nach Absatz 1 Satz 1 Nummer 9 oder Nummer 11, gegen die sich die Maßnahme nicht gerichtet hat, unterbleibt, wenn diese von der Maßnahme nur unerheblich betroffen ist und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Eine Benachrichtigung unterbleibt, wenn die Feststellung der Identität aus den Gründen des § 75 Absatz 3 Satz 1 unterblieben ist.

(3) Die Benachrichtigung wird zurückgestellt, sofern

1. ihr eine Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, entgegensteht,

2. der Zweck der Maßnahme durch sie gefährdet wird oder

3. dadurch die Möglichkeit einer konkret absehbaren weiteren Verwendung der Verdeckten Ermittlerin, des Verdeckten Ermittlers oder der V-Person gewahrt bleibt.

Nach Wegfall des Hinderungsgrundes ist die Benachrichtigung nachzuholen. Wurde wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen die betroffene Person eingeleitet, entscheidet die Strafverfolgungsbehörde entsprechend den Vorschriften der Strafprozessordnung über die Zurückstellung; für das weitere Verfahren gilt § 101 Absatz 6 der Strafprozessordnung. Die Entscheidung hierüber und über die Zurückstellung gemäß Satz 1 ist mit Begründung zu dokumentieren.

(4) Erfolgt die nach Absatz 3 zurückgestellte Benachrichtigung nicht innerhalb von sechs Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der gerichtlichen Zustimmung. Über die Zurückstellung und ihre Dauer entscheidet das Gericht, das für die Anordnung der Maßnahme zuständig gewesen ist oder wäre, in den übrigen Fällen das Gericht am Sitz der zuständigen Polizeidienststelle. Im Falle des § 65 darf die Dauer der Zurückstellung sechs Monate nicht überschreiten.

(5) Eine Benachrichtigung der betroffenen Person kann mit richterlicher Zustimmung für eine längere Dauer zurückgestellt werden oder endgültig unterbleiben, wenn die Maßnahme

1. für diese keine weiteren Folgen hatte, insbesondere, weil keine personenbezogenen Daten aufgezeichnet wurden und die Unterrichtung den Grundrechtseingriff weiter vertiefen würde,

2. die betroffene Person nur unerheblich betroffen hat und anzunehmen ist, dass diese kein Interesse an einer Benachrichtigung hat, oder

3. sich gegen die betroffene Person nicht gerichtet hat und

   a) überwiegende Interessen einer anderen betroffenen Person entgegenstehen oder

   b) deren Identität oder Aufenthaltsort nicht oder nur mit unverhältnismäßigem Aufwand ermittelt werden kann.

§ 75

Besondere Protokollierungspflichten

(1) Bei der Erhebung von Daten nach den §§ 57a bis 68 sowie nach § 70 Absatz 1 Satz 2 und Absatz 2 sind zu protokollieren:

1. der Zeitpunkt des Einsatzes (Beginn und Ende sowie Zeiten der Unterbrechung),

2. die Bezeichnung des zur Datenerhebung eingesetzten Mittels,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, welche die Maßnahme durchführt.

(2) Zu protokollieren sind auch:

1. bei Maßnahmen nach § 57a Absatz 1 Satz 4 und Absatz 2 die Personen, gegen die im Trefferfall weitere Maßnahmen angeordnet wurden,

2. bei Maßnahmen nach § 58 die Personen, gegen die im Trefferfall nach § 58 Absatz 3 Satz 3 weitere Maßnahmen angeordnet wurden,

3. bei Maßnahmen nach § 60 die ausgeschriebenen Personen und die Personen, deren personenbezogene Daten infolge einer auf der Ausschreibung beruhenden Maßnahme übermittelt wurden,

4. bei Maßnahmen nach § 62

   a) die im Übermittlungsersuchen nach § 62 Absatz 3 enthaltenen Merkmale und

   b) die Personen, gegen die nach Auswertung der durch die Rasterfahndung erlangten Daten weitere Maßnahmen getroffen wurden,

5. bei Maßnahmen nach § 62b die Zielpersonen, gegen die im Trefferfall weitere Maßnahmen angeordnet wurden,

6. bei Maßnahmen nach § 63 die Zielperson und die erheblich mitbetroffenen Personen,

7. bei Maßnahmen nach § 64

   a) die Zielperson,

   b) die erheblich mitbetroffenen Personen und

   c) die Personen, deren nicht allgemein zugängliche Wohnung die Verdeckte Ermittlerin, der Verdeckte Ermittler oder die V-Person betreten hat,

8. bei Maßnahmen nach § 65

   a) die Zielperson,

   b) die erheblich mitbetroffenen Personen,

   c) Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten, und

   d) die Bezeichnung der überwachten Wohnung,

9. bei Maßnahmen nach § 66 die Beteiligten der überwachten Telekommunikation,

10. bei Maßnahmen nach § 66a die Zielperson, im Fall von § 66a Absatz 3 die Zielperson und der räumliche Umfang der Maßnahme,

11. bei der Erhebung von Verkehrsdaten nach § 67 Absatz 1 Satz 2 die Beteiligten der betroffenen Telekommunikation,

12. bei Erhebung von Nutzungsdaten nach § 67 Absatz 1 Satz 2 der Nutzer,

13. bei Maßnahmen nach § 68 die Zielperson sowie

14. bei Maßnahmen nach § 70 Absatz 1 Satz 2 die Zielperson.

(3) Nachforschungen zur Feststellung der Identität einer Person nach Absatz 2 sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität und der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist. Die Zahl der Personen, deren Dokumentation unterblieben ist, ist im Protokoll anzugeben.

(4) Die Protokolldaten dürfen nur verwendet werden, um die betroffene Person nach § 74 Absatz 1 zu benachrichtigen und ihr oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahmen rechtmäßig durchgeführt worden sind. Sie sind sechs Monate nach der Benachrichtigung nach § 74 oder sechs Monate nach Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung zu löschen. Ist die Datenschutzkontrolle nach § 94 noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.“

24. In § 76 Absatz 2 Satz 3 wird die Angabe „§ 61 Absatz 3“ durch die Angabe „§ 61 Absatz 2“ ersetzt.

25. § 78 wird wie folgt geändert:

a) In Absatz 1 Satz 1 wird die Angabe „§§ 59, 62 bis 71“ durch die Angabe „§§ 62 bis 68 und 70“ ersetzt.

b) In Absatz 3 wird die Angabe „71“ durch die Angabe „70“ ersetzt.

26. Die §§ 79 und 80 werden durch die folgenden §§ 79 bis 80d ersetzt:

„§ 79

Befugnis zur Datenverarbeitung

(1) Die Polizei kann personenbezogene Daten verarbeiten, soweit dies zur jeweiligen Aufgabenerfüllung erforderlich ist und dieses Gesetz oder andere Rechtsvorschriften keine zusätzlichen besonderen Voraussetzungen vorsehen.

(2) Die Polizei kann personenbezogene Daten zur Vorgangsverwaltung oder zur befristeten Dokumentation behördlichen Handelns speichern und ausschließlich zu diesem Zweck verarbeiten.

(3) Soweit gesetzliche Regelungen die Einrichtung eines Informationsverbundes unter Beteiligung der Polizei vorsehen, kann sie nach Maßgabe dieses Gesetzes personenbezogene Daten in Dateisystemen des Informationsverbundes verarbeiten.

(4) Soweit zu einer Person bereits Daten vorhanden sind, kann die Polizei zu dieser Person auch personengebundene Hinweise verarbeiten, die zum Schutz dieser Person oder zum Schutz der Bediensteten der Polizei erforderlich sind, oder weitere Hinweise, die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen. Soweit es sich hierbei um besondere Kategorien von personenbezogenen Daten handelt, sind die Vorgaben des § 54 zu beachten.

§ 79a

Zweckbindung, Zweckänderung, Hypothetische Datenneuerhebung

(1) Die Polizei kann personenbezogene Daten, die sie selbst erhoben hat, weiterverarbeiten, wenn dies unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift erforderlich ist

1. zur Erfüllung derselben Aufgabe und

2. zum Schutz derselben Rechtsgüter oder zur Verhütung oder Verfolgung derselben Straftaten.

Satz 1 gilt entsprechend für personenbezogene Daten, denen keine Erhebung vorausgegangen ist, mit der Maßgabe, dass für die Weiterverarbeitung der Zweck der Speicherung zu berücksichtigen ist. Für die weitere Verarbeitung von personenbezogenen Daten, die aus Maßnahmen nach § 65 Absatz 1 und 2 erlangt wurden, muss im Einzelfall eine Gefahrenlage im Sinne des § 65 Absatz 1 Satz 1 oder Absatz 2 Satz 2 vorliegen.

(2) Die Polizei kann zur Erfüllung ihrer Aufgaben personenbezogene Daten zu anderen Zwecken, als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, soweit dies erforderlich ist und wenn unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift

1. mindestens

   a) vergleichbar schwerwiegende Straftaten oder Ordnungswidrigkeiten verhütet oder verfolgt werden sollen oder

   b) vergleichbar bedeutsame Rechtsgüter geschützt werden sollen und

2. sich im Einzelfall konkrete Ermittlungsansätze

   a) zur Verhütung solcher Straftaten oder Ordnungswidrigkeiten ergeben oder

   b) zur Abwehr von in absehbarer Zeit drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter erkennen lassen,

   und Vorschriften dieses Gesetzes oder andere Rechtsvorschriften die zweckändernde Weiterverarbeitung nicht besonders regeln.

(3) Für die Weiterverarbeitung von personenbezogenen Daten, die durch eine Maßnahme nach § 65 Absatz 1 und 2 erlangt wurden, gilt Absatz 2 Nummer 2 Buchstabe b mit der Maßgabe, dass im Einzelfall eine Gefahrenlage im Sinne des § 65 Absatz 1 Satz 1 oder Absatz 2 Satz 2 vorliegen muss. Personenbezogene Daten, die durch Herstellung von Lichtbildern oder Bildaufzeichnungen über eine Person im Wege eines verdeckten Einsatzes technischer Mittel in oder aus Wohnungen erlangt wurden, dürfen nicht zu Strafverfolgungszwecken weiterverarbeitet werden. Für die Weiterverarbeitung erlangter personenbezogener Daten, die durch einen Eingriff in informationstechnische Systeme durch die Polizei eines anderen Landes oder des Bundes erhoben wurden, muss im Einzelfall eine Gefahrenlage im Sinne des § 49 Absatz 1 des Bundeskriminalamtgesetzes vorliegen.

(4) Die Polizei kann der Identifizierung einer Person dienende Daten wie insbesondere Namen, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit und Anschrift auch dann zur Identifizierung dieser Person weiterverarbeiten, wenn die Voraussetzungen von Absatz 2 nicht erfüllt sind.

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

§ 79b

Weiterverarbeitung zu Aus- und Fortbildungszwecken, zu statistischen, archivarischen oder wissenschaftlichen Zwecken, Weiterverarbeitung von Vorgangsverwaltungs- und Protokolldaten

(1) Die Polizei und die Hochschule der Sächsischen Polizei (FH) können personenbezogene Daten zur polizeilichen Aus- und Fortbildung oder zu statistischen Zwecken weiterverarbeiten, soweit eine Weiterverarbeitung anonymisierter Daten zu diesem Zweck nicht möglich ist und jeweils die berechtigten Interessen der oder des Betroffenen an der Geheimhaltung der Daten nicht überwiegen.

(2) Die Polizei kann personenbezogene Daten einer Person, bei der tatsächliche Anhaltspunkte dafür vorliegen, dass sie beabsichtigt, die Begehung von Straftaten durch andere Personen zu unterstützen, zu fördern, vorzubereiten oder zu planen, zum Zweck der Gefahrenvorsorge weiterverarbeiten.

(3) Die Polizei kann personenbezogene Daten zu im öffentlichen Interesse liegenden archivarischen oder wissenschaftlichen Forschungszwecken nach Maßgabe des § 6 des Sächsischen Datenschutz-Umsetzungsgesetzes weiterverarbeiten.

(4) Die Polizei kann personenbezogene Daten, die ausschließlich zum Zweck der Vorgangsverwaltung, der zeitlich befristeten Dokumentation behördlichen Handelns oder gemäß § 32 Absatz 1 des Sächsischen Datenschutz-Umsetzungsgesetzes zu Zwecken der Protokollierung gespeichert worden sind, nach Anordnung durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion zum Zweck der Abwehr von Gefahren für Leben, Gesundheit oder Freiheit einer Person oder für bedeutende Sach- oder Vermögenswerte sowie zur Verhütung von Straftaten von erheblicher Bedeutung weiterverarbeiten. Die Anordnung ist schriftlich zu begründen. Die oder der Sächsische Datenschutz- und Transparenzbeauftragte ist unverzüglich über die Datenverarbeitung gemäß Satz 1 zu unterrichten.

§ 79c

Training und Test von lernenden IT-Systemen

(1) Die Polizei darf zum Trainieren und Testen von lernenden IT-Systemen, die sie für die eigene Aufgabenwahrnehmung entwickelt oder nutzt, soweit erforderlich bei ihr vorhandene personenbezogene Daten nach Maßgabe der Absätze 2 bis 5 weiterverarbeiten und dafür auch an Dritte oder Auftragsverarbeiter übermitteln. Es ist dabei sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Soweit technisch möglich, muss die Nachvollziehbarkeit des verwendeten Verfahrens sichergestellt werden. Die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen nach § 65 Absatz 1 oder durch Überwachung und Aufzeichnung von Telekommunikation nach § 66 Absatz 1 und 2 erhoben wurden, ist unzulässig.

(2) Personenbezogene Daten sind für die Verwendung zu Test- oder Trainingszwecken zu anonymisieren. Kann der Zweck des Tests oder Trainings mit anonymisierten Daten nicht erreicht werden oder ist die Anonymisierung nur mit unverhältnismäßigem Aufwand möglich, sind sie zu pseudonymisieren. Kann der Zweck des Tests oder Trainings mit pseudonymisierten Daten nicht erreicht werden oder ist die Pseudonymisierung nur mit unverhältnismäßigem Aufwand möglich, dürfen personenbezogene Daten zum Zweck des Tests oder Trainings verarbeitet werden. Besondere Kategorien personenbezogener Daten dürfen unter Gewährleistung von Garantien im Sinne des § 4 Absatz 2 des Sächsischen Datenschutz-Umsetzungsgesetzes zum Zweck des Tests oder Trainings verwendet werden.

(3) Personenbezogene Daten dürfen zum Testen und Trainieren von lernenden IT-Systemen nur an Auftragsverarbeiter übermittelt werden, wenn eine Verarbeitung bei der Polizei selber nur mit unverhältnismäßigem Aufwand möglich ist. An Dritte dürfen die Daten nur übermittelt werden, wenn eine Verarbeitung durch die Polizei auch unter Zuhilfenahme eines Auftragsverarbeiters nur mit unverhältnismäßigem Aufwand möglich ist. Sofern personenbezogene Daten zum Testen oder Trainieren von lernenden IT-Systemen an Dritte oder im Wege der Auftragsverarbeitung übermittelt werden, ist die Übermittlung von personenbezogenen Daten unzulässig, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen nach § 65 Absatz 1 oder durch Überwachung und Aufzeichnung von Telekommunikation nach § 66 Absatz 1 und 2 erhoben wurden.

(4) Personenbezogene Daten dürfen nur an solche Personen übermittelt werden, die Amtsträgerinnen oder Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2 und

3 sowie Absatz 4 Nummer 2 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(5) Auftrags- und Drittverarbeiter dürfen die übermittelten Daten nur im Rahmen des jeweiligen Trainings und der jeweiligen Tests verarbeiten. Sie sind verpflichtet, die Daten nach Abschluss von Training und Test des lernenden Systems wieder zu löschen. Sie dürfen die trainierten Modelle für eigene Zwecke weiternutzen, wenn die Polizei dies genehmigt und sichergestellt werden kann, dass aus den trainierten Modellen keine Trainingsdaten abgeleitet werden können.

(6) Für das Testen oder Trainieren von lernenden IT-Systemen hat das Staatsministerium des Innern in einer nach Anhörung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten zu erlassenden Verwaltungsvorschrift das Nähere zu dem Verfahren zu regeln und insbesondere zu bestimmen

1. Art und Umfang der zu verarbeitenden Daten,

2. den Personenkreis, der von der Verarbeitung betroffen ist,

3. ein Verfahren, das die Einhaltung der maßgeblichen fachlichen und rechtlichen Anforderungen an das Training und den Test von lernenden IT-Systemen sicherstellt,

4. Sicherungsmaßnahmen zur Datenaktualität und -qualität,

5. Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe,

6. die Mindeststandards zur technischen Durchführung der Anonymisierung und Pseudonymisierung von Daten sowie die Beschreibung eines etwaigen unverhältnismäßigen Aufwands im Sinne von Absatz 2 Satz 2 und 3 und Absatz 3 Satz 1 und 2,

7. die Lösch- und Protokollierungspflichten sowie

8. die Entscheidungsträger.

§ 80

Vorsorgende Speicherung von personenbezogenen Daten zu Verurteilten, Beschuldigten, Verdächtigen und Anlasspersonen

(1) Die Polizei kann, soweit Bestimmungen der Strafprozessordnung nicht entgegenstehen, personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten gewonnen hat, zur künftigen Verhütung oder Verfolgung von Straftaten vorsorgend speichern von:

1. Verurteilten,

2. Beschuldigten,

3. Personen, die einer Straftat verdächtig sind, und

4. Personen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden (Anlasspersonen).

Zu Personen nach Satz 1 Nummer 1 bis 3 darf eine vorsorgende Speicherung nur erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse eine hinreichende Wahrscheinlichkeit dafür besteht, dass die betroffene Person Straftaten begehen wird und gerade die Weiterverarbeitung der gespeicherten Daten zu deren Verhütung oder Verfolgung erforderlich ist.

(2) Zu den in Absatz 1 bezeichneten Personen kann die Polizei vorsorgend speichern:

1. die Grunddaten gemäß § 1 Absatz 1 der BKA-Daten-Verordnung vom 4. Juni 2010 (BGBl. I S. 716), die zuletzt durch Artikel 6 Absatz 12 des Gesetzes vom 13. April 2017 (BGBl. I S. 872) geändert worden ist,

2. soweit erforderlich, andere zur Identifizierung geeignete Merkmale gemäß § 1 Absatz 2 der BKA-Daten-Verordnung,

3. die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer,

4. die Tatzeiten und Tatorte sowie

5. die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten.

Von Personen nach Absatz 1 Nummer 1 und 2 können weitere personenbezogene Daten gemäß § 2 der BKA-Daten-Verordnung vorsorgend gespeichert werden. Von Personen nach Absatz 1 Satz 2 können, soweit erforderlich, weitere personenbezogene Daten gespeichert werden.

(3) Wird eine Beschuldigte oder ein Beschuldigter rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen sie oder ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt, sind die Daten zu löschen, wenn sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat.

(4) Für die weitere Verarbeitung der Daten nach Absatz 2 gilt § 79a Absatz 2.

§ 80a

Vorsorgende Speicherung von personenbezogenen Daten zu Zeuginnen und Zeugen, Opfern, Hinweisgeberinnen und -gebern, Kontakt- und Begleitpersonen

(1) Die Polizei kann, soweit es zur Verhütung oder zur Vorsorge für die Verfolgung einer Straftat von erheblicher Bedeutung erforderlich ist, personenbezogene Daten von Personen vorsorgend speichern, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass

1. sie bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen,

2. sie als Opfer einer künftigen Straftat in Betracht kommen,

3. es sich um Hinweisgeberinnen und -geber und sonstige Auskunftspersonen handelt oder,

4. es sich um Kontakt- und Begleitpersonen der Personen nach § 80 Absatz 1 Nummer 1 bis 3 handelt.

Die vorsorgende Speicherung zu Personen nach Satz 1 Nummer 1 bis 3 darf ohne Einwilligung der Person nur dann erfolgen, wenn das Bekanntwerden der Speicherungsabsicht den mit der Speicherung verfolgten Zweck gefährden würde.

(2) Zu Personen nach Absatz 1 Satz 1 Nummer 1 bis 3 dürfen nur die in § 80 Absatz 2 Satz 1 bezeichneten Daten vorsorgend gespeichert werden, sowie die Angabe, in Bezug auf welche Eigenschaft der Person im Sinne von Absatz 1 Satz 1 Nummer 1 bis 3 und in Bezug auf welchen Sachverhalt die vorsorgende Speicherung der Daten erfolgt. Zu Personen nach Absatz 1 Satz 1 Nummer 4 dürfen nur die in § 80 Absatz 2 Satz 1 und Satz 3 bezeichneten Daten vorsorgend gespeichert werden.

(3) Für die weitere Verarbeitung der Daten nach Absatz 2 gilt § 79a Absatz 2.

§ 80b

Vorsorgende Speicherung von zu Gefahrenabwehrzwecken erhobenen Daten

(1) Die Polizei kann personenbezogene Daten, die sie auf der Grundlage dieses Gesetzes erhoben hat

1. zu gefährdeten, hilflosen oder vermissten Personen vorsorgend speichern, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass wegen der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse eine hinreichende Wahrscheinlichkeit dafür besteht, dass die vorsorgende Speicherung der Daten zur Abwehr einer Gefahr für die betroffene Person erforderlich ist, oder

2. zu Anlasspersonen vorsorgend speichern, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass diese in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden und die vorsorgende Speicherung der Daten zur Verhütung von Straftaten von erheblicher Bedeutung erforderlich ist.

Zu Personen nach Satz 1 Nummer 1 dürfen die in § 80 Absatz 2 Satz 1 Nummer 1 und 2 bezeichneten Daten, zu Personen nach Satz 1 Nummer 2 die in § 80 Absatz 2 Satz 1 bis 3 bezeichneten Daten vorsorgend gespeichert werden.

(2) Für die weitere Verarbeitung der Daten nach Absatz 1 Satz 1 Nummer 1 gilt § 79a Absatz 1, für die weitere Verarbeitung der Daten nach Absatz 1 Satz 1 Nummer 2 gilt § 79a.

§ 80c

Vorsorgende Speicherung von personenbezogenen Daten zu sonstigen Personen

Zu Personen nach den §§ 80 bis 80b können Daten von Erziehungsberechtigten, Vormündern und Bewährungshelferinnen und -helfern (sonstige Personen) vorsorgend gespeichert werden, soweit dies im Zusammenhang mit der vorsorgenden Speicherung einer Person nach den §§ 80 bis 80b erforderlich ist. Die Speicherung der Daten sonstiger Personen darf nicht recherchefähig erfolgen. Zu sonstigen Personen dürfen vorsorgend gespeichert werden nur der Name, das Geburtsdatum, Adressdaten und Daten zur Erreichbarkeit sowie die Angabe, in Bezug auf welche Eigenschaft der Person im Sinne von Satz 1 und in Bezug auf welchen Sachverhalt deren Speicherung erfolgt. Für die weitere Verarbeitung der Daten nach Satz 1 gilt § 79a Absatz 2.

§ 80d

Dauer der Speicherung, Aussonderungsprüffristen, Höchstspeicherfristen

(1) Personenbezogene Daten dürfen solange gespeichert werden, wie dies für die Erfüllung der konkreten Aufgabe und des Zwecks, zu dem sie erhoben worden sind, erforderlich ist. Die Dauer der Speicherung ist auf das erforderliche Maß zu beschränken. Hierzu sind Fristen festzulegen, zu denen spätestens zu prüfen ist, ob die Speicherung für die Erfüllung der Aufgaben noch erforderlich ist (Aussonderungsprüffristen). Die Aussonderungsprüffristen dürfen bei Erwachsenen fünf Jahre, bei Jugendlichen drei Jahre und bei Kindern zwei Jahre nicht überschreiten und beginnen an dem Tag, an dem die Polizei Kenntnis von dem Ereignis erlangt hat.

(2) Bei der Festlegung von Aussonderungsprüffristen für gemäß § 80 vorsorgend gespeicherte personenbezogene Daten sind insbesondere die Art und Schwere der zugrundeliegenden Straftat und die Herkunft der Daten zu berücksichtigen.

(3) Die Aussonderungsprüffristen für vorsorgend gespeicherte personenbezogene Daten dürfen nicht überschreiten in Bezug auf Personen nach:

1. § 80 Absatz 1 Nummer 1 bei Erwachsenen 10 Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre,

2. § 80 Absatz 1 Nummer 2 und 3

   a) in Bezug auf schwere Straftaten nach § 100a Absatz 2 der Strafprozessordnung bei Erwachsenen fünf Jahre, bei Jugendlichen 4 Jahre und bei Kindern 2 Jahre,

   b) in Bezug auf sonstige Straftaten bei Erwachsenen drei Jahre, bei Jugendlichen zwei Jahre und bei Kindern ein Jahr.

3. § 80 Absatz 1 Nummer 4 und 80b Absatz 2 bei Erwachsenen zwei Jahre, bei Jugendlichen und Kindern ein Jahr,

4. § 80a Absatz 1 Nummer 1 bis 3, soweit die Speicherung

   a) ohne Einwilligung erfolgt ist, ein Jahr;

   b) mit Einwilligung erfolgt ist, bei Erwachsenen fünf Jahre, bei Jugendlichen drei Jahre,

5. § 80a Absatz 1 Nummer 4 in Bezug auf

   a) schwere Straftaten nach § 100a Absatz 2 der Strafprozessordnung bei Erwachsenen fünf Jahre und bei Jugendlichen drei Jahre,

   b) sonstige Straftaten bei Erwachsenen drei Jahre und bei Jugendlichen zwei Jahre,

6. § 80b Absatz 1

   a) im Hinblick auf Personen nach § 80b Absatz 1 Nummer 1 für Erwachsene fünf Jahre und für Kinder drei Jahre

   b) im Hinblick auf Personen nach § 80b Absatz 1 Nummer 2 bei Erwachsenen drei Jahre und bei Jugendlichen zwei Jahre.

7. § 80c zwei Jahre.

Abweichend von der in Satz 1 Nummer 2 Buchstabe a bestimmten Frist gilt, dass im Fall einer Erstspeicherung diese bei Erwachsenen nicht länger als drei Jahre, bei Jugendlichen nicht länger als zwei Jahre und bei Kindern nicht länger als ein Jahr betragen darf. Die Aussonderungsprüffristen nach Satz 1 beginnen an dem Tag, an dem die vorsorgende Speicherung erfolgt ist, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder der Beendigung einer mit der Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung.

(4) Liegen bei Ablauf der nach Absatz 3 Satz 1 bestimmten Aussonderungsprüffrist weiterhin relevante Umstände vor oder sind neue relevante Umstände hinzugetreten, kann eine erneute Aussonderungsprüffrist nach Absatz 3 Satz 1 bestimmt werden; anderenfalls sind die Daten zu löschen. In den Fällen des

1. Absatz 3 Satz 1 Nummer 2 Buchstabe b kann die Aussonderungsprüffrist höchstens zweimal verlängert werden,

2. Absatz 3 Satz 1 Nummer 4 Buchstabe a kann die Aussonderungsprüffrist um ein Jahr verlängert werden.

In den Fällen des Absatzes 3 Satz 1 Nummer 4 Buchstabe a darf die Aussonderungsprüffrist insgesamt drei Jahre nicht überschreiten.

(5) Das Staatsministerium des Innern hat das Nähere zum Verfahren in einer nach Anhörung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten zu erlassenden Verwaltungsvorschrift zu regeln und insbesondere zu bestimmen

1. von der vorsorgenden Speicherung ausgenommene Sachverhalte,

2. Anforderungen an die erforderliche Prüfung, die Zulässigkeit und den Umfang der vorsorgenden Speicherungen nach den §§ 80 bis 80c,

3. Anforderungen an die erstmalige Festsetzung, die Verlängerung und an Ausnahmen von der Verlängerung von Aussonderungsprüffristen nach den Absätzen 2 bis 4,

4. bestehende Löschungsverpflichtungen,

5. Anforderungen an die Dokumentationspflichten der Entscheidung, die der vorsorgenden Speicherung zugrunde liegt, und zur Bestimmung und Verlängerung von Aussonderungsprüffristen,

6. ein Verfahren, das durch technische und organisatorische Vorkehrungen die Einhaltung der rechtlichen Anforderungen an

   a) die vorsorgende Speicherung,

   b) die Festsetzung und die Verlängerung von Aussonderungsprüffristen,

   c) die Einhaltung von Löschungspflichten und

   d) die Einhaltung von Dokumentationspflichten

   gewährleistet.“

27. § 81 wird wie folgt geändert:

a) In Absatz 1 Satz 1 Nummer 3 Buchstabe b wird nach der Angabe „Verhütung“ die Angabe „oder Verfolgung“ eingefügt.

b) Absatz 4 Satz 2 wird gestrichen.

28. Die §§ 83 und 84 werden durch die folgenden §§ 83, 84 und 84a ersetzt:

„§ 83

Übermittlungsverbote und Verweigerungsgründe

Übermittlungen nach den Vorschriften dieses Gesetzes haben zu unterbleiben,

1. wenn für die übermittelnde Stelle erkennbar ist, dass unter Berücksichtigung der Art der Daten und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person das Allgemeininteresse an der Übermittlung überwiegen, oder

2. besondere Verwendungsregelungen entgegenstehen; die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

Die Datenübermittlung unterbleibt darüber hinaus,

1. wenn hierdurch wesentliche Sicherheitsinteressen des Bundes oder der Länder 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 steht; die verantwortliche Polizeidienststelle hat die Entscheidung auf der Grundlage der vom Bundeskriminalamt gemäß § 28 Absatz 3 des Bundeskriminalamtgesetzes zu führenden Aufstellung über die Einhaltung der elementaren rechtsstaatlichen Grundsätze und Menschenrechtsstandards sowie das Datenschutzniveau in Drittstaaten zu treffen.

§ 84

Datenübermittlung im innerstaatlichen Bereich

(1) Die Polizei kann unter Beachtung des § 79a Absatz 2 und 3 an die Polizeidienststellen anderer Länder oder des Bundes personenbezogene Daten übermitteln, soweit dies zur Erfüllung ihrer Aufgaben oder zur Erfüllung der Aufgaben des Empfängers erforderlich ist.

(2) Die Polizei kann an andere Stellen als die Behörden nach Absatz 1 personenbezogene Daten, die sie in Erfüllung ihrer Aufgaben erlangt hat, übermitteln, soweit dies

1. in anderen Rechtsvorschriften vorgesehen ist oder

2. nach § 79a Absatz 2 bis 4 zulässig und erforderlich ist

   a) zur Erfüllung ihrer Aufgaben,

   b) zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Strafvollstreckung oder zum Strafvollzug,

   c) zum Zweck der Gefahrenabwehr an die für die Gefahrenabwehr zuständigen öffentlichen Stellen,

   d) zur Aufgabenerfüllung der empfangenden Stelle, soweit durch besondere gesetzliche Regelung ein Datenübermittlungsersuchen vorgesehen ist und die Übermittlung der Daten durch die Polizei zur Aufgabenerfüllung der empfangenden Stelle erforderlich ist, oder

   e) zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner.

(3) Die Polizei kann von sich aus personenbezogene Daten an nichtöffentliche Stellen im Sinne des § 2 Absatz 4 des Bundesdatenschutzgesetzes übermitteln, soweit dies unter Beachtung des § 79a Absatz 2 bis 4 erforderlich ist zur

1. Erfüllung ihrer Aufgaben,

2. Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl,

3. Wahrung schutzwürdiger Interessen einzelner, soweit kein Grund zu der Annahme besteht, dass Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben, oder

4. zur Ermöglichung einer Kontaktaufnahme durch eine durch das Staatsministerium für Soziales, Gesundheit und Gesellschaftlichen Zusammenhalt bestimmte Beratungsstelle mit einer betroffenen Person, bei der auf Grund tatsächlicher Anhaltspunkte Bedarf für eine Beratung zum Schutz vor häuslicher Gewalt besteht.

Bei Übermittlungen nach Nummer 4 darf die Beratungsstelle die Daten ausschließlich und nur einmalig dazu nutzen, der betroffenen Person unverzüglich Beratung zur Verhütung weiterer Handlungen häuslicher Gewalt anzubieten. Lehnt die betroffene Person die Beratung ab, hat die Beratungsstelle die übermittelten Daten zu löschen.

(4) Auf Ersuchen einer nichtöffentlichen Stelle können personenbezogene Daten übermittelt werden, soweit diese

1. ein rechtliches Interesse an der Kenntnisnahme der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der betroffenen Person überwiegen, oder

2. ein berechtigtes Interesse geltend macht und offensichtlich ist, dass die Datenübermittlung im Interesse der betroffenen Person liegt und diese in Kenntnis der Sachlage ihre Einwilligung hierzu erteilen würde.

(5) Die empfangende Stelle darf die übermittelten Daten nur zu dem Zweck verarbeiten, zu dessen Erfüllung sie ihr übermittelt worden sind. Bei Übermittlungen an

nichtöffentliche Stellen hat die Polizei die empfangende Stelle darauf hinzuweisen. In den Fällen der Absätze 1 und 2 ist eine Verarbeitung zu anderen Zwecken unter Beachtung des § 79a Absatz 2 bis 4 zulässig. In den Fällen der Absätze 3 und 4 ist eine Verarbeitung zu anderen Zwecken nur zulässig, soweit eine Übermittlung nach Absatz 3 oder 4 zulässig wäre und nur, soweit die Polizeidienststelle zugestimmt hat.

(6) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung.

§ 84a

Öffentlichkeitsfahndung

Die Polizei kann Daten und Abbildungen zu einer Person zum Zweck der Ermittlung der Identität oder des Aufenthaltsortes öffentlich bekannt geben, soweit

1. die Abwehr einer Gefahr für Leib, Leben oder Freiheit dieser Person sonst nicht möglich ist oder wesentlich erschwert wird oder

2. von dieser Person eine Gefahr für Leib, Leben oder Freiheit anderer Personen ausgeht.“

29. § 86 wird durch folgenden § 86 ersetzt:

„§ 86

Aufzeichnung von Notrufen und Anrufen, Erhebung von Standortdaten

(1) Die Polizei kann von einem Diensteanbieter im Rahmen einer Notrufverbindung im automatisierten Verfahren übermittelte personenbezogene Daten verarbeiten, soweit dies für die Abwehr von Gefahren oder zur Verhütung von Straftaten erforderlich ist. Die Notrufverbindungen einschließlich der zugehörigen personenbezogenen Daten und der den Notruf begleitenden personenbezogenen Daten einschließlich Standortdaten können gespeichert werden.

(2) Die Polizei kann über sonstige Anrufe Aufzeichnungen fertigen, die über öffentlich bekanntgegebene Rufnummern eingehen, welche der Entgegennahme sachdienlicher Hinweise im Zusammenhang mit der Erfüllung ihrer Aufgaben dienen; auf die Aufzeichnungen ist hinzuweisen, soweit dadurch die Aufgabenerfüllung nicht gefährdet wird.

(3) Aufzeichnungen und dazugehörige gespeicherte Daten nach Absatz 1 oder 2 sind spätestens nach einem Monat zu löschen, soweit die weitere Verarbeitung nicht zur Abwehr einer Gefahr oder zur Verfolgung von Straftaten erforderlich ist. § 79b Absatz 1 bleibt unberührt.“

30. § 88 wird durch den folgenden § 88 ersetzt:

„§ 88

Zuverlässigkeitsüberprüfung zum Schutz von besonders gefährdeten Veranstaltungen

(1) Die Polizei kann zum Schutz einer besonders gefährdeten Veranstaltung auf Ersuchen einer öffentlichen oder nichtöffentlichen Stelle zum Zweck der Durchführung von Zuverlässigkeitsüberprüfungen Daten von Personen verarbeiten, denen ein privilegierter Zugang zu der Veranstaltung gewährt werden soll.

(2) Die Zuverlässigkeitsüberprüfung darf nur durchgeführt werden, wenn

1. die betroffene Person zugestimmt hat,

2. dies insbesondere im Hinblick auf den Zugang der betroffenen Person zu einer besonders gefährdeten Veranstaltung und das berechtigte Interesse des Veranstalters erforderlich ist und

3. dies im Hinblick auf den Anlass der Überprüfung, insbesondere den Zugang der betroffenen Person zu der Veranstaltung, mit Rücksicht auf ein berechtigtes Sicherheitsinteresse des Empfängers angemessen ist.

Vor der Zustimmung ist die betroffene Person zu informieren über

1. den konkreten Ablauf der Zuverlässigkeitsüberprüfung

2. den Inhalt der Übermittlung an die in Absatz 4 genannten Stellen,

3. die mit der Überprüfung verbundenen Datenverarbeitungen,

4. die Erkenntnisse, die zur Bewertung, dass Bedenken gegen die Zuverlässigkeit bestehen, führen können und

5. die Möglichkeit der Verweigerung oder des jederzeitigen Widerrufs der Zustimmung.

(3) Zur Durchführung der Zuverlässigkeitsüberprüfung kann die Polizei die Identität der zu überprüfenden Person feststellen und zu diesem Zweck vorgelegte Ausweisdokumente kopieren oder Kopien von Ausweisdokumenten anfordern. Die Durchführung der Zuverlässigkeitsüberprüfung erfolgt auf der Grundlage der Datenbestände

1. der Polizeien von Bund und Ländern,

2. der Strafverfolgungsbehörden und Gerichte, soweit Erkenntnisse über Strafverfahren vorliegen,

3. des Bundesamtes für Migration und Flüchtlinge,

4. des Landesamtes für Verfassungsschutz, soweit im Einzelfall erforderlich sowie

5. der zuständigen Polizeien im Ausland, sofern die zu überprüfende Person ihren Wohnsitz im Ausland hat und dies im Einzelfall erforderlich ist.

(4) Die Polizei darf zum Zweck des Datenabgleichs die erforderlichen personenbezogenen Daten der betroffenen Person an die in Absatz 3 Satz 2 genannten Stellen übermitteln. Personenbezogene Daten, die die Polizei bei diesen Stellen zum Zweck der Durchführung der Zuverlässigkeitsüberprüfung erhoben hat, darf sie ausschließlich

zu diesem Zweck verarbeiten. Die Polizei kann das Ergebnis der Zuverlässigkeitsüberprüfung an die öffentliche oder nichtöffentliche Stelle gemäß Absatz 1 übermitteln, soweit dies wegen der Art und des Umfangs der Erkenntnisse über die betroffene Person angemessen ist. Die Übermittlung an eine nichtöffentliche Stelle beschränkt sich auf die Auskunft zum Vorliegen von Zuverlässigkeitsbedenken. Die betroffene Person ist über den Inhalt der Übermittlung zu informieren.

(5) Die empfangende Stelle darf die übermittelten Daten nur zu dem Zweck der Zuverlässigkeitsüberprüfung verarbeiten. Die Polizei hat den Empfänger schriftlich zu verpflichten, diese Zweckbestimmung einzuhalten.

(6) Die Polizei kann die im Rahmen der Zuverlässigkeitsüberprüfung verarbeiteten personenbezogenen Daten für die Dauer von sechs Monaten speichern. Die Frist beginnt mit dem Ende des Jahres, in dem die Zuverlässigkeitsüberprüfung erfolgt ist.

(7) Die oder der Sächsische Datenschutz- und Transparenzbeauftragte ist über ein nach Absatz 1 beabsichtigtes Verfahren zu unterrichten.“

31. § 91 wird durch folgenden § 91 ersetzt:

„§ 91

Berichtigung, Löschung und Einschränkung der Verarbeitung

(1) Personenbezogene Daten sind nach Maßgabe der §§ 14 und 31 des Sächsischen Datenschutz-Umsetzungsgesetzes zu berichtigen, zu löschen oder in der Verarbeitung einzuschränken, soweit durch Vorschriften dieses Gesetzes keine abweichenden Regelungen getroffen werden.

(2) Unbeschadet von sonstigen durch dieses Gesetz bestimmten Höchstspeicher- oder Löschfristen hat der Verantwortliche personenbezogene Daten unverzüglich zu löschen, soweit

1. ihre Speicherung unzulässig war,

2. sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen,

3. die weitere Speicherung unzulässig ist, weil die Ermittlungen oder eine der Polizei bekannte Entscheidung der Staatsanwaltschaft oder eines Gerichts ergeben, dass die Gründe, die zu der Speicherung geführt haben, nicht zutreffen,

4. aus Anlass einer Einzelfallbearbeitung oder aus Anlass des Ablaufs einer Aussonderungsprüffrist festgestellt wird, dass ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist,

5. nach Ablauf der Aussonderungsprüffrist die Umstände, die zur Speicherung geführt haben, entfallen sind,

6. die Höchstspeicherfrist abgelaufen ist,

7. die betroffene Person die Einwilligung für die Speicherung widerrufen hat, oder

8. zwei Jahre nach dem Tod der betroffenen Person vergangen sind.

(3) Sind personenbezogene Daten in Akten gespeichert und wird deren Unrichtigkeit festgestellt, ist die Berichtigungspflicht nach § 31 Absatz 1 des Sächsischen Datenschutz-Umsetzungsgesetzes dadurch zu erfüllen, dass dies in der Akte vermerkt

wird. Bestreitet die betroffene Person die Richtigkeit sie betreffender personenbezogener Daten und lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, sind die Daten zu kennzeichnen, um eine Einschränkung der Verarbeitung gemäß § 14 Absatz 1 Satz 3 des Sächsischen Datenschutz-Umsetzungsgesetzes zu ermöglichen. Die Verarbeitung personenbezogener Daten in Akten ist einzuschränken, wenn Daten

1. nach Absatz 2,

2. auf Grund von sonstigen durch dieses Gesetz bestimmten Löschungsverpflichtungen oder

3. nach § 14 Absatz 2 des Sächsischen Datenschutz-Umsetzungsgesetzes

zu löschen sind. Die Unterlagen sind mit einem entsprechenden Einschränkungsvermerk zu versehen. Die gesamte Akte ist zu vernichten, wenn sie insgesamt zur Erfüllung der Aufgaben nicht mehr erforderlich ist.

(4) § 5 Absatz 1 und 2 des Archivgesetzes für den Freistaat Sachsen bleibt unberührt.“

32. In § 93 Absatz 1 Nummer 10 wird die Angabe „personellen,“ gestrichen und die Angabe „27“ durch die Angabe „20“ ersetzt.

33. In § 94 Nummer 1 wird die Angabe „§§ 59 bis 69“ durch die Angabe „nach § 57a Absatz 1 Satz 4 und Absatz 2 sowie den §§ 58 und 60 bis 68“ ersetzt.

34. In § 97 Absatz 1 Nummer 3 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

35. In § 101 Absatz 1 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

36. § 106 Absatz 1 Nummer 1 und 2 wird durch die folgenden Nummern 1 und 2 ersetzt:

„1. einer vollstreckbaren gerichtlichen Anordnung nach § 21 Absatz 3 Satz 1 oder einer vollziehbaren Anordnung nach § 21 Absatz 3 Satz 3 zuwiderhandelt und dadurch den Zweck der Anordnung gefährdet oder

2. einer vollstreckbaren gerichtlichen Anordnung nach § 61 Absatz 3 Satz 1 oder einer vollziehbaren Anordnung nach § 61 Absatz 3 Satz 2 zuwiderhandelt und dadurch die kontinuierliche Feststellung seines Aufenthaltsortes durch die Polizei verhindert.“

37. Nach § 106 wird folgender § 106a eingefügt:

„§ 106a

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig einer vollziehbaren Anordnung nach den §§ 18 bis 20 oder nach § 21 Absatz 1 zuwiderhandelt.

(2) Ordnungswidrigkeiten nach Absatz 1 können mit einer Geldbuße bis zu fünftausend Euro geahndet werden.

(3) Zuständige Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist die Polizeidienststelle, die die Maßnahme angeordnet hat.“

38. § 107 wird durch folgenden § 107 ersetzt:

„§ 107

Berichtspflichten gegenüber dem Landtag

Das Staatsministerium des Innern berichtet der Öffentlichkeit und dem Landtag jährlich über abgeschlossene Maßnahmen nach § 21 Absatz 2 und 3, § 57 Absatz 4 Satz 2 und Absatz 5 Satz 2, § 57a Absatz 1 Satz 4 und Absatz 2, nach den §§ 58 und 60 bis 68 sowie über Übermittlungen nach § 90. Der Bericht hat statistische Angaben über Anlass, Zweck, Dauer und Ergebnis solcher Maßnahmen sowie über die Benachrichtigung der Betroffenen und die Löschung der personenbezogenen Daten zu enthalten. Die Staatsregierung teilt dazu in einem ergänzenden Bericht jeweils die Anzahl rechtskräftig abgeschlossener Verfahren nach § 106 mit.“

39. § 108 wird durch folgenden § 108 ersetzt:

„§ 108

Außerkrafttreten

Am 31. Dezember 2031 treten außer Kraft:

1. § 40 Absatz 4 Satz 2, soweit hierdurch das Staatsministerium des Innern ermächtigt wird zu bestimmen, dass auch Polizeibediensteten, die außerhalb von Spezialeinheiten zum Einsatz kommen, der Einsatz von Vorrichtungen für den Abschuss besonderer Formen von Projektilen eröffnet wird,

2. § 57 Absatz 4 Satz 2 und Absatz 5 Satz 2 sowie

3. . § 66 Absatz 2, 2a und 3.“

Artikel 2

Änderung des Sächsischen Polizeibehördengesetzes

Das Sächsische Polizeibehördengesetz vom 11. Mai 2019 (SächsGVBl. S. 358, 389), das durch Artikel 2 des Gesetzes vom 22. Juli 2024 (SächsGVBl. S. 724) geändert worden ist, wird wie folgt geändert:

1. § 23 Absatz 2 wird durch folgenden Absatz 2 ersetzt:

„(2) Während der Nachtzeit (§ 104 Absatz 3 der Strafprozessordnung) darf eine Wohnung nur in den Fällen des Absatz 1 Satz 1 Nummer 2 betreten und durchsucht werden. Diese Einschränkung gilt nicht, wenn von der Wohnung eine erhebliche, die Gesundheit Dritter beeinträchtigende Störung ausgeht.“

2. § 30 Absatz 1 wird durch folgenden Absatz 1 ersetzt:

„(1) Die Polizeibehörden können personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Bildaufnahme und -aufzeichnung erheben, soweit Tatsachen die Annahme rechtfertigen, dass

1. an, in oder in unmittelbarer Nähe von öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Kulturgütern, Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen künftig Straftaten oder Ordnungswidrigkeiten begangen werden, durch die Personen oder Sach- oder Vermögenswerte gefährdet werden, oder

2. in öffentlich zugänglichen Bereichen sonstige erhebliche Gefahren für die öffentliche Sicherheit entstehen,

und die Bildaufnahmen und Aufzeichnungen zur Abwehr dieser Gefahren erforderlich sind.“

3. § 40 Absatz 1 wird durch folgenden Absatz 1 ersetzt:

„(1) Soweit die Polizeibehörden personenbezogene Daten zur Erfüllung ihrer Aufgaben verarbeiten, die in den Anwendungsbereich von § 1 des Sächsischen Datenschutz-Umsetzungsgesetzes fallen, gelten die §§ 54 bis 56, § 79 Absatz 1 und 2, § 79a, § 81 Absatz 3, § 82, § 83, § 84 Absatz 1, 2 und 3 Nummer 1 bis 3 sowie Absatz 4 und 5 sowie die §§ 89 und 91 bis 93 des Sächsischen Polizeivollzugsdienstgesetzes entsprechend und ergänzend die Vorschriften des Sächsischen Datenschutz-Umsetzungsgesetzes.“

4. In § 42 Absatz 3 Satz 2 wird die Angabe „Erwerbstätigkeit“ durch die Angabe „Erwerbsfähigkeit“ ersetzt.

Artikel 3

Änderung des Sächsischen Kontrollgesetzes

Das Sächsische Kontrollgesetz vom 22. April 2003 (SächsGVBl. S. 106), das zuletzt durch Artikel 14 des Gesetzes vom 11. Mai 2019 (SächsGVBl. S. 358) geändert worden ist, wird wie folgt geändert:

In § 2 wird die Angabe „§§ 59 bis 69“ durch die Angabe „§§ 60 bis 62 und 63 bis 68“ ersetzt.

Artikel 4

Änderung des Sächsischen Gesetzes zur Regelung polizeilicher Zuverlässigkeitsüberprüfungen

Das Sächsische Gesetz zur Regelung polizeilicher Zuverlässigkeitsüberprüfungen vom 12. April 2024 (SächsGVBl. S. 405, 429) wird wie folgt geändert:

In § 4 Satz 3 Nummer 4 wird die Angabe „einer Zuverlässigkeitsüberprüfung nach § 1 Absatz 1 Satz 1 für die Ernennung in der Fachrichtung Polizei unterzogen werden soll und“ gestrichen.

Artikel 5

Folgeänderung im Sächsischen Besoldungsgesetz

Das Sächsische Besoldungsgesetz vom 6. Juli 2023 (SächsGVBl. S. 467, 476), das zuletzt durch Artikel 4 des Gesetzes vom 27. Juni 2025 (SächsGVBl. S. 285) geändert worden ist, wird wie folgt geändert:

In Anlage 2 Besoldungsgruppe B 3 wird die Angabe „Polizeiverwaltungsamts“ durch die Angabe „Polizeipräsidiums für Service und IT“ ersetzt.

Artikel 6

Folgeänderung im Sächsischen Verwaltungsorganisationsgesetz

Das Sächsische Verwaltungsorganisationsgesetz vom 25. November 2003 (SächsGVBl. S. 899), das zuletzt durch Artikel 9 des Gesetzes vom 27. Juni 2025 (SächsGVBl. S. 285) geändert worden ist, wird wie folgt geändert:

In § 8 Absatz 1 Nummer 4 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

Artikel 7

Folgeänderung im Sächsischen Personalvertretungsgesetz

Das Sächsische Personalvertretungsgesetz vom 29. August 2018 (SächsGVBl. S. 570), das zuletzt durch Artikel 3 des Gesetzes vom 5. Juli 2024 (SächsGVBl. S. 600) geändert worden ist, wird wie folgt geändert:

In § 68 Absatz 1 Nummer 4 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

Artikel 8

Folgeänderungen im Sächsischen Straßenverkehrsrechtsgesetz

Das Sächsische Straßenverkehrsrechtsgesetz vom 3. Mai 2019 (SächsGVBl. S. 317) wird wie folgt geändert:

1. In § 14 Absatz 1 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

2. In § 18 Absatz 2 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

Artikel 9

Folgeänderungen in der Sächsischen Polizeiorganisationsverordnung

Die Sächsische Polizeiorganisationsverordnung vom 17. März 2020 (SächsGVBl. S. 97) wird wie folgt geändert:

1. In § 1 Absatz 1 wird die Angabe „des Polizeiverwaltungsamtes“ durch die Angabe „des Polizeipräsidiums für Service und IT“ ersetzt.

2. In § 4 Absatz 1, 2, 3 Satz 1 und 2 sowie Absatz 4 wird jeweils die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

Artikel 10

Folgeänderung in der Sächsischen Waffengesetzdurchführungsverordnung

Die Sächsische Waffengesetzdurchführungsverordnung vom 30. August 2017 (SächsGVBl. S. 502), die zuletzt durch die Verordnung vom 22. November 2024 (SächsGVBl. S. 922) geändert worden ist, wird wie folgt geändert:

In § 2 Absatz 1 Nummer 2 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

Artikel 11

Folgeänderung in der Sächsischen Vertretungsverordnung

Die Sächsische Vertretungsverordnung vom 4. April 2023 (SächsGVBl. S. 124) wird wie folgt geändert:

In § 6 Absatz 3 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

Artikel 12

Folgeänderungen in der Sächsischen Heilfürsorgeverordnung

Die Sächsische Heilfürsorgeverordnung vom 16. Juni 2025 (SächsGVBl. S. 254) wird wie folgt geändert:

1. In § 2 Absatz 7 Satz 2 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

2. In § 30 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

Artikel 13

Folgeänderungen in der Sächsischen Straßenverkehrsrechtsverordnung

Die Sächsische Straßenverkehrsrechtsverordnung vom 28. April 2021 (SächsGVBl. S. 514), die zuletzt durch die Verordnung vom 16. August 2024 (SächsGVBl. S. 847) geändert worden ist, wird wie folgt geändert:

1. In § 5 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

2. In § 9 Absatz 2 Satz 2 wird die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

Artikel 14

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

EU-Rechtsakte

Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7. Dezember 2018, S. 56); ABl. 2019 L 316 I S. 4, ABl. 2021 L 336 S. 51, 2022 ABl. L 181 S. 37), zuletzt geändert durch Art. 1 VO (EU) 2022/1190 vom 6. Juli 2022 (ABl. L 185, S. 1).

Begründung

A. Allgemeiner Teil

Seit der letzten grundlegenden Novellierung des Polizeirechts durch das Gesetz zur Neustrukturierung des Polizeirechts des Freistaates Sachsen vom 11. Mai 2019 hat sich umfangreicher Ergänzungs- und Änderungsbedarf bei den polizeirechtlichen Vorschriften ergeben. Dieser folgt zum einen aus einem Urteil des Sächsischen Verfassungsgerichtshofs und zum anderen aus verschiedenen - zum Teil grundsätzlichen - Urteilen des Bundesverfassungsgerichts zu polizeirechtlichen Fragestellungen. Weiterer Änderungsbedarf folgt aus dem Koalitionsvertrag 2024 bis 2029 zwischen CDU und SPD vom 4. Dezember 2024. Ferner besteht umfassender Änderungsbedarf aus polizeifachlicher Sicht und in Folge von EU-Recht.

I. Änderungsbedarf in Folge von höchstrichterlicher Rechtsprechung

Durch Urteil vom 25. Januar 2024, Vf. 91-II-19, hat der Sächsische Verfassungsgerichtshof bestimmte Befugnisregelungen des Sächsischen Polizeivollzugsdienstgesetzes in Teilen als mit der Verfassung des Freistaates Sachsen für unvereinbar erklärt. Dies betrifft zum einen die Befugnisregelungen zu verdeckten Überwachungsmaßnahmen; hier besteht Bedarf die Eingriffsschwellen an die Vorgaben des Sächsischen Verfassungsgerichtshofs anzupassen. Zum anderen hat der Sächsische Verfassungsgerichtshof die Befugnisregelungen zur Weiterverarbeitung von in Informationssystemen der Polizei vorsorgend gespeicherten personenbezogenen Daten beanstandet. In Konsequenz besteht auch hier Änderungsbedarf. Ferner hat der Sächsische Verfassungsgerichtshof die Regelung der Datenerhebung durch den Einsatz technischer Mittel zur Bildaufnahme und -aufzeichnung im Sächsischen Polizeibehördengesetz als nicht mit der Sächsischen Verfassung für vereinbar erklärt. Auch insoweit besteht Anpassungsbedarf.

Durch Urteil vom 1. Oktober 2024, 1 BvR 1160/19 (Bundeskriminalamtsgesetz II), hat das Bundesverfassungsgericht ein Grundsatzurteil rechtliche Anforderungen an die „vorsorgende Speicherung“ von personenbezogenen Daten im Bereich des polizeilichen Informationsverbundes erlassen. Die grundlegenden verfassungsrechtlichen Ausführungen des Bundesverfassungsgerichts sind auf die Datenverarbeitung der Landespolizei Sachsen zu übertragen. Die vom Bundesverfassungsgericht vorgegebenen Ableitungen für die Gestaltung von gesetzlichen Regelungen führen daher auch zu Regelungsbedarf im Sächsischen Polizeivollzugsdienstgesetz.

Mit Beschluss vom 27. Mai 2020, 1 BvR 1873/13, 1 BvR 2618/13 (Bestandsdatenauskunft II), hat das Bundesverfassungsgericht über die Anforderungen an die Ausgestaltung der Auskunft über Bestandsdaten von Telekommunikationsdiensten entschieden und die bisherige Rechtsprechung zum „Doppeltürmodell“ weiter präzisiert. In Konsequenz des Urteils erfolgten umfassende Änderungen und Anpassungen in den Fachgesetzen des Bundes im Bereich Telekommunikationsdienste und digitale Dienste. Diese Änderungen müssen in den Regelungen des Sächsischen Polizeivollzugsdienstgesetzes, die den Abruf solcher Daten erlauben, umgesetzt werden.

Ferner sind umzusetzen:

- die Anpassung der Nachtzeitregelung von 4 auf 6 Uhr im Rahmen der Durchsuchung von Wohnungen (BVerfG Beschluss 12.03.2019, 2 BvR 675/14) und

- die Stärkung des Kernbereichsschutzes auf der Erhebungs-, Auswertungs- und Verwertungsebene beim Einsatz von verdeckten Ermittlerinnen, verdeckten Ermittlern und V-Personen (BVerfG Beschluss vom 09.12.2022, 1 BvR 1345/21).

II. Regelungsbedarfe in Umsetzung des Koalitionsvertrages

In Umsetzung des Regelungsauftrags gemäß den Ziffern 1408 bis 1413 des Koalitionsvertrags wird eine Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) zur Abwehr erheblicher terroristischer Gefahren oder zur Verhinderung schwerster Kapitalverbrechen im Sächsischen Polizeivollzugsdienstgesetz aufgenommen, die Anwendung durch gesetzliche Regelung befristet und nach einem Anwendungszeitraum von drei Jahre evaluiert. Die herkömmlichen Überwachungsmethoden stoßen angesichts der weit verbreiteten Verschlüsselung in der digitalen Kommunikation zunehmend an ihre Grenzen. Die nahezu flächendeckende Verwendung von Verschlüsselungstechnologien in der modernen Kommunikation macht die Quellen-TKÜ zu einem unverzichtbaren Ermittlungsinstrument, da heute standardmäßig eine Verschlüsselung in den meisten Messaging-Anwendungen implementiert ist.

Gemäß Ziffer 1417 des Koalitionsvertrags wird die bestehende gesetzliche Regelung für den Einsatz von Bodycams in öffentlich zugänglichen Bereichen auf den Bereich Wohnungen bzw. Privaträume unter Beachtung der verfassungsrechtlichen Vorgaben erweitert. Der Wohnungsbegriff des Sächsischen Polizeivollzugsdienstgesetzes umfasst neben Wohn- und Nebenräumen auch Arbeits-, Betriebs-, und Geschäftsräume, auch während der Öffnungszeiten. Die Erweiterung des Einsatzes von Bodycams in Wohnungen entspricht einem praktischen Bedürfnis. Gerade in Wohnungen können die polizeilichen Einsatzkräfte – etwa bei Wohnungsverweisungen im Zusammenhang mit häuslicher Gewalt – auf Situationen treffen, in denen die betroffenen Personen unter hohem Stress stehen und auf Einsatzmaßnahmen besonders aggressiv reagieren. In kritischen Situationen dieser Art kann der Einsatz der Bodycam eine deeskalierende Wirkung entfalten und die eingesetzten Kräfte vor Angriffen schützen. Dies bestätigen die bundesweit praktischen Erfahrungen.

III. Regelungsbedarf in Umsetzung von EU-Recht, sonstiger aus polizeifachlicher Sicht bestehender Regelungsbedarf und redaktionelle Anpassungen

1. Umsetzung von EU-Recht

Ein wesentliches Ziel der Novellierung ist die Verbesserung des Schutzes von Opfern und potenziellen Opfern häuslicher Gewalt. Durch das Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (Istanbul-Konvention), das am 1. Februar 2018 in Deutschland in Kraft trat, ist die Bundesrepublik auf sämtlichen Verwaltungsebenen dazu verpflichtet, Gewalt gegen Frauen und häusliche Gewalt zu verhüten, zu bekämpfen und Betroffenen umfassenden Schutz sowie Unterstützung zu gewähren. In Umsetzung des sächsischen Koalitionsvertrags 2024-2029 ist in den Ziffern 3287 bis 3290 festgehalten: "Der Schutz von Frauen vor Gewalt hat für uns einen hohen Stellenwert. Hierzu werden wir die Istanbul-Konvention auf Basis des Landesaktionsplans des Freistaats zur Verhütung und Bekämpfung geschlechtsspezifischer Gewalt umsetzen und die dazu notwendigen Mittel wollen wir verlässlich zur Verfügung stellen.". Das bestehende Instrumentarium zum staatlichen Gewaltschutz umfasst sowohl polizeirechtliche Verfügungen als auch familiengerichtliche Anordnungen nach dem Gesetz zum zivilrechtlichen Schutz vor Gewalttaten und Nachstellungen (Gewaltschutzgesetz). Beide Rechtsregime sehen Schutzmaßnahmen vor, die darauf abzielen, Gewaltausübende fernzuhalten. Dazu gehören Wohnungsverweisungen, Betretungsverbote für Räumlichkeiten, die das Opfer regelmäßig aufsucht, sowie Kontakt- und Näherungsverbote. Das vorliegende Gesetz verfolgt das Ziel, die Wirksamkeit dieser Schutzmaßnahmen und deren Durchsetzung gegenüber den bisherigen Regelungen zu erweitern und klarer zu strukturieren und damit den Schutz insgesamt zu verbessern.

Darüber hinaus resultiert auch aus dem Schengener Informationssystem der dritten Generation (EU VO 2018/1862) eine erforderliche Anpassung polizeirechtlicher Vorschriften durch Erweiterung der Ausschreibungsgründe auf den der Ermittlungsanfrage.

2. Sonstiger aus polizeifachlicher Sicht bestehender Regelungsbedarf

Um den aktuellen technischen Fortschritten und den sich wandelnden Gefahrenlagen gerecht zu werden, ist eine kontinuierliche Anpassung und gezielte Stärkung der polizeilichen Befugnisse erforderlich. Nur so kann die effektive Wahrnehmung polizeilicher Aufgaben auch künftig im Interesse der Bürgerinnen und Bürger sichergestellt werden.

Die durch die voranschreitende Digitalisierung bedingten Datenmengen, die unterschiedlichen Datenformate und die Vielzahl an Datensystemen wird zunehmend die Aufgabenwahrnehmung der Polizei bei der Auswertung und Analyse von Daten erschwert, insbesondere bei Gefahrenlagen, in denen die Gewinnung relevanter Erkenntnisse zur Durchführung geeigneter polizeilicher Maßnahmen unter hohem zeitlichen Druck steht. Um die Auswertung dieser Datenmengen für die Polizeiarbeit zu ermöglichen, wird in das Sächsische Polizeivollzugsdienstgesetz eine Befugnis zur automatisierten Datenanalyse (§ 62a-neu) aufgenommen. Diese Befugnis soll dazu dienen, im Anlassfall einer bestimmten Gefahrenlage gespeicherte Daten zum Zweck einer Analyse zusammenzuführen und durch den Einsatz technischer Anwendungen bei großen Datenmengen bestehende Verbindungen oder Beziehungen zwischen den Daten herstellen zu können. Durch Urteil vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) hat das Bundesverfassungsgericht umfassend zur verfassungsrechtlichen Zulässigkeit von technischen Anwendungen zur automatisierten Datenerhebung und -analyse bei der Polizei ausgeführt und grundlegende Vorgaben für die gesetzgeberische Ausgestaltung solcher Datenverarbeitung abgeleitet. Die vorgesehene Befugnisregelung setzt diese Anforderungen des Bundesverfassungsgerichts um.

Anknüpfend an den bestehenden Rechtsrahmen des § 57 Sächsisches Polizeivollzugsdienstgesetz, der u. a. eine offene Beobachtung und Aufzeichnung von Bilddaten an Kriminalitätsbrennpunkt-Bereichen ermöglicht, soll durch eine Befugnis zur „intelligenten Videoüberwachung“ (§ 57a-neu), eine vollständige und ausreichend schnelle Auswertung des Bildmaterials ermöglicht werden, um Gefahren in diesen Bereichen frühzeitig erkennen und die Begehung von Straftaten verhindern zu können. Aufgrund der begrenzten menschlichen Wahrnehmungsfähigkeiten, aber auch aufgrund des erheblichen zeitlichen Aufwandes einer laufenden Auswertung von Bildmaterial, wird der Einsatz von Bildanalysesoftware, die automatisiert bestimmte (Bewegungs-)Muster, die auf die Begehung von Straftaten hindeuten, gesetzlich geregelt. Anknüpfend an eine erfolgte Mustererkennung und Verifizierung einer potentiell gefährlichen Situation durch polizeiliche Bedienstete wird durch gesetzliche Regelung bei bestimmten deutlich gesteigerten Gefährdungslagen die Befugnis zur biometrischen Echtzeit-Fernidentifizierung auf der Grundlage der Datenbestände der polizeilichen Auskunfts- und Fahndungssysteme eröffnet.

Damit die Polizei gezielt nach Personen suchen kann, von denen eine die konkrete oder tatsachenbasierte vorhersehbare Gefahr einer terroristischen Straftat ausgeht, ist die Aufnahme einer Regelung zur biometrischen Echtzeit-Fernidentifizierung auf der Grundlage von in polizeilichen Auskunfts- und Fahndungssystemen gespeicherten biometrischen Daten vorgesehen (§ 57a Absatz 2-neu). Eine gleiche Befugnis ist im Hinblick auf Opfer von Entführung, Menschenhandel oder sexueller Ausbeutung sowie für vermisste Personen vorgesehen.

Zur Verhütung der besonders sicherheitsrelevanten Verkehrsordnungswidrigkeit des unerlaubten Nutzens von elektronischen Geräten wird die Polizei ermächtigt, die Einhaltung der Verkehrsvorschrift des § 23 Absatz. 1a der Straßenverkehrs-Ordnung durch Videoaufnahmen an bestimmten relevanten Straßenabschnitten präventiv zu überwachen (§ 57 Absatz 9-neu). Verhindert werden solche Verkehrsverstöße, die regelmäßig zu schweren Unfällen und damit zu einer Gefahr für Leib und Leben führen.

Zum Zweck des Einsatzes von durch die Polizei entwickelter oder genutzter lernender Analysesoftware zur Aufgabenerfüllung wird eine Befugnis aufgenommen, die den gesetzlichen

Rahmen für das Training oder den Test von lernenden Systemen durch die Polizei erlaubt, so beispielsweise zur automatisierten (Verhaltens-)Mustererkennung, (§ 79c-neu).

Zur Effektivierung der vorbeugenden Straftatenbekämpfung durch die Verhütung von Straftaten wurde eine Befugnis zum anlassbezogenen biometrischen Datenabgleich von polizeilichen Daten mit öffentlich zugänglichen Daten aus dem Internet aufgenommen, um Personen, von denen solche Gefahren ausgehen, ausfindig machen oder zu identifizieren zu können (§ 62b-neu).

Der Gesetzentwurf sieht weiterhin vor:

- Die Neufassung der Befugnis zur Durchführung von Zuverlässigkeitsüberprüfungen bei besonders gefährdeten Veranstaltungen (§ 88).

- Die Aufnahme von Befugnissen zur Abwehr und zum Einsatz von unbemannten Fahrzeugsystemen in Anpassung an technischen Veränderungen (§§ 12a-neu, 71-neu).

- Die Erweiterung der bestehenden Regelung zur automatisierten Kennzeichenerkennung zur effizienteren Gefahrenabwehr unter Berücksichtigung von Rechtsprechung des Bundesverfassungsgerichts (§ 58).

- Die Aufnahme einer Befugnis zur Standortdatenübermittlung bei Notrufen, um Menschen in Notsituationen metergenau orten zu können (§ 86 Absatz 1-neu).

- Die Aufnahme einer Befugnis zur öffentlichen Ausschreibung von gefährdeten Personen oder von Personen, von denen eine Gefahr ausgeht (§ 84a-neu).

- Die Umbenennung des Polizeiverwaltungsamtes in „Polizeipräsidium für Service und IT“ zur Steigerung der Arbeitgeberattraktivität. Hierzu bedarf es der Folgeanpassung in zahlreichen Gesetzen und Verordnungen (§ 97 und weitere Vorschriften).

- Eine Vielzahl redaktioneller Anpassungen, so u. a. Folgeänderungen in Konsequenz von Änderungen im Bundesrecht und die Behebung sonstiger redaktionelle Versehen.

In Artikel 2 sieht der Gesetzentwurf bezüglich des Sächsischen Polizeibehördengesetzes im Wesentlichen die Anpassung an die Rechtsprechung des Sächsischen Verfassungsgerichtshofes zur Zulässigkeit der Videoüberwachung nach § 30 SächsPBG sowie an die Rechtsprechung des BVerfG zur Nachtzeit vor.

In Konsequenz der Aufnahme neuer eingriffsintensiver Befugnisse in das Sächsische Polizeivollzugsdienstgesetz erweitert der Gesetzentwurf die Kontrollbefugnisse des Parlamentarischen Kontrollgremiums im Sächsischen Kontrollgesetz (Artikel 3).

Die Änderung durch Artikel 4 dient der gesetzlichen Harmonisierung, die durch die Artikel 5 bis 12 erfolgenden Änderungen betreffen die durch die Umbenennung des bisherigen Polizeiverwaltungsamtes erforderlichen Folgeänderungen.

IV. Gesetzesfolgen

Die Regelungen des Gesetzes zur Änderung polizeilicher Vorschriften des Freistaates Sachsen tragen zum besseren Schutz der öffentlichen Sicherheit und Ordnung bei und verbessern die Rechte der durch die Datenverarbeitung betroffenen Personen.

1) Haushaltauswirkungen

Zu den Haushaltsauswirkungen können derzeit nur grundsätzliche Aussagen getroffen werden und Schätzungen erfolgen. Die voraussichtlichen finanziellen Auswirkungen auf den Landeshaushalt sind, soweit bezifferbar, derzeit weder im Haushaltsplan 2025/2026 noch der mittelfristigen Finanzplanung – bis auf einen Betrag von insgesamt 300 TEUR für den Einsatz von unbemannten Luftfahrtsystemen (§ 71) – enthalten und bleiben daher dem weiteren Gesetzgebungsverfahren, insbesondere der Beschlussfassung durch den Sächsischen Landtag, vorbehalten (Haushaltsvorbehalt). Mögliche Mehrausgaben im Haushaltsjahr 2026 sollen im Rahmen der im Doppelhaushalt 2025/2026 veranschlagten Ansätze des Epl. 03 abgebildet werden.

Der Gesetzentwurf sieht für das Sächsische Polizeivollzugsdienstgesetz klarstellende Befugnisregelungen, die Erweiterung bestehender Befugnisregelungen und die Aufnahme neuer Befugnisregelungen vor. Die Haushaltsauswirkungen sind jeweils abhängig vom Umfang des künftigen polizeifachlichen Realisierungsbedarfs. Dabei sind nachfolgende Kosten relevant.

- Befugnis zur „Drohnenabwehr“ (§ 12a SächsPDVG)

Erfüllungsaufwand entsteht durch die neu geschaffene Befugnis zum Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme. Die für die Umsetzung der Vorschrift erforderliche technische Grundausstattung ist den aktuellen Bedingungen entsprechend teilweise vorhanden und im Einsatz. Zur weiteren Steigerung der Einsatzfähigkeit im Rahmen des ggf. zur Verfügung stehenden Sondervermögens des Bundes ist eine Beschaffung weiterer Technik (u.a. Peiltechnik für etwa 1,5 Mio. EUR, zusätzlich jährliche Betriebskosten ca. 150.000 EUR) vorgesehen, jedoch nur für den Fall, dass durch den Bund die Mittel tatsächlich bereitgestellt werden. Zusätzliche Kosten für Personal sind nicht zu erwarten.

Änderung der Befugnis zur Erteilung eines Aufenthalts- oder Kontaktverbotes (§ 21 Absatz 2)

Die Änderung der Befugnis zur Erteilung von Aufenthalts- oder Kontaktverboten nach § 21 Absatz 2 verursacht keine Haushaltsauswirkungen beim Polizeivollzugsdienst.

Einmalige Kosten fallen infolge einer Evaluierungsverpflichtung in Hinblick auf die Änderung der Vorschrift an. Hierzu können – nach den Erfahrungen der letzten Evaluierung zu verschiedenen Vorschriften des Sächsischen Polizeivollzugsdienstgesetzes – Kosten von geschätzt 30.000 bis 50.000 EUR für die Haushaltsjahre 2027 (Abschlagszahlung) und 2028 oder 2029/30 (Restzahlung) angesetzt werden.

- Ausweitung des Einsatzes von Distanzelektroimpulsgeräten (§ 40 Absatz 4 Satz 2 SächsPDVG)

Mir der neuen Regelung wird die Verwendungsbeschränkung aufgehoben. Nach Abschluss der frühestens 2026 beginnenden Pilotierungsphase werden zur Umsetzung der Befugnis Kosten in Höhe von ca. 1 Mio. EUR, verteilt auf drei Jahre, geschätzt. Davon sind ca. 324.000 EUR Beschaffungskosten für 120 „Taser“ und jährliche Betriebskosten in Höhe von ca. 219.000 EUR enthalten.

Einmalige Kosten fallen infolge einer Evaluierungsverpflichtung zur Ausweitung des Einsatzes von Distanzelektroimpulsgeräten an (siehe § 40 Absatz 5). Hierzu können – nach den Erfahrungen der letzten Evaluierung zu verschiedenen Vorschriften des Sächsischen Polizeivollzugsdienstgesetzes – Kosten von geschätzt 30.000 bis 50.000 EUR für die Haushaltsjahre 2027 (Abschlagszahlung) und 2028 oder 2029/30 (Restzahlung) angesetzt werden.

- Befugniserweiterung zum Einsatz von Bodycam in Wohnungen (§ 57 Absatz 4 Satz 2, Absatz 5 Satz 2 SächsPDVG)

Die neue Regelung verursacht keine Haushaltsauswirkungen beim Polizeivollzugsdienst, da die vorhandenen Geräte eingesetzt werden können. Mit der Erweiterung der Befugnis zu einem möglichen Einsatz von Bodycam in Wohnungen ist im Anwendungsfall ein Zeit- und Arbeitsaufwand verbunden. Dieser führt in der Gesamtbilanz nicht zu einem höheren Aufwand in der Gesamtbewältigung des Gefährdungssachverhalts, da der Bodycam-Einsatz ggf. zu einer vorzeitigen Beendigung des polizeilichen Einsatzes und damit zu einem geringeren Personaleinsatz führen kann.

Einmalige Kosten fallen infolge einer Evaluierungsverpflichtung zum Einsatz von Bodycam in Wohnungen an (siehe § 57 Absatz 11). Hierzu können – nach den Erfahrungen der letzten Evaluierung zu verschiedenen Vorschriften des Sächsischen Polizeivollzugsdienstgesetzes – Kosten von geschätzt 30.000 bis 50.000 EUR für die Haushaltsjahre 2027 (Abschlagszahlung) und 2028 oder 2029/30 (Restzahlung) angesetzt werden.

- Befugniserweiterung zur Verhütung einer besonders sicherheitsrelevanten Verkehrsordnungswidrigkeit (§ 57 Absatz 9 SächsPDVG)

Die neu geschaffene Regelung ermächtigt den Polizeivollzugsdienst zur Überwachung der Einhaltung der Verkehrsvorschrift nach 23 Absatz 1a der Straßenverkehrsordnung durch den Einsatz entsprechender Technik mittels unbemannter Luftfahrtsystemen. Zur präventiven Verkehrsüberwachung ist für jede Polizeidirektion die Ausstattung mit einem Überwachungssystem vorgesehen. Für die Erstausstattung beläuft sich die Kostenschätzung auf 1,0 Mio. EUR. Angaben zu den Kosten des Betriebs können nicht erfolgen. Dem gegenüber stehen Einnahmen durch die Ahndung festgestellter Verkehrsverstöße, zu deren Höhe mangels gesonderter statistischer Erfassung keine Angaben erfolgen können und die zudem den Haushalten der zentralen Bußgeldstelle bzw. der kommunalen Bußgeldstellen zufließen.

- Befugnis zur automatisierten Datenverarbeitung von an öffentlichen Orten durch „Videoüberwachung“ erhobenen personenbezogenen Daten (§ 57a SächsPDVG)

Im Hinblick auf die neue Befugnis zur „gestuften“ Datenverarbeitung nach § 57a Absatz 1 SächsPDVG wird nach derzeitigem Erkenntnisstand von einem Bedarf von zwei Anlagen pro Polizeidirektion ausgegangen. Zur Realisierung im Jahr 2028 werden Investitionskosten in Höhe von 750.000 EUR geschätzt. Für die jährlichen Betriebskosten werden 150.000 EUR und für die Sachkosten 50.000 EUR veranschlagt. Aufgrund bestehender Erfahrungen ist davon auszugehen, dass auf der Grundlage bestehender Befugnisregelungen zur Videoüberwachung (§ 57 Absatz 3 SächsPVDG) bereits vorhandene Videoüberwachungstechnik nicht aufrüstungsfähig ist.

Im Hinblick auf die Befugnis zur gezielten biometrischen Identifizierung (§ 57a Absatz 2 SächsPVDG) kann die in der Polizeidirektion Görlitz bestehende Technik PerIS eingesetzt werden. Das Erfordernis der Beschaffung weiterer mobiler Technik wird derzeitig nicht gesehen.

- Befugniserweiterung der zum verdeckten Einsatz von automatisierten Kennzeichenerkennungssystemen – AKES (§ 58 SächsPDVG)

Zur Steigerung der Effizienz dieser Maßnahme ist deren verdeckter Einsatz neu vorgesehen (so bereits die Vorgängerfassung § 19a Absatz 1 Satz 4 SächsPolG). Aus polizeifachlicher Sicht besteht Bedarf für den Erwerb von weiteren drei stationären Anlagen. Dabei ist von Investitionskosten in Höhe von insgesamt 125.000 EUR und Sachkosten in Höhe von 165.000 EUR auszugehen. Für den Betrieb der stationären Anlagen wird für die Jahre 2026 und 2027 ein Betrag in Höhe von 230.000 EUR angesetzt.

Einmalige Kosten fallen infolge einer Evaluierungsverpflichtung in Hinblick auf die Regelung des stationären Technikeinsatzes an (siehe § 58 Absatz 6). Hierzu können – nach den Er-

fahrungen der letzten Evaluierung zu verschiedenen Vorschriften des Sächsischen Polizeivollzugsdienstgesetzes – Kosten von geschätzt 30.000 bis 50.000 EUR für die Haushaltsjahre 2027 (Abschlagszahlung) und 2028 oder 2029/30 (Restzahlung) angesetzt werden.

- Erweiterung zur Ausschreibung zur Ermittlungsanfrage (§ 60 Abs. 1, 2. Fallvariante SächsPDVG)

Mit der Erweiterung der Ausschreibung auf die Ermittlungsanfrage ist im Anwendungsfall ein Zeit- und Arbeitsaufwand verbunden. Dieser führt in der Gesamtbilanz nicht zu einem höheren Aufwand in der Gesamtbewältigung des Gefährdungssachverhalts, da hierdurch ggf. andere polizeiliche Maßnahmen entbehrlich werden.

- Ausweitung des Einsatzes der Elektronischen Aufenthaltsüberwachung (§ 61 Abs. 1 Nummer 1 SächsPDVG)

Die Erweiterung der Befugnis der elektronischen Aufenthaltsüberwachung auf Hochrisikofälle von häuslicher Gewalt verursacht keine Investitionskosten, jedoch wiederkehrenden Personalaufwand, dessen Umfang fallabhängig ist. Der Umfang der Mehrkosten ist zudem abhängig davon, ob die länderübergreifende Verbundlösung zur Datenverarbeitung (Nutzung der gemeinsamen Überwachungsstelle der Länder mit Sitz in Hessen) durch gesonderte Vereinbarung mit dem Land Hessen fortgesetzt werden kann. Soweit dies möglich ist, entstehen für die Erstanlegung der elektronischen Fußfessel Kosten im mittleren vierstelligen Bereich pro Person, die durch das Land Hessen für die Zurverfügungstellung der Ausstattung mit der „elektronischen Fußfessel“ in Rechnung gestellt werden. Für die Folgemonate fallen Pauschalen (Geräteleasing) und ggf. außergewöhnliche Kosten (Geräteaustausch) an. Nach gegenwärtiger Einschätzung wird von Anwendungsfällen im einstelligen Bereich pro Jahr ausgegangen. Stellenmehrbedarf besteht ggf. nicht, da die elektronische Aufenthaltsüberwachung andere verdeckte Maßnahmen ergänzen und je nach Sachlage Personalressourcen schonen kann.

Einmalige Kosten fallen infolge einer Evaluierungsverpflichtung in Hinblick auf die geänderte Regelung des § 61 an (siehe § 61 Absatz 7). Hierzu können – nach den Erfahrungen der letzten Evaluierung zu verschiedenen Vorschriften des Sächsischen Polizeivollzugsdienstgesetzes – Kosten von geschätzt 30.000 bis 50.000 EUR für die Haushaltsjahre 2027 (Abschlagszahlung) und 2028 oder 2029/30 (Restzahlung) angesetzt werden.

- Befugnis zur anlassbezogenen automatisierten Datenanalyse (§ 62a SächsPDVG)

Welche Software zur Umsetzung der neuen Befugnisregelung zur anlassbezogenen automatisierten Datenanalyse geeignet ist und in die Auswahl einbezogen wird, kann gegenwärtig nicht eingeschätzt werden. Favorisiert wird die Einbindung in ein länderübergreifendes Verfahren zur Beschaffung und Bereitstellung der Software. Sofern die Möglichkeit der länderübergreifenden Vernetzung durch den Bund umgesetzt wird, ergibt sich ein jährlicher Anteil Sachsens an der Kostenverteilung nach dem Königsteiner-Schlüssel in Höhe von 2,5 Mio. EUR, die jedoch voraussichtlich erst nach 2028 haushaltswirksam werden würden. Die Mehrkosten werden jedoch aufgrund eingesparter Personalressourcen gegenüber einer konventionellen Analyse kompensiert.

- Befugnis zum anlassbezogenen nachträglichen Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§ 62b SächsPDVG)

Welche Software zur Umsetzung der neuen Befugnisregelung geeignet ist und in die Auswahl einbezogen wird, kann gegenwärtig nicht eingeschätzt werden. Demzufolge können die voraussichtlichen Kosten für die Beschaffung der Software nicht genau beziffert werden. Die zentrale Beschaffung einer entsprechenden Software für die Polizeien des Bundes und der Länder (vorzugswürdig) erscheint derzeitig aufgrund absehbarer Kostensteigerung eher unwahrscheinlich. Für monatliche Lizenzen für eine flexibel kündbare Anwendung ist bei sachsenweit 15 erforderlichen Lizenzen bei einem geschätzten Kostenansatz von

10.000 EUR pro Lizenzgebühr von jährlichen Betriebskosten von 150.000 EUR auszugehen. Für die Beschaffung der erforderlichen Monitore werden einmalige Investitionskosten in Höhe von 15.000 EUR veranschlagt und jährliche Sachkosten in Höhe von 60.000 EUR. Fallzahlen für die Schätzung der Anzahl künftiger präventiver Maßnahmen liegen nicht vor, da eine repressive Befugnis in der Strafprozessordnung nicht besteht.

- Befugniserweiterung zur Quellen-TKÜ (§ 66 Absatz 2 SächsPVDG)

Für die neu eingefügte Quellen-TKÜ kann als Ausgangsschätzwert die Anzahl entsprechender repressiver Maßnahmen zu Grunde gelegt werden. Die Nutzungsstatistiken des Bundesministeriums der Justiz und für Verbraucherschutz zeigen, dass die Quellen-TKÜ nach § 100a Strafprozessordnung im Jahr 2022 in Sachsen insgesamt sieben Mal angeordnet wurde.

Investitionskosten fallen nicht an, da entsprechende Technik vorhanden ist. Erforderliche Personalkosten sind fallabhängig und nicht bezifferbar.

Zusätzliche Kosten fallen infolge der Umsetzung der im Koalitionsvertrag verankerten Evaluierungsverpflichtung bezüglich der Befugnis zur Quellen-TKÜ an (siehe § 66 Absatz 6). Hierzu können – nach den Erfahrungen der letzten Evaluierung zu verschiedenen Vorschriften des Sächsischen Polizeivollzugsdienstgesetzes – Kosten von geschätzt 30.000 bis 50.000 EUR für die Haushaltsjahre 2027 (Abschlagszahlung) und 2028 oder 2029/30 (Restzahlung) angesetzt werden.

- Befugnis zum Einsatz von unbemannten Luftfahrtsystemen – Drohnen (§ 71 SächsPVDG)

In verschiedenen Organisationseinheiten des Polizeivollzugsdienstes kommen bereits Drohnen zur Überwachung zum Einsatz. Der Drohneneinsatz erfolgt zukünftig auf Grundlage einer spezialgesetzlichen Regelung. In der Regel sind diese Drohnen mit Technik zur Anfertigung von Luftbildern, Bildübertragung zum Zweck der Lagebeurteilung und Einsatzführung ausgestattet. Insgesamt verfügt die sächsische Polizei über 47 Drohnen. Davon werden derzeitig sechs Drohnen in zwei ausgewählten Polizeidirektionen eingesetzt, um im Rahmen eines Pilotprojekts die praktische Einführung und Wirksamkeit technischer Mittel zur Unterstützung vollzugspolizeilicher Aufgaben zu testen. Aus polizeifachlicher Sicht besteht Bedarf für den Erwerb von 20 weiteren Drohnen. Hierfür sind im Doppelhaushalt 2027/2028 bereits 300.000 EUR als reine Investitionskosten ausgewiesen.

- Befugnis zum Einsatz von Software zum Training von lernenden IT-Systemen (§ 79c SächsPVDG)

Kosten im Zusammenhang mit der Umsetzung der neuen Befugnis können nicht beziffert werden, da deren Höhe davon abhängig ist, ob entsprechende Software eigenentwickelt wird, externe Dienstleister in Anspruch genommen werden oder einer Bundeslösung (vorzugswürdig) „beigetreten“ werden kann. Welche Software in Betracht kommt, ist derzeitig nicht absehbar. Die Ergebnisse und die sich daraus ergebenden Kosten wären nach einer Marktanalyse unter haushälterischen Gesichtspunkten zu begutachten. Neben den Kosten für die zu beschaffende/entwickelnde Software wären zudem nicht bezifferbare Betriebskosten für Server zu berücksichtigen. Zusätzliche Kosten für Personal sind nicht zu erwarten.

- Befugniserweiterung zur Erhebung von den Notruf 110 begleitenden personenbezogenen Daten einschließlich Standortdaten eines Mobilfunkendgerätes (§ 86 Absatz 1 SächsPVDG)

Mit der neuen Regelung zur Erweiterung von Notrufverbindungen über andere Kommunikationsformen (bspw. mittels Notruf-Apps) und zur Standortdatenerhebung bei Notrufen über Mobilfunkendgeräte wird der Polizeivollzugsdienst zugleich als gemäß § 164 Absatz 1

Telekommunikationsgesetz örtlich zuständige Notrufabfragestelle in Sachsen bestimmt. Der Polizeivollzugsdienst Sachsen nimmt seit dem 8. November 2024 an einem Pilotprojekt zur Implementierung und Pilotierung der Advanced Mobile Location (AML) Technologie teil, das durch Baden-Württemberg federführend für alle Länder betrieben wird. Nach Abschluss der Pilotphase bei der beteiligten Polizeidirektion Dresden ist ein sukzessiver Anschluss aller Polizeidirektionen vorgesehen. Im Rahmen des Pilotprojekts fallen derzeitig keine Kosten an. Für den bundesweiten Dauerbetrieb wird von einem niedrigen sechsstelligen Betrag ausgegangen, der voraussichtlich über den Königsteiner Schlüssel auf die Länder verteilt wird. Ein konkreter Zeitpunkt hierfür ist nicht bekannt. Zusätzliche Kosten für Personal sind nicht zu erwarten.

- Änderung der Bezeichnung Polizeiverwaltungsamtes in „Polizeipräsidium für Service und IT“ (§ 97 Absatz 2 Nummer 3 SächsPVDG)

Die mit der Umbenennung verbundenen Sachkosten werden mit 3.000 EUR veranschlagt.

- Befugnis zur Ahndung und Verfolgung von Ordnungswidrigkeiten bei Zuwiderhandlungen gegen vollziehbare Anordnungen nach §§ 18 bis 20 oder nach § 21 Absatz 1 SächsPVDG (§ 106a SächsPVDG)

Mit Einführung der neuen Befugnis wurde die Möglichkeit geschaffen, bei einem Verstoß gegen vollziehbare Anordnungen nach §§ 18 bis 21 Abs. 1 durch dessen Ahndung Einnahmen von bis zu 5.000 EURO zu erzielen. Mangels gesonderter Ausweisung in der Statistik können die zu erwartenden Einnahmen nicht näher beziffert werden.

2) Erfüllungsaufwand

a) Erfüllungsaufwand für die Bürgerinnen und Bürger

Das Gesetz bewirkt keinen Erfüllungsaufwand bei Bürgerinnen und Bürgern.

b) Erfüllungsaufwand für die Wirtschaft

Das Gesetz bewirkt keinen Erfüllungsaufwand bei der Wirtschaft

c) Erfüllungsaufwand für die Verwaltung

aa) Polizeivollzugsdienst

Der Gesetzentwurf sieht für das Sächsische Polizeivollzugsdienstgesetz klarstellende Befugnisregelungen, die Erweiterung bestehender Befugnisregelungen und die Aufnahme neuer Befugnisregelungen vor. Der jährliche Erfüllungsaufwand ist abhängig vom Umfang des künftigen polizeifachlichen Realisierungsbedarfs, welcher lage- und erforderlichkeitsabhängig ist.

Demzufolge ist der dem Polizeivollzugsdienst entstehende einmalige sowie wiederkehrende Mehraufwand infolge der Neuregelungen sowohl hinsichtlich des Umfangs, als auch im Hinblick auf die zeitliche Einordnung grundsätzlich nicht ermittelbar bzw. kann allenfalls nur grob geschätzt werden. Dabei kann grundsätzlich davon ausgegangen werden, dass infolge von Technikeinsatz, insbesondere durch neue Softwarelösungen, die Polizeiarbeit insgesamt erleichtert wird, wodurch einerseits Zeitersparnisse entstehen und andererseits Personalressourcen eingespart werden bzw. in der Gesamtbilanz nicht zu einem höheren Aufwand in der Gesamtbewältigung eines Gefahrensachverhaltes führen.

bb) Polizeibehörden

Normadressat der Änderungen im Sächsischen Polizeivollzugsdienstgesetz ist der Polizeivollzugsdienst, so dass die Neuregelung keinen Erfüllungsaufwand bei den Polizeibehörden bewirken. Die Änderungen im Sächsischen Polizeibehördengesetz bedingen keinen Erfüllungsaufwand.

cc) Sächsische Datenschutz- und Transparenzbeauftragte

Die neuen oder ergänzten Befugnisregelungen in den § 57a Absatz 1 Satz 4 und Absatz 2, § 58, § 60, § 61, § 62a, § 62b und § 66 führen zu einer Erweiterung der Kontrollen der Sächsischen Datenschutz- und Transparenzbeauftragten gemäß § 94 SächsPVDG. Der zusätzliche Zeitaufwand für die gesetzeskonforme Prüfung wird durch die Sächsische Datenschutz- und Transparenzbeauftragte mit ca. 565 Stunden geschätzt.

dd) Justiz

Der Umfang der durch die Neuregelungen im sächsischen Polizeirecht ausgelösten personellen Mehrbelastungen im Bereich der Justiz hängt insbesondere von der Zahl zusätzlicher gerichtlicher Antragsverfahren ab. Mit Blick auf die neuen Verfahren für richterliche Anordnungen in Bezug auf

- Datenweiterverarbeitung von durch Bodycam-Einsatz in Wohnungen erlangten Daten (§ 57 Absatz 8 Satz 6)

- besondere Datenverarbeitungsbefugnis im Hinblick auf Daten aus einer Videoüberwachung (§ 57a Absatz 3 Satz 1)

- Verlängerung der Ausschreibung zur verdeckten Beobachtung (§ 60 Absatz 3 Satz 2)

- biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§ 62b Absatz 3 Satz 1)

- Quellen-TKÜ (§§ 66 Absatz 4 Satz 1)

und die Erweiterung der Befugnis zur elektronischen Aufenthaltsüberwachung (§ 61 Absatz 3 Satz 1) wird vorläufig von einer Näherungsschätzgröße von insgesamt jährlich zusätzlichen ca. 500 gerichtlichen Verfahren ausgegangen. Der insoweit mögliche künftige Geschäftsanfall der Gerichte für die erforderlichen richterlichen Anordnungen wird landesweit auf 0,26 Arbeitskraftanteile (AKA) eingeschätzt. Daran würde sich ein weiterer Personalbedarf im richterlichen Unterstützungsbereich (Laufbahngruppe 1, Einstiegsebene 2, ehemals mittlerer Dienst) anschließen, der vom Staatsministerium der Justiz landesweit mit 0,53 AKA eingeschätzt wird.

Eine valide Gesamtschätzung ist abhängig von der Anzahl zukünftiger Verfahren und derzeit nicht möglich.

2) weitere Gesetzesfolgen

Soweit Gesetze oder Rechtsverordnungen, bei denen keine Änderungen im vorliegenden Referentenentwurf vorgenommen wurden, auf das Sächsische Polizeivollzugsdienstgesetz verweisen bzw. Bezug nehmen, sind Anpassungen durch die Ressorts im Rahmen ihrer eigenen Rechtssetzung vorzunehmen.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Sächsischen Polizeivollzugsdienstgesetzes)

Zu Nummer 1

Inhaltsübersicht

Die Änderungen des Inhaltsverzeichnisses ergeben sich aus den nachfolgenden Normanpassungen.

Zu Nummer 2

§ 3

Durch die Ergänzung in Satz 1 wird klargestellt, dass der Polizeivollzugsdienst, wenn er bei Gefahr in Verzug die erforderlichen unaufschiebbaren Maßnahmen trifft, im eigenen Namen mit rechtlicher Wirkung für den Freistaat Sachsen handelt. Erforderliche Folgemaßnahmen wie beispielsweise die Verwahrung, Rückgabe oder Verwertung von sichergestellten Gegenständen sind hingegen durch die jeweils zuständige Polizeibehörde zu treffen. So auch die Anordnung einer tierärztlichen Untersuchung eines aggressiven freilaufenden Hundes. Durch die ergänzende Regelung wird zudem klargestellt, dass unterschieden wird bei Maßnahmen, die in der Zuständigkeit der Polizeibehörden liegen oder Maßnahmen, die für andere Stellen (keine Gefahrenabwehrbehörden) erfolgen.

Zu Nummer 3

§ 4

Der Sächsische Verfassungsgerichtshof hat im Urteil vom 25. Januar 2024, Vf. 91.II-19 ausgeführt, das bei bestimmten eingriffsintensiven Befugnisregelungen des Sächsischen Polizeivollzugsdienstgesetzes (§§ 21 Absatz 2 Nummer 1, 60 Absatz 2 Nummer 1 und 2, § 61 Absatz 1 und 2, § 63, § 64, § 66, § 67, § 68) die bestehenden Eingriffsschwellen zu niederschwellig gefasst seien, da durch die Regelungssystematik des Inbezugnehmens von Straftatenkatalogen, die teilweise auch die Gefahr der Verhütung von solchen Straftaten genügen lassen, die bloße Vorbereitungshandlungen oder Rechtsgütergefährdungen unter Strafe stellen, erfasst wären (Beispiele seien die §§ 83, 84, 86, 89a, 129a und 129b StGB). Bei solchermaßen eingriffsintensiven Befugnissen sei verfassungsrechtlich gefordert, dass im jeweiligen Einzelfall zumindest auch tatsächliche Anhaltspunkte für eine Gefahr für das durch die jeweilige Straftat geschützte Rechtsgut vorliegen müssten.

Mit der Aufnahme einer Legaldefinition zu dem Begriff „Vorfeldstraftat“ wird in Ergänzung zu weiteren Anpassungen in den jeweiligen Befugnisvorschriften die bestehende Regelungstechnik geändert und die betreffenden Eingriffsschwellen dahingehend eingeschränkt, dass diese den Anforderungen des Sächsischen Verfassungsgerichtshofs jeweils genügen.

Der Begriff der „terroristischen Straftat“ findet im Sächsischen Polizeivollzugsdienstgesetz insbesondere Verwendung bei der Formulierung von Eingriffsschwellen für grundrechtsintensive Eingriffsbefugnisse wie beispielsweise die §§ 66 ff SächsPVDG, für die das Bundesverfassungsgericht bei Maßnahmen, die der Gefahrenabwehr dienen, gefordert hat, dass diese dem Schutz von besonders gewichtigen Rechtsgütern dienen müssen. Hierzu gehören, Leib, Leben und Freiheit der Person, sowie der Bestand oder die Sicherheit des Bundes oder eines Landes (siehe zuletzt BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rz. 132ff). Mit der Änderung der Regelung werden die Anforderungen des Bundesverfassungsgerichts umgesetzt und durch die Beschränkung auf die in § 129a Absatz 1 und 2 Nummer 2 bis 5 StGB genannten Straftaten, sichergestellt, dass nur solche Straftaten in Bezug genommen werden, die dem Schutz hochrangiger Rechtsgüter dienen.

Die Änderungen in den Nummern 7 bis 9 dienen der Korrektur eines redaktionellen Versehens.

Zu Nummer 4

§ 12a

Zweck der Regelung ist eine spezifische Befugnisregelung, die den Einsatz von technischen Mitteln zum Erkennen und zur Abwehr von unbemannten Land- Luft und Wasserfahrzeugsystemen erlaubt. Zum Zweck der Abwehr einer konkreten Gefahr durch unbemannte Fahrzeugsysteme darf die Polizei technische Mittel wie beispielsweise Laser, Jamming, GPS-Störung einsetzen sowie durch physische Mittel auf die unbemannten Fahrzeugsysteme einwirken (Satz 1). Zum Erkennen einer Gefahr kann die Polizei geeignete technische Mittel einsetzen (Satz 2).

Zu Nummer 5

§ 15

Mit der Änderung in Nummer 5 wird klargestellt, dass Personen, die sich in einem Fahrzeug befinden, das zur gezielten Kontrolle ausgeschrieben ist, einer Identitätsfeststellung unterzogen werden dürfen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme zur Abwehr einer Gefahr erforderlich ist.

Mit den Änderungen in den Nummern 6 und 7 werden die bisherigen Regelungsinhalte von Nummer 5 und 6 überführt und zugleich die gesetzlichen Verweise, die durch das Gesetz zur Änderung versammlungs- und polizeirechtlicher Vorschriften vom 22. Juli 2024 geändert wurden, angepasst. Nicht jede drohende Straftat gemäß § 24 des sächsischen Versammlungsgesetzes (SächsVersG) rechtfertigt die Einrichtung einer Kontrollstelle oder die Anordnung eines Kontrollbereichs, sondern nur die im Gesetz genannten Vorschriften (§ 24 Absatz 1 Nummer 3 und 4 sowie Absatz 2 Nummer 4 SächsVersG). Das Vorliegen einer konkretisierenden Anordnung nach §§ 9 Absatz 2,10 Absatz 2 oder 19 Absatz 3 SächsVersG oder § 31a Absatz 2 Sächsisches Polizeibehördengesetz (SächsPBG) ist für die Einrichtung einer Kontrollstelle oder die Anordnung eines Kontrollbereichs nicht Voraussetzung.

Das Sächsische Versammlungsrecht wurde im Rahmen der Novellierung von Strafnormen bereinigt, die nicht im Zusammenhang mit Versammlungen stehen. Deshalb wurde zur Verhinderung einer Strafbarkeitslücke die landesrechtliche Strafnorm im Bereich des Waffen-, Schutzausrüstungs-und Vermummungsverbots bei öffentlichen Veranstaltungen unter freiem Himmel bei besonderer Gefährdungslage für Leib, Leben, Gesundheit oder bedeutende Sach- oder Vermögenswerte in § 31a Sächsisches Polizeibehördengesetz geschaffen. Mit der Aufnahme des Verweises auf § 31a Sächsisches Polizeibehördengesetz in die Nummern 6 und 7 wird diesen rechtssystematischen Änderungen Rechnung getragen.

Die Änderungen der Nummern 8 und 9 sind Folge der Einfügung der neuen Ziffer 5.

Zu Nummer 6

§ 19

Die Bekämpfung von häuslicher Gewalt ist eine der polizeilichen Kernaufgaben. Nach dem Bundeslagebild des Bundeskriminalamts zu häuslicher Gewalt für das Kalenderjahr 2023 wurden 256.276 Menschen Opfer solcher Gewalt. Die sogenannte Istanbul-Konvention (Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häusliche Gewalt) verpflichtet Deutschland auf allen staatlichen Ebenen, solcher Gewalt vorzubeugen und sie zu bekämpfen. Zu den staatlichen Schutzinstrumenten

gehören auch Maßnahmen nach dem Polizeirecht. Zu diesem Zweck sind ergänzende Regelungen im Sächsischen Polizeivollzugsdienstgesetz vorgesehen (§ 19, § 61, § 84). Durch eine spezifische Befugnisregelung, die sämtliche relevante polizeiliche Standardmaßnahmen beinhaltet, sollen der Polizei klare Maßstäbe an die Hand gegeben werden, damit diese in den besonders eilbedürften Situationen Handlungssicherheit hat.

Dem Begriff häusliche Gewalt unterfallen alle Formen körperlicher, sexueller oder psychischer Gewalt. Er umfasst familiäre sowie partnerschaftliche Gewalt. Häusliche Gewalt liegt vor, wenn die Gewalt zwischen Personen stattfindet, die in einer familiären oder partnerschaftlichen Beziehung zusammenwohnen. Sie liegt auch vor, wenn sie unabhängig von einem gemeinsamen Haushalt innerhalb der Familie oder in aktuellen oder ehemaligen Partnerschaften geschieht (siehe Definition Häusliche Gewalt, Bundeslagebild 2022, BKA, S. 1). Mit dem Begriff „sonstige Nachstellungen“ sollen sog. „Stalking-Fälle“ gemäß § 238 Strafgesetzbuch erfasst werden.

Absatz 1

In Ergänzung der bisherigen Regelung werden in Absatz 1 Satz 1 weitere Standardbefugnisse zum Schutz vor häuslicher Gewalt sowie Nachstellung aufgenommen und eine einheitliche Eingriffsschwelle für alle Maßnahmen bestimmt. Neben der Wohnungsverweisung mit Rückkehrverbot und dem Kontaktverbot wurden als weitere Standardbefugnisse ein Annäherungsverbot, ein Betretungsverbot und ein Aufenthaltsverbot aufgenommen. Solche Maßnahmen konnten bisher auf der Grundlage von § 12 bzw. § 21 SächsPVDG, mit der Anforderung der konkreten Gefahr, angeordnet werden.

Satz 1: In Änderung der bestehenden Regelung wird die Eingriffsschwelle für sämtliche Standardbefugnisse von „gegenwärtiger Gefahr“ auf das Vorliegen einer „konkreten Gefahr“ für bestimmte Schutzgüter abgesenkt. Die Anknüpfung an eine gegenwärtige Gefahr ist bei den betreffenden Lebenssachverhalten nicht sachgerecht, da dieser Gefahrengrad im Unterschied zur konkreten Gefahr voraussetzt, dass das schädigende Ereignis bereits begonnen hat oder die Einwirkung unmittelbar oder in allernächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit bevorsteht (siehe Begriffsbestimmung in § 4 Nummer 3b) SächsPVDG). Vielfach wird die Sachlage zwar so gestaltet sein, dass bei räumlicher Nähe durch eine gemeinsam genutzte Wohnung oftmals erneute Rechtsgutsverletzungen jederzeit verwirklicht werden können und somit eine Dauergefahr besteht. Hängt hingegen jedoch die Gefahrenverwirklichung von äußeren Faktoren ab, wie etwa dem Konsum von Alkohol, kann eine Dauergefahr regelmäßig nicht angenommen werden. Zur effektiven Gefahrenabwehr wird die Eingriffsschwelle daher nicht vom Vorliegen einer besonderen Nähe des Schadensereignisses abhängig gemacht. In Änderung zur bestehenden Regelung wird der Kreis der geschützten Rechtsgüter auf Leben, Leib, Freiheit oder sexuelle Selbstbestimmung analog zum Gewaltschutzgesetz geändert.

Nummer 1 beinhaltet die Wohnungsverweisung und das Rückkehrverbot. Nummer 2 a) beinhaltet eine spezifische Befugnisregelung zur Erteilung von Aufenthaltsverboten, die die Regelung des § 21 verdrängt. Nummer 2 b) beinhaltet ein Betretungsverbot für bestimmte Orte, an denen sich die gefährdete Person oder ihr nahestehende Personen (Kinder am Kindergarten oder Schule) aufhalten. Nummer 2 c) das bisher bereits geregelte Kontaktverbot, Nummer 2 d) das Annäherungsverbot.

In den Sätzen 2 und 3 werden die bestehenden Regelungen zur Befristung übernommen. In Satz 4 wird der Regelungsinhalt des bisherigen Absatz 3 übernommen.

Zu Nummer 7

§ 21

Absatz 1

Die Neufassung von Satz 1 dient der Klarstellung der Abgrenzung der Anwendungsbereiche von räumlich begrenzten tatortbezogenen Aufenthaltsverboten nach Absatz 1 zu nichttatortbezogenen räumlich weitreichenden Aufenthaltsverboten nach Absatz 2. Für den Erlass eines räumlich begrenzten tatortbezogenen Aufenthaltsverbots nach Absatz 1 ist die Prognose einer Straftatenbegehung durch die betroffene Person an einem bestimmten Ort, in einem bestimmten Gemeindeteil oder einem bestimmten Gemeindegebiet ausreichend. Durch die sprachliche Fassung „bestimmter Ort“, ein bestimmtes Gebiet innerhalb einer Gemeinde oder ein Gemeindegebiet wird klarstellend die räumlich begrenzte Reichweite eines solchen Aufenthaltsverbots bestimmt. Im Hinblick auf das Erfordernis einer durch Tatsachen gestützten Straftatenprognose und angesichts des Beschränkungserfordernisses in räumlicher/zeitlich Hinsicht bedarf es neben den Regelungen der Sätze 2 und 3, die dies bereits sicherstellen, keiner gesetzlich bestimmten Höchstfrist. Typische Anwendungsfälle für Aufenthaltsverbote nach Absatz 1 sind Gefahren im Zusammenhang mit gewalttätigen Fußballfans oder Drogendealern. Mit den Sätzen 2 und 3 werden die bestehenden Regelungen zum Erfordernis der räumlich/zeitlichen Begrenzung eines Aufenthaltsverbots aus dem bisherigen Absatz 7 übernommen.

Absatz 2

Satz 1 beinhaltet die bisherigen Regelungen zum Aufenthaltsgebot und zum nichttatortbezogenen Aufenthaltsverbot. Im Unterschied zum Aufenthaltsverbot nach Absatz 1 kann ein Aufenthaltsverbot nach Absatz 2 durch die Begriffsverwendung „Bereich“ (analog § 68b Absatz 1 Nummer 1 Strafgesetzbuch) über das Gebiet einer Gemeinde hinaus und daher sogar bezogen auf den gesamten Freistaat Sachsen erteilt werden. In Satz 2 werden die Anforderungen des Sächsischen Verfassungsgerichtshofs an die gesetzgeberische Ausgestaltung der Eingriffsschwellen umgesetzt (siehe Begründung zu § 4 Nummer 6). Satz 3 übernimmt die Regelung aus dem bisherigen Absatz 3 zum Erlass eines Kontaktverbots. Satz 4 beinhaltet die Fristenregelung aus dem bisherigen Absatz 2 Satz 1. In Satz 5 erfolgt in Korrektur eines redaktionellen Versehens die Verkürzung der Verlängerungsfrist von drei (bisher geregelt in Absatz 7 Satz 5) auf zwei Monate.

Absatz 3

Absatz 3 beinhaltet die bisherige Regelung des Absatzes 4.

Absatz 4

Absatz 4 beinhaltet die bisherige Regelung des Absatzes 5.

Absatz 5

Absatz 5 beinhaltet die bisherige Regelung des Absatzes 6.

Absatz 6

In Absatz 6 wurde die Verpflichtung zur Evalutaion aus der bisherigen Regelung des Absatzes 8 mit einer neuen Fristsetzung übernommen.

Die Streichung der Absätze 7 und 8 erfolgt in Konsequenz der Änderungen in den Absätzen 2 bis 6.

Zu Nummer 8

§ 28

Die Änderungen erfolgen in Konsequenz von Änderungen in § 15.

Mit der Aufnahme der neu gefassten Nummern 6, 7 und 8 erfolgt in Umsetzung von Artikel 37 Absatz 5 VO (EU) 2018/1862 die erforderliche nationale Regelung zu den polizeilichen Befugnissen, wenn eine betroffene Person, die zur gezielten Kontrolle ausgeschrieben ist, angetroffen wird.

Zu Nummer 9

§ 29

Mit der Änderung in Satz 1 durch den Verweis auf § 104 Absatz 3 der Strafprozessordnung wird der Beschluss des Bundesverfassungsgerichts vom 29. März 2019, 2 BvR 675/14, Rz. 66 umgesetzt und geregelt, dass die Nachtzeit ganzjährig die Zeit zwischen 21.00 Uhr und 6 Uhr erfasst. Infolge der Aufnahme der Verweisung ist Satz 3 zu streichen.

Zu Nummer 10

§ 40

Absatz 4

Der Einsatz von Vorrichtungen für den Abschuss von besonderen Formen von Projektilen, bspw. Distanz-Elektroimpulsgeräte bzw. Taser, ist nach der geltenden Rechtslage den polizeilichen Spezialeinheiten vorbehalten. Mit der vorgesehenen Aufhebung dieser Beschränkung wird die Möglichkeit eröffnet, generell Beamtinnen und Beamte des Polizeivollzugsdienstes mit diesem Einsatzmittel auszustatten. Die Ausstattung dieser Einsatzkräfte bedarf auch weiterhin der ausdrücklichen Zulassung durch das Sächsische Staatsministerium des Innern. Damit bleibt sichergestellt, dass die Ausgabe des Einsatzmittels praxis- und bedarfsorientiert an hierfür ausgebildete Einsatzkräfte erfolgt.

Mit der Freigabe des Einsatzmittels für den gesamten Polizeivollzugsdienst kann effektiver und gleichzeitig in verhältnismäßiger Weise auf Bedrohungslagen reagiert werden, mit denen in fast allen Einsatzlagen, bspw. des Streifendienstes, gerechnet werden muss. Es ermöglicht ein abgestuftes Vorgehen bei der Lagebewältigung, indem anstelle des tödlich wirkenden Schusswaffengebrauchs als bislang letztes zur Verfügung stehendes Mittel zur Abwehr einer Leib- oder Lebensgefahr nunmehr gewalttätige Angreifer aus sicherer Distanz mit einem geringen Verletzungsrisiko überwältigt werden können. Zudem zeigen Erfahrungen aus anderen Bundesländern, dass der Einsatz des Tasers ein bewährtes Einsatzmittel ist und bereits die Androhung der Anwendung des Einsatzmittels deeskalierend wirken kann.

Absatz 5

In Absatz 5 wurde eine Verpflichtung zur Evaluierung aufgenommen. Hierdurch soll sichergestellt werden, dass die Ausweitung des Einsatzes von Distanz-Elektroimpulsgeräten auf Beamtinnen und Beamten des Polizeivollzugsdienstes evaluiert wird.

Zu Nummer 11

§ 41

Mit der Änderung in Satz 3 erfolgt die Korrektur eines redaktionellen Versehens.

Zu Nummer 12

§ 48

Mit der Änderung in Absatz 3 Satz 2 erfolgt die Korrektur eines redaktionellen Versehens.

Zu Nummer 13

§ 57

Absätze 4 bis 8

Mit der Neufassung der Regelungen in den Absätzen 4 bis 8 wird die bestehende gesetzliche Regelung für den Einsatz von Bodycams in öffentlich zugänglichen Bereichen auf den Bereich von Wohnungen erweitert. Die Erweiterung des Einsatzes auf Wohnungen entspricht einem praktischen Bedürfnis. Gerade in Wohnungen können die polizeilichen Einsatzkräfte – etwa bei Wohnungsverweisungen im Zusammenhang mit häuslicher Gewalt – auf Situationen treffen, in denen die betroffenen Personen unter hohem Stress stehen und auf Einsatzmaßnahmen besonders aggressiv reagieren. In kritischen Situationen dieser Art kann der Einsatz der Bodycam eine deeskalierende Wirkung entfalten und die eingesetzten Kräfte vor Angriffen schützen.

Absatz 4

Absatz 4 regelt die Anforderungen an das sog. Pre-Recording in Wohnungen. Satz 1 entspricht der bestehenden Regelung in Absatz 4 Satz 1 zum sog. Pre-Recording in öffentlich zugänglichen Bereichen unter Beibehaltung der bisherigen Eingriffsschwelle. Ergänzend wurde zur Klarstellung aufgenommen, im Kontext welcher Aufgabenerfüllung ein Pre-Recording erfolgen kann. Satz 2 beinhaltet neu die Befugnis zum Pre-Recording in Wohnraum mit der Eingriffsschwelle der „dringende Gefahr“. Satz 3 neu bestimmt im Hinblick auf den weiten Wohnraumbegriff des § 29 Absatz 5 eine Ausnahme von den Anforderungen des Satzes 2. Der Schrankenregelung des Artikel 13 Absatz 7 Grundgesetz (Artikel 30 Absatz 3 Sächsische Verfassung) wurde dadurch Rechnung getragen, dass es sich bei den Rechtsgütern Leib oder Leben um besonders gewichtige Rechtsgüter handelt. Die Dringlichkeit der Gefahr im Sinne des Artikel 13 Absatz 7 Grundgesetz bezieht sich nicht auf die Wahrscheinlichkeit des Schadenseintritts, sondern auf den Umfang des drohenden Schadens.

Absatz 5

Absatz 5 bestimmt, unter welchen Anforderungen Aufzeichnungen von Bild- und Tondaten durchgeführt werden dürfen. Satz 1 beinhaltet die bisherigen Anforderungen an die Aufzeichnung von außerhalb von Wohnungen aufgenommenen Bild- und Tondaten. Der neue Satz 2 beinhaltet die Anforderungen an die Aufzeichnung von Bild- und Tondaten, die innerhalb von Wohnungen aufgenommen wurden und fordert, dass dies zum Schutz von Polizeibediensteten oder Dritten gegen eine dringende Gefahr für Leib oder Leben erforderlich sein muss. Satz 3 überführt den Regelungsgehalt der bisherigen Regelung in § 57 Absatz 4 Satz 2 zur Löschungsverpflichtung, soweit die Voraussetzungen für eine Aufzeichnung nicht vorliegen.

Absatz 6

Satz 1 entspricht der Regelung des bisherigen Absatzes 7 Satz 2 und wurde an die Erweiterung der Befugnis auf Wohnraum angepasst.

Satz 2 (neu) enthält im Hinblick auf den Einsatz von Bodycam in Wohnungen und der damit verbundenen möglichen Kernbereichsrelevanz die Verpflichtung zur Unterbrechung von Aufzeichnungen, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass der Kernbereich privater Lebensgestaltung betroffen ist. Satz 3 (neu) regelt, wann die Fortsetzung der Maßnahme erfolgen darf. Satz 4 (neu) enthält ein Verwendungsverbot und die Löschungsverpflichtung für Kernbereich-relevante Daten. Satz 5 (neu) bestimmt besondere Dokumentationspflichten, soweit Kernbereichs-relevante Daten erfasst wurden. Satz 6 (neu) regelt eine enge Zweckbeschränkung der Dokumentation nach Satz 5.

Absatz 7

Absatz 7 Satz 1 entspricht der Regelung des bisherigen Absatzes 6 Satz 1 und wurde ergänzt um die Anforderung, dass der Einsatz durch einen optischen oder akustischen Warnhinweis besonders erkennbar zu machen ist. Die Sätze 2 und 3 entsprechen den bisherigen Regelungen in Absatz 6 Sätze 2 und 3.

Absatz 8

Satz 1 entspricht der Regelung des bisherigen Absatzes 7 Satz 1.

Die Sätze 2, 3 und 5 entsprechen den Regelungen des bisherigen Absatzes 7 Sätze 3 bis 5.

Satz 4 (neu) beinhaltet die Verpflichtung zur Information der betroffenen Personen über das Recht auf Einsichtnahme.

Satz 6 (neu) regelt, dass die weitere Verarbeitung von in Wohnraum aufgezeichneten Daten nur zulässig ist, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt wurde. Für das Verfahren gelten gemäß Satz 7 neu bestimmt die Regelungen des Buches 1 des FamFG für entsprechend anwendbar.

Absatz 9

Mit § 57 Absatz 9 wird eine neue Rechtsgrundlage geschaffen, die der Polizei die präventive Überwachung von fahrzeugführenden Personen ermöglicht, die infolge des Begehens einer bedeutenden Ordnungswidrigkeit erhebliche Gefährdungen für den Straßenverkehr und damit für Leib und Leben hervorrufen. Zu den polizeilichen Aufgaben gemäß § 2 Absatz 1 SächsPVDG zählt auch die staatliche Verkehrsüberwachung. Denn die Gefahrenabwehr betrifft nicht nur die Abwehr selbst, sondern auch vorgelagerte Maßnahmen zu deren Verhütung oder zur Vorbereitung von Maßnahmen, die der späteren Gefahrenabwehr dienen. Sie schließt damit auch Vorfeldmaßnahmen speziell der Verhütung von Straftaten oder Ordnungswidrigkeiten ein (vgl. BVerfG, Urteil vom 27. Juli 2005 - 1 BvR 668/04 - Rz. 93 ff.). Bei der verdachtslosen Überwachung des betreffenden Verkehrsverstoßes scheidet eine Ermächtigung aus dem repressiven Straf- oder Ordnungswidrigkeitenrecht aus, da zunächst kein entsprechender Anfangsverdacht gegenüber allen Verkehrsteilnehmenden oder auch nur einer erheblichen Anzahl unter ihnen gegeben ist. Im Gegensatz zu üblichen Überwachungsmethoden mit hohem personellen und sachlichem Aufwand ist der offene Einsatz technischer Mittel insoweit generalpräventiv wirksamer zur Verhinderung des besonders gefahrgeneigten Verkehrsverstoßes nach § 23 Absatz 1a StVO, der die unerlaubte Nutzung elektronischer Geräte während der Fahrt verbietet. Die Ablenkung durch elektronische Geräte ist eine der Hauptunfallursachen bei schweren Personenschäden.

Im Rahmen eines noch nicht abgeschlossenen Pilotprojekts wird der präventive Einsatz von Drohnen zur Überwachung von Verkehrsverstößen getestet. Der offene Einsatz des Systems schärft das Bewusstsein der Verkehrsteilnehmer für die Einhaltung von Regeln und reduziert dadurch regelwidriges Verhalten. Dies belegen auch andere Projekte wie zuletzt in Rheinland-Pfalz, auf deren Grundlage Anfang 2025 in deren Polizeigesetz zur präventiven Verhütung der unerlaubten Nutzung von elektronischen Geräten eine entsprechende Rechtsgrundlage zur Verringerung von Unfällen geschaffen wurde (§ 30 Absatz 8 POG). Aus diesem Grund soll der Einsatz eines entsprechenden kameragestützten Systems in den Regelbetrieb überführt werden, wofür es einer bereichsspezifischen Ermächtigung bedarf.

Satz 1 ermächtigt die Polizei zum offenen Einsatz technischer Mittel zur Bildübertragung und -aufzeichnung im öffentlichen Verkehrsraum zur Verhütung der unerlaubten Nutzung elektronischer Geräte während der Fahrt. Eine solche Bildübertragung ist nur an solchen Örtlichkeiten und Verkehrsbereichen gerechtfertigt, bei denen tatsächliche Anhaltspunkte bestehen, dass in regelmäßiger Weise gegen die genannte Vorschrift verstoßen wird oder

es sich in sonstiger Weise um einen Bereich mit besonderer Unfallträchtigkeit handelt. Damit wird eine flächendeckende Anwendung aus Gründen der Verhältnismäßigkeit ausgeschlossen.

Satz 2 regelt, welche Daten aufgezeichnet werden dürfen: Fahrzeug, Kennzeichen, Fahrtrichtung, Zeit und Ort sowie die fahrzeugführende Person.

Satz 3 regelt die unverzügliche Löschung der Daten, wenn kein Verkehrsverstoß feststellt wird. Damit wird eine unverzügliche Überprüfung nach systemseitig festgestellten Verstößen gefordert. Bei nicht bestätigten Verstößen sind die Daten sofort und spurenlos zu löschen.

Satz 4 schreibt eine enge Zweckbindung vor: Die nicht gelöschten Daten dürfen ausschließlich zur Verfolgung und Ahndung der betreffenden Verstöße verarbeitet werden. Bei erkannten Verstößen erfolgt der Übergang in das repressive Verfahren nach § 100h Absatz 1 Satz 1 Nummer 1 StPO i. V. m. § 46 Absatz 1 OWiG.

Absatz 10

Absatz 10 entspricht der Regelung des bisherigen Absatz 8.

Absatz 11

Absatz 11 beinhaltet eine geänderte Evaluierungsklausel beschränkt auf den Einsatz von Bodycam in Wohnraum.

Absatz 12

Absatz 12 entspricht der Regelung des bisherigen Absatz 10.

§ 57a

Anknüpfend an den bestehenden Rechtsrahmen des § 57 Absatz 2 und 3 Sächsisches Polizeivollzugsdienstgesetz, der eine offene Beobachtung und Aufzeichnung von Bilddaten u.a. an Kriminalitätsbrennpunkt-Bereichen oder bei Ansammlungen ermöglicht, soll in Anlehnung an § 14 Absatz 8 HSOG durch eine Befugnis zur „intelligenten Videoüberwachung“ eine vollständige und ausreichend schnelle Auswertung des Bildmaterials ermöglicht werden, um mittels Kontrolle dieser Bereiche Gefahren frühzeitig zu erkennen und hierdurch die Begehung von Straftaten verhindern zu können. Aufgrund der begrenzten menschlichen Wahrnehmungsfähigkeiten, aber auch aufgrund des erheblichen zeitlichen Aufwandes einer laufenden Auswertung von Bildmaterial soll der Einsatz von Bildanalysesoftware, die automatisiert bestimmte (Bewegungs-)Muster, die auf die Begehung von Straftaten hindeuten, erkennt, gesetzlich geregelt werden. Anknüpfend an eine erfolgte Mustererkennung und Verifizierung einer potentiell gefährlichen Situation durch polizeiliche Bedienstete soll durch gesetzliche Regelung bei Vorliegen bestimmter deutlich gesteigerter Gefährdungslagen eine biometrische Echtzeit-Fernidentifizierung auf der Grundlage der Datenbestände der polizeilichen Auskunfts- und Fahndungssysteme erfolgen können.

Darüber hinaus soll angelehnt an § 14 Absatz 9 HSOG daneben eine gesonderte Befugnis zur biometrischen Echtzeit-Fernidentifizierung aufgenommen werden (Absatz 2), um gezielt nach Personen suchen zu können, von denen die konkrete Gefahr oder die vorhersehbare Gefahr einer terroristischen Straftat ausgeht. Weiterer Regelungsbedarf für eine biometrische Echtzeit-Fernidentifizierung besteht für in den polizeilichen Auskunfts- und Fahndungssystemen gespeicherte biometrische Daten von Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie für vermisste Personen.

Flankierend sind in verfahrensrechtlicher Hinsicht Regelungen zum Richtervorbehalt, zu den Anforderungen an die polizeiliche Antragstellung, zur Transparenz, zur aufsichtlichen

Kontrolle und zur Gewährleistung effektiven Rechtsschutzes vorgesehen (siehe Ergänzungen in den § 73 ff, 94, § 107 SächsPVDG).

Absatz 1

Der neue § 57a Absatz 1 knüpft in Bezug auf die Zulässigkeit der Datenerhebung an den bestehenden Rechtsrahmen in § 57 Absatz 2 und 3 (u. a. Videoüberwachung an Kriminalitätsschwerpunkten, Ansammlungen) an und ermöglicht den Einsatz intelligenter Bildanalysesoftware nach einer unter Verhältnismäßigkeitserwägungen (zunehmende Eingriffsintensität/höhere Eingriffsschwelle) gestuft gestalteten Datenverarbeitungsbefugnis.

Satz 1 regelt die erste Stufe und erlaubt den Einsatz von Bildanalysesoftware bzw. intelligenter Videoüberwachung zur Erkennung von Mustern von auf der Grundlage von § 57 Absatz 2 und 3 rechtmäßig erhobenen personenbezogenen Daten an. Satz 3 regelt die zweite Stufe und erlaubt die Nachverfolgung nur solcher Personen, die eine Gefahr nach Satz 3 verursachen. Satz 4 regelt die dritte und letzte Stufe und erlaubt die biometrische Echtzeit-Fernidentifizierung. Die Befugnisregelungen der Sätze 2 und 3 stellen dabei sicher, dass die Auswertung von Trefferfällen nicht automatisiert, sondern durch den Menschen erfolgt.

Satz 1 ermöglicht so durch den Einsatz von Bildanalysesoftware auf der Grundlage künstlicher Intelligenz (KI) eine tatsächliche Kontrolle von Kriminalitätsschwerpunkten, die aufgrund menschlich begrenzter Wahrnehmungsfähigkeiten nicht möglich wäre, um Gefahren frühzeitig zu erkennen und hierdurch die Begehung von Straftaten zu verhindern oder die weitere Tatausführung zu unterbinden sowie um Opfer zu schützen. Ziel der Mustererkennung ist zunächst die Identifikation von Gefahrensituationen. Die Zuordnung potenziell gefährlicher Gegenstände oder Bewegungen zu einer Person findet dabei nicht statt. Gegenstand der Auswertung sind nur Bilddaten, nicht hingegen Tondaten.

Nummer 1 eröffnet den Einsatz von Bildanalysesoftware, die automatisiert Bewegungsmuster erkennt und auswertet, die auf die Begehung einer Straftat hindeuten.

Nummer 2 ermöglicht durch den Einsatz von Bildanalysesoftware das Erkennen von Mustern bezogen auf Waffen im Sinne des § 1 Absatz 2 des Waffengesetzes, Messer und gefährliche Gegenstände. Bei Ansammlungen, Veranstaltungen, öffentlich zugänglichen Orten wie Bahnhöfen oder Kriminalitätsschwerpunkten können bestimmte Gegenstände bereits aufgrund ihrer Beschaffenheit oder der Art und Weise, wie sie eingesetzt werden, als gefährlich gelten (Gegenstände wie Scheren, Hämmer, Schraubendreher, Äxte, Metallstangen oder Baseballschläger, andere scharfe oder spitze Objekte). Ein Gegenstand gilt erfahrungsgemäß als gefährlich, wenn er von der Art oder Beschaffenheit her potenziell dazu geeignet ist, eine erhebliche Verletzung zu verursachen, auch wenn er nicht unmittelbar als Waffe gedacht ist. Darunter fallen auch unbeaufsichtigte Gepäckstücke, die als sogenannte unkonventionelle Spreng- und Brandvorrichtungen eingesetzt werden können. Die schnellstmögliche Erkennung solcher Gegenstände ist für eine effektive Gefahrenabwehr unerlässlich.

Wesensmerkmal der eingesetzten Technik ist ein bereits austrainiertes und ausgelerntes System, das die einzelnen Bildaufzeichnungen in Echtzeit auswertet und dadurch auffällige Bewegungsmuster aufspüren bzw. kenntlich machen kann. Die verwendeten KI-Modelle werden von dem jeweiligen Anbieter trainiert und sind als solche unveränderlich vorprogrammiert, d. h. die eingesetzten Modelle lernen nicht auf Grundlage der polizeilichen Daten weiter. Eine Verknüpfung oder ein Abgleich mit gespeicherten Daten findet nicht statt. Es werden lediglich tatsächliche Geschehensabläufe mit abstrakten Bewegungsmustern abgeglichen, um ein polizeilich relevantes Verhalten zu identifizieren. Personenbezogene Daten sind daher nicht bzw. nur in einem sehr geringfügigen Umfang betroffen. Durch die Mustererkennung erfolgt zwar eine quantitative Steigerung der Datenverarbeitung, die, da die Auswertung aber nicht auf der Grundlage personenbezogener Merkmale erfolgt, jedoch

nicht eingriffsintensiver ist, als die Datenerfassung im Vergleich zur konventionellen Videoüberwachung.

Satz 2 verpflichtet die Polizei nach erfolgreicher Mustererkennung durch die Technik („Alarmmeldung“ in Form einer optischen Markierung bzw. Kennzeichnung der Gefahrensituation) zur unverzüglichen Überprüfung am Überwachungsmonitor, ob mit Straftaten von erheblicher Bedeutung (§ 4 Nummer 4) in absehbarer Zeit mit hinreichender Wahrscheinlichkeit gerechnet werden kann. Alle weiteren Schritte unterliegen damit einer zwischengeschalteten menschlichen Überprüfung.

Sofern die Voraussetzungen nach Satz 2 vorliegen, kann die Polizei nach Satz 3 eine automatisierte Nachverfolgung einer Zielperson im Sinne von Satz 2 durch ihre Kennzeichnung in den vorliegenden Bildübertragungen und -aufzeichnungen vornehmen. Durch eine KI-gestützte Trackingfunktion können — vor allem in unübersichtlichen Lagen wie Menschenmengen — sodann potenzielle Straftäterinnen oder Straftäter auf den Bildaufzeichnungen verfolgt werden. Bis zu diesem Zeitpunkt erfasst die Bildanalysesoftware die potenziell gefährliche Situation bzw. die potenziellen Störer automatisch. Liegen die Voraussetzungen des Satzes 2 nicht vor, hebt die Beobachterin oder der Beobachter am Überwachungsmonitor die konkrete Erfassung der jeweiligen Personen auf.

Durch Satz 4 wird die Rechtsgrundlage zur biometrischen Echtzeit-Fernidentifizierung im Stufenmodell geschaffen. Ein biometrisches Echtzeit-Fernidentifizierungssystem ist ein System i. S. d. Artikel 3 Nummer 42 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 (KI-VO). Satz 4 stellt dabei die dritte und letzte Stufe des Stufenmodells dar. Aufgrund der hohen Eingriffstiefe bedarf es nach Satz 4 insoweit deutlich gesteigerter Anwendungsvoraussetzungen (erhebliche gegenwärtige Gefahr für Leben oder körperliche Unversehrtheit) im Vergleich zu Stufe 1 und 2 (Sätze 1 und 3). Gleichzeitig muss die Abwehr dieser Gefahr auf diese Weise unbedingt erforderlich sein. Bei Vorliegen und Bestätigung einer solchen tatsächlichen Gefahrensituation durch die Polizei kann diese nach richterlicher Anordnung oder bei Gefahr im Verzug unverzüglich eine biometrische Echtzeit-Fernidentifizierung anhand der Datenbestände der polizeilichen Auskunfts- und Fahndungssysteme veranlassen. Dadurch können effektiv Menschenleben geschützt und schwere Straftaten verhindert werden. Die automatisierte Datenanalyse und der Einsatz von KI ermöglichen einen schnellen Abgleich und eine Identifizierung der Person. Zugleich dient die Maßnahme nur der Identifizierung von bestimmten Personen, d. h. verbotene Praktiken im Sinne der KI-VO, wie z. B. Risikobewertung oder Kategorisierung, bleiben ausgeschlossen.

Absatz 2

Durch die Regelung in Satz 1 wird eine – neben der Regelung des Absatzes 1 stehende - spezifische Befugnis zum Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme zur gezielten Suche nach Personen, die eine bestehende oder vorhersehbare Gefahr durch die Begehung einer terroristischen Straftat verursachen, in das Sächsische Polizeivollzugsdienstgesetz aufgenommen. Die Regelung orientiert sich eng an dem von Artikel 5 Absatz 1 Ziffer h) ii) der KI-VO gesetzten Regelungsrahmen. Satz 2 enthält eine spezifische Befugnisregelung zum Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme zur gezielten Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung oder von vermissten Personen. Auch diese Befugnisregelung hält den durch Artikel 5 Absatz 1 Ziffer h) i) KI-VO gesetzten Regelungsrahmen ein und greift deren Wortlaut auf. Ein Abgleich der erhobenen Daten darf nur mit Daten erfolgen, die durch Maßnahmen nach § 57 Absatz 2 und 3 erhoben wurden. Die Befugnisse nach Satz 1 und 2 dürfen nur dann angewandt werden, wenn die Suche nach den Personen auf diese Weise unbedingt erforderlich ist. Satz 2 sichert im Hinblick auf die vom Sächsischen Verfassungsgerichtshof durch Urteil vom 25. Januar 2024, Vf. 91-II-19, Seite 54) erfolgte Rechtsprechung zur gesetzgeberischen Gestaltung von Eingriffsschwellen im Vorfeld von Gefahren, die Einhal-

tung der verfassungsrechtlich geforderten Eingriffsschwelle. Satz 3 stellt sicher, dass Maßnahmen nach Satz 1 und 2 in zeitlicher und räumlicher Hinsicht auf das unbedingt erforderliche Maß zu begrenzen sind.

Absatz 3

Gemäß den Anforderungen in Artikel 5 Absatz 3 Unterabsatz 2 der KI-VO und im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts (Urteil vom 20. April 2016, 1 BvR 966/09, Rz. 117) werden die Maßnahmen nach Absatz 1 Satz 4 und Absatz 2 unter Richtervorbehalt und unter den Vorbehalt der Behördenleitungsanordnung gestellt. Satz 2 stellt die vollständige Information durch die antragstellende Behörde über den zu beurteilenden Sachverhalt durch substantiierte Begründung des Antrags sicher. Die Beantragung der Maßnahme und auch deren Anordnung bei Gefahr in Verzug wird unter Behördenleiteranordnung gestellt (Satz 3).

Ergänzend gelten die Regelungen über die Anordnung und gerichtliche Zuständigkeit in § 73. Über § 73 Absatz 1 Nummer 2 besteht das Schriftformerfordernis für die richterliche Anordnung und für die Anordnung bei Gefahr in Verzug.

Absatz 4

Satz 1 verpflichtet, durch die von § 75 abweichende Regelung zur vollständigen Protokollierung der Maßnahme und sichert damit einerseits die Transparenz polizeilichen Handelns und andererseits die nachträgliche aufsichtliche Kontrolle. Die Regelung dient zusammen mit der Benachrichtigungspflicht nach § 74 Absatz 1 Nummer 5 auch der Gewährleistung effektiven Rechtsschutzes.

Durch die in Satz 2 geregelte Verpflichtung, die oder den Sächsische(n) Datenschutz- und Transparenzbeauftragte(n) über abgeschlossene Maßnahmen nach Absatz 1 Satz 4 oder Absatz 2 zu informieren, wird eine zeitnahe aufsichtliche Kontrolle gewährleistet.

Durch Satz 3 wird das Sächsische Staatsministerium des Innern beauftragt, das Nähere zum Verfahren, insbesondere unter Berücksichtigung der gesetzlich angeordneten Regelungsinhalte, durch zu veröffentlichende Verwaltungsvorschrift zu bestimmen. Klarstellend wurde auf die bereits nach § 39 Absatz 3 Sächsisches Datenschutz-Umsetzungsgesetz bestehende Pflicht zur Anhörung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten verwiesen.

§ 58

In Umsetzung der Rechtsprechung des Bundesverfassungsgerichts zu Kfz-Kennzeichenkontrollen in Bayern, Baden-Württemberg und Hessen (Beschluss vom 18. Dezember 2018 – 1 BvR 2795/09 und Beschluss vom 18. Dezember 2018 – 1 BvR 142/15) wurde die bestehende Regelung zur automatisierten Kennzeichenerkennung zur effizienteren Gefahrenabwehr neugefasst. Das Bundesverfassungsgericht hat in den bezeichneten Beschlüssen ausdrücklich die verdeckte Durchführung der Kennzeichenkontrolle verfassungsrechtlich für unbedenklich bewertet (siehe Urteil, Rz. 154). Im Hinblick auf den zulässigen Einsatz von Technik zur automatisierten Kennzeichenkontrolle zur Bekämpfung grenzüberschreitender Kriminalität hat das Gericht angeführt, dass der Gesetzgeber sicherstellen muss, dass nur Orte mit einem klaren Grenzbezug für Maßnahmen der automatisierten Kennzeichenerkennung bestimmt werden. Für Orte außerhalb des 30-km Bereichs müsse ein hinreichend klarer Grenzbezug durch gesetzliche Regelung sichergestellt sein (siehe Urteil, Rz. 149). Ferner hat das Gericht ausgeführt, dass automatisierte Kennzeichenerkennung aufgrund des erheblichen Eingriffsgewichts zum Schutz von Rechtsgütern von zumindest erheblichem Gewicht erfolgen muss.

Absatz 1

In Umsetzung der Rechtsprechung des Bundesverfassungsgerichts zur verfassungsrechtlichen Zulässigkeit verdeckter automatisierter Kennzeichenerkennung und zur Effektivierung polizeilicher Gefahrenabwehr wird durch die Ergänzung „ohne Wissen der Person“ in Satz 1 der verdeckte Einsatz erlaubt. In den Nummern 3 bis 5 werden die bereits bisher geregelten Anlassfälle für den Einsatz von technischen Mitteln zur anlassbezogenen automatisierten Kennzeichenerkennung in Umsetzung der Anforderungen des Bundesverfassungsgerichts an verhältnismäßige Eingriffsschwellen sprachlich ergänzt. Im Hinblick auf die Ausführungen des Bundesverfassungsgerichts, dass die automatisierte Kennzeichenerkennung dem Schutz von Rechtsgütern von zumindest erheblichen Gewicht oder sonst vergleichbaren öffentlichen Interessen dienen muss, aber auch im Hinblick auf die Ausgestaltung der Befugnis als verdeckte Maßnahme, wurden die bisherigen Anlassfälle „Verhinderung der Weiterfahrt mit einem gestohlenen oder abhandengekommenen Kraftfahrzeugkennzeichen“ und „Verhinderung der Weiterfahrt von Kraftfahrzeugen ohne ausreichenden Pflichtversicherungsschutz“ gestrichen. Mit der Neufassung der Nummer 2 wurde als neuer Anlass der Schutz der in § 15 Absatz 1 Nummer 3 bezeichneten Anlagen, Einrichtungen, Gebäude oder Objekte bei Vorliegen von Tatsachen, die auf die Begehung von Straftaten von erheblicher Bedeutung hinweisen, aufgenommen. In den Nummern 3 und 5 wurden Orte bzw. Anlassfälle getrennt aufgenommen, die bisher von Nummer 4 unter dem Aspekt der Bekämpfung der grenzüberschreitenden Kriminalität erfasst waren und angepasst. Aufgrund der Ausführungen des Bundesverfassungsgerichts, dass ein solcher Anlassfall als Eingriffsschwelle einer gesetzlichen Regelung bedarf, die einen klaren Grenzbezug des jeweiligen Kontrollorts bestimmen muss, bestand hier Anpassungsbedarf. Nummer 4 beinhaltet die bisherigen Regelungsinhalt von Nummer 5 mit weiteren verfassungsrechtlich erforderlichen Ergänzungen.

Satz 2 entspricht der bisherigen Regelung in Absatz 3 Satz 3.

Absatz 2

Satz 1 führt in Umsetzung der Rechtsprechung des Bundesverfassungsgerichts (BVerfG, a. a. a. O, Rz. 72ff) an, welcher Fahndungsbestand grundsätzlich herangezogen werden darf. Je nach dem Anlassfall, zu dem der Einsatz der Maßnahme im jeweiligen Einzelfall erfolgt, ist aus dem (möglichen) Abgleichsdatenbestand der jeweilige Abgleichsdatenbestand anlassabhängig zu bestimmen.

Satz 2 entspricht der bisherigen Regelung in Absatz 2 Satz 4, Satz 3 der bisherigen Regelung in Absatz 2 Satz 6. Satz 4 enthält die Klarstellung, dass ein Abgleich nur mit vollständig erfassten Kennzeichen erfolgen darf. In Umsetzung des Urteils des Bundesverfassungsgerichts (BVerfG, a. a. O., Rz. 72ff) werden in den Nummern 1 bis 4 präventive und repressive Fahndungsbestände (als mögliche Grundlage für den jeweils anlassbezogen zu bestimmenden Abgleichsdatenbestand) angeführt.

Absatz 3

Sätze 1 und 2 entsprechen den bisherigen Regelungen in Absatz 2 Sätze 1 und 2. Satz 3 enthält neu die Verpflichtung zum unverzüglichen manuellen Überprüfung eines Trefferfalls. Sätze 4 und 5 enthalten die Löschungsverpflichtung bei Nichtübereinstimmung (bisher Absatz 2 Satz 7) und soweit die manuelle Überprüfung zum Ausschluss eines Trefferfalls führt. Satz 6 entspricht der bisherigen Regelung in Absatz 3 Satz 4. Satz 6 bestimmt die Zulässigkeit der Weiterverarbeitung von Daten im Fall eines Treffers. Satz 7 stellt durch das Verbot der Protokollierung sicher, das zu löschende Daten nicht wiederherstellbar sind.

Absatz 4

Die Regelung entspricht der Bisherigen in Absatz 3 Satz 1.

Absatz 5

Die Regelung entspricht der Bisherigen in Absatz 4. Die Regelung zur Evaluierung wurde im Hinblick auf den durch die Staatsregierung geleisteten Bericht gestrichen.

Absatz 6

In Absatz 6 wurde die bisherige Verpflichtung zur Evaluation aus § 58 Absatz 5 unter Änderung der Fristsetzung aufgenommen.

Zu Nummer 14

§ 59

Gemäß § 108 Absatz 1 ist § 59 am 31. Dezember 2023 außer Kraft getreten. Mit der Streichung der Vorschrift wird dem Außerkrafttreten Rechnung getragen.

Zu Nummer 15

§ 60

Die Änderung der Vorschrift resultiert zum einen aus den Vorgaben des Sächsischen Verfassungsgerichtshofs zu den Anforderungen an die gesetzgeberische Gestaltung der Eingriffsschwelle (siehe auch Begründungen zu § 4 Nummer 6). Zum anderen erfolgte zur Umsetzung von Artikel 36 Absatz 4 Verordnung (EU) 2018/1862 die Erweiterung der bestehenden Ausschreibungsgründe auf den neuen Ausschreibungsgrund der „Ermittlungsanfrage“. Die Verordnung (EU) 2018/1862 bildet neben zwei weiteren EU-Verordnungen die Rechtsgrundlage für das Schengener Informationssystem (SIS) der dritten Generation. Das SIS der dritten Generation wurde mit zusätzlichen Funktionen am 7. März 2023 in Betrieb genommen. Zusätzlich zu der Ausschreibung zur verdeckten Kontrolle (polizeilichen Beobachtung) sowie der gezielten Kontrolle gibt es als neue Ausschreibungsart die sogenannte Ermittlungsanfrage. Auf nationaler Ebene bedarf es neben den bereits geregelten Befugnissen der verdeckten Kontrolle und der gezielten Kontrolle einer Rechtsgrundlage für die Ausschreibung zur Ermittlungsanfrage im Sächsischen Polizeivollzugsdienstgesetz.

Absatz 1

In Satz 1 wird die „Ermittlungsanfrage“ als weiterer Ausschreibungsgrund aufgenommen und zugleich für sämtliche Ausschreibungen eine einheitliche Befugnisschwelle bestimmt. Die Ausschreibung zur verdeckten Kontrolle stellt als Maßnahme, die der betroffenen Person nicht bekannt wird, eine Grundrechts-intensivere Maßnahme gegenüber den Ausschreibungen der gezielten Kontrolle oder der Ermittlungsanfrage dar, da letztere der betroffenen Person bekannt werden. Gleichwohl sah die bisherige Regelung für die Befugnis der gezielten Kontrolle eine höhere Eingriffsschwelle als für die verdeckte Kontrolle vor. Mit der Regelung einer einheitlichen Eingriffsschwelle für sämtliche Ausschreibungsarten wird dies korrigiert. Die bisherige Regelung zur Befugnis zur Ausschreibung von Kontakt- und Begleitpersonen wird aus Gründen der Verhältnismäßigkeit gestrichen.

Mit Satz 2 erfolgt die Anpassung an die Anforderungen des Sächsischen Verfassungsgerichtshofs zur Ausgestaltung von Eingriffsschwellen.

Absatz 2

Mit den Änderungen in Absatz 2 werden die im Fall eines Antreffens einer ausgeschriebenen Person oder Sache zulässigen Anschlussbefugnisse unter Berücksichtigung des neu aufgenommenen Ausschreibungsgrundes der „Ermittlungsanfrage“, unterscheidend nach Art der Ausschreibung, gesetzlich bestimmt. Nummer 1 beinhaltet die bisherige Regelung des § 60 Absatz 4 Satz 1, Nummer 2 beinhaltet die bisherige Regelung des § 60 Absatz 4

Satz 2 und präzisiert diese. Mit der Regelung in Nummer 3 wird im Hinblick auf den Ausschreibungsgrund der Ermittlungsanfrage klarstellend auf die Befugnis der Befragung verwiesen.

Absatz 3

In den Sätzen 1 und 2 wurden die Regelungen des bisherigen § 60 Absatz 5 Sätze 1 und 2 übernommen. In Satz 3 wurde zur verfahrensrechtlichen Sicherung der Einhaltung der gesetzlichen Anforderungen ein Richtervorbehalt als Voraussetzung für die Verlängerung einer Anordnung zur Ausschreibung zur Mitteilung über die verdeckte Kontrolle als eingriffsintensiver Maßnahme aufgenommen. In den Sätzen 4 bis 6 wurden die Regelungen des bisherigen § 60 Absatz 5 Sätze 3 bis 5 übernommen.

Absatz 4

In Absatz 4 wird der Regelungsinhalt des bisherigen § 60 Absatz 6 übernommen.

§ 61

Zielstellung der Neufassung der Vorschrift ist die Umsetzung der Vorgaben des Sächsischen Verfassungsgerichtshofs im Hinblick auf die erforderliche Einschränkung der Eingriffsschwellen. Zur Verbesserung der Bekämpfung von häuslicher Gewalt soll im Kontext der Umsetzung der Istanbul-Konvention eine spezifische Befugnisregelung für bestimmte Hochrisikofälle häuslicher Gewalt aufgenommen werden. Die Änderung der Regelungen in § 21 bedingen zudem Folgeanpassungen in § 61.

Absatz 1

Die Regelung in Satz 1 Nummer 1 (neu) beinhaltet zum Zweck der Verbesserung der Bekämpfung von häuslicher Gewalt eine neue, auf Hochrisikofälle von häuslicher Gewalt „zugeschnittene“ Befugnisregelung. Mit dieser ergänzenden Regelung erfolgt ein weiterer Baustein zur Bekämpfung häuslicher Gewalt aber auch im Hinblick auf sonstige Fälle von Nachstellung (Stalking). Nummer 2 beinhaltet die Regelung des bisherigen § 61 Absatz 2 unter Berücksichtigung der Änderungen des § 21. Nummer 3 beinhaltet die Regelung des bisherigen § 61 Absatz 1. Mit der Ergänzung in Satz 2 erfolgt die erforderliche Umsetzung der Vorgaben des Sächsischen Verfassungsgerichtshofs (siehe auch Begründung zu § 4 Nummer 6).

Absatz 2

In Absatz 2 wird der Regelungsinhalt des bisherigen § 61 Absatz 3 übernommen (siehe Sätze 1, 3 bis 6). Zur Klarstellung wurde in Satz 2 eine Regelung zur Erstellung eines Bewegungsbildes aufgenommen. Die zulässigen Verwendungszwecke von nach Satz 1 und 2 erhobenen Daten werden durch die in Satz 7 angepassten Regelungen zur Zweckbindung bzw. im Rahmen der Zweckänderung mit Anpassungen bestimmt. Satz 8 (neu) setzt die Vorgaben des Urteils des Sächsischen Verfassungsgerichtshofs um.

Absatz 3

In Absatz 3 wird der Regelungsinhalt des bisherigen § 61 Absatz 5 mit redaktionellen Folgeänderungen übernommen.

Absatz 4

In Absatz 4 wird der Regelungsinhalt des bisherigen § 61 Absatz 6 mit redaktionellen Änderungen übernommen. Der bisherige Regelungsinhalt von § 61 Absatz 4 wurde mangels gesetzlichen Regelungsbedarfs gestrichen.

Absatz 5

In Absatz 5 wurde der Regelungsinhalt des bisherigen § 61 Absatz 7 mit der Abweichung übernommen, dass für die Erstellung eines Bewegungsbildes bei Anordnungen nach Absatz 1 Nummer 3 kein Erfordernis ausdrücklicher richterlicher Anordnung besteht.

Absatz 6

Absatz 6 Satz 1 (neu) bestimmt, dass auf Antrag der Polizei die Erstellung eines Bewegungsbildes nur dann zulässig ist, wenn dies durch richterlichen Anordnung ausdrücklich gestattet ist. Die Sätze 2 bis 4 beinhalten die Regelungen des bisherigen § 61 Absatz 8 Sätze 1 bis 3.

Absatz 7

In Absatz 7 wurde die bisherige Verpflichtung zur Evaluation aus § 61 Absatz 9 unter Änderung der Fristsetzung aufgenommen.

Zu Nummer 16

§ 62a

Mit der neu aufgenommenen Regelung in § 62a wird die Polizei in die Lage versetzt, bereits vorhandene Informationen einfacher, schneller und wirksamer auszuwerten. Die informationstechnische Entwicklung der letzten Jahre ermöglicht es, bisher unverbundene automatisierte Dateien und Datenquellen auf einer Analyseplattform zusammenzuführen und die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen. Hierdurch können über die bisherigen Erkenntnismöglichkeiten hinaus Zusammenhänge zum Beispiel zwischen Personen oder Personengruppierungen und Handlungsmuster erkannt und dadurch die Wirksamkeit der vorbeugenden Straftatenbekämpfung gesteigert werden. In seinem Urteil vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) hat das Bundesverfassungsgericht grundsätzlich geklärt, unter welchen Voraussetzungen eine automatisierte Datenanalyse verfassungskonform geregelt werden kann. Die Verarbeitung gespeicherter personenbezogener Daten im Rahmen einer automatisierten Datenanalyse greift in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG in zweifacher Weise ein. Zum einen stellt die Nutzung der Daten über den ursprünglichen Anlass hinaus einen neuen Grundrechtseingriff dar, der nach dem Grundsatz der Zweckbindung gerechtfertigt sein muss. Zum anderen hat das Bundesverfassungsgericht in der bezeichneten Entscheidung der automatisierten Datenanalyse ein besonderes Eigengewicht zugewiesen, das über das Eingriffsgewicht der weiteren Verwendung vormals getrennter Daten hinausgeht (BVerfG, a. a. O., Rz. 50, 67 ff.). Für eine verfassungskonforme Ausgestaltung der automatisierten Datenanalyse ist eine Bestimmung dieses Eigengewichts erforderlich, das je nach Art und Umfang der einzubeziehenden Daten und der Methode der Analyse sehr unterschiedlich sein kann (BVerfG, a. a. O., Rz. 72 ff.). Die gesetzlichen Anforderungen für eine verfassungskonforme Regelung der Eingriffsschwellen bestimmen sich daher nach dem Eingriffsgewicht der automatisierten Datenanalyse und deren Gestaltung durch eingriffsminimierende Vorkehrungen und Schutzmaßnahmen. Zum Zweck einer praxistauglichen Anwendung der automatisierten Datenanalyse wird von der in der Entscheidung des Bundesverfassungsgerichts eröffneten Möglichkeit, die Regelungen zur Begrenzung der Eingriffsintensität zwischen dem Gesetzgeber und der Verwaltung aufzuteilen (BVerfG, a. a. O. , Rz. 110), Gebrauch gemacht. Zur Wahrung des Gesetzesvorbehalts werden jedoch die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden gesetzlich bestimmt. Auf der Ebene der Verwaltung sind durch eine unter Beteiligung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten zu erstellenden Verwaltungsvorschrift insbesondere weitere Vorgaben zur Begrenzung der Eingriffsintensität im Hinblick auf den jeweiligen Anwendungsfall zu bestimmen. Die allgemeinen Regelungen zur Datenverarbeitung

und zum Datenschutz gemäß dem Sächsischen Datenschutz-Umsetzungsgesetz, insbesondere zur Sicherheit der Datenverarbeitung und dem Erfordernis einer Datenschutz-Folgenabschätzung nach § 23 des Sächsischen Datenschutz-Umsetzungsgesetzes, bleiben hiervon unberührt. Das Bundesverfassungsgericht hat in seiner Entscheidung die „automatisierte Datenanalyse“ von einem „einfachen Datenabgleich“ abgegrenzt. Bei einem einfachen Abgleich erfolgt die Suche nach einem vorhandenen Datenbestand etwa über eine Person, indem im jeweiligen System die eingegebenen Daten des Betroffenen an den gespeicherten Daten vorbeigeführt werden. Der einfache Datenabgleich ist daher – so das Bundesverfassungsgericht – ein suchender Vergleich von Daten zur Feststellung von Übereinstimmungen (BVerfG, a. a. O. , Rz. 91). Demgegenüber bedingt die Zusammenführung, Verknüpfung und Auswertung von Datenbeständen auf einer Analyseplattform komplexere Formen des Datenabgleichs als die einfache Suche nach Übereinstimmungen zwischen einzelnen Datensätzen. Daraus folgt, dass eine automatisierte Datenanalyse über einen einfachen Datenabgleich hinausgeht und einer bereichsspezifischen Ermächtigungsgrundlage bedarf. Der Sächsische Verfassungsgerichtshof hat in seinem Urteil vom 25. Januar 2024 entsprechend formuliert und darauf verwiesen, dass die Regelung § 80 Absatz 1 SächsPVDG nicht zu automatisierten Datenanalysen oder -auswertungen ermächtige, die über ein automatisiertes Abrufverfahren nach § 85 hinausgehen (siehe Urteil a. a. O, Seite 118 letzter Absatz).

Absatz 1 regelt die Eingriffsschwellen und bezeichnet das technische Verfahren einer automatisierten Datenanalyse. Das technische Verfahren besteht aus zwei aufeinander aufbauenden Schritten, nämlich dem Zusammenführen von Daten aus unterschiedlichen Dateisystemen und der sich daran anschließenden Recherche innerhalb der zusammengeführten Datenbestände und deren automatisierter Analyse. Mit dem automatisierten Zusammenführen wird das strukturelle Problem, dass in den Beständen der Polizei Daten in unterschiedlichen Formaten und getrennten Dateien gespeichert sind, und damit nicht im selben Bearbeitungskontext gleichzeitig verfügbar sind, behoben. Daran knüpft die automatisierte Datenanalyse, die in einer Verknüpfung, Aufbereitung und Auswertung der zusammengeführten Datenbestände besteht, an. Der zweite Schritt, die zulässige Methode der automatisierten Datenanalyse, wird in Absatz 2 geregelt. Bei einer Maßnahme zur Abwehr einer konkreten Gefahr für hochrangige Rechtsgüter kann das Eingriffsgewicht vergleichsweise hoch sein, hingegen muss es bei der vorbeugenden Bekämpfung von Straftaten erheblich gesenkt werden (BVerfG, a. a. O., Rz. 110). Besondere Anforderung gelten für die verhältnismäßige Ausgestaltung des Eingriffsgewichts, wenn die automatisierte Datenanalyse bereits im Gefahrenvorfeld zur Anwendung kommen soll.

Satz 1 regelt in den Nummern 1 bis 3 drei unterschiedliche Eingriffsschwellen, die jeweils Anlass für eine automatisierte Datenanalyse sein können. Die Eingriffsschwellen stehen in Beziehung zum jeweiligen Eingriffsgewicht der automatisierten Datenanalyse, damit die Verhältnismäßigkeit der Maßnahme gewahrt bleibt. Mit der Verweisung auf § 79a wird sichergestellt, dass die weitere Nutzung der Daten im Rahmen der automatisierten Datenanalyse nach den Grundsätzen der Zweckbindung und Zweckänderung verfassungsrechtlich gerechtfertigt ist. Im Rahmen der automatisierten Datenanalyse können personenbezogene Daten sowohl zweckwahrend als auch zweckändernd weiterverarbeitet werden. Die weiterverarbeitende zweckwahrende Nutzung von Daten kommt dabei immer nur dann in Betracht, wenn die Voraussetzungen des § 79a Absatz 1 SächsPVDG vorliegen. Für die zweckändernde Verarbeitung gelten die Anforderungen des § 79a Absatz 2 SächsPVDG. Zur praktischen Umsetzung des verfassungsrechtlichen Grundsatzes der Zweckbindung erfolgt die Kennzeichnung der Daten entsprechend § 81 SächsPVDG.

Die Eingriffsschwelle in Nummer 1 sieht die engen Voraussetzungen vor, die allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten, indem das Vorliegen einer konkreten Gefahr (siehe Begriffsbestimmung in § 4 Nummer 3a SächsPVDG) für besonders gewichtige Rechtsgüter gefordert wird. Da der Eingriffsanlass mit dem Erfordernis einer konkreten Gefahr streng begrenzt ist und hohe Anforderungen an die zu schützenden Rechtsgüter gestellt werden (es muss sich um besonders gewichtige Rechtsgüter handeln),

darf das Eingriffsgewicht der Datenanalyse unter diesen Voraussetzungen vergleichsweise hoch sein. Liegen beispielsweise konkrete Hinweise auf einen bevorstehenden terroristischen Anschlag auf eine Großveranstaltung vor, dürfen die in eine Datenanalyse einzubeziehenden Daten nach Art und Umfang sowie die Verarbeitungsmethode weiter gefasst sein als in den Fällen der Nummern 2 und 3.

Die Eingriffsschwelle in Nummer 2 erlaubt weniger gewichtige Eingriffe, die nach der Rechtsprechung des Bundesverfassungsgerichts beim Vorliegen einer konkretisierten Gefahr bereits dann zu rechtfertigen sind, wenn sie dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht dienen, wie dies bei der Verhütung von Straftaten von zumindest erheblicher Bedeutung der Fall ist (BVerfG, a. a. O., Rz 107). Eine hinreichend konkretisierte Gefahr kann schon vorliegen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen darauf hinweisen, dass eine entsprechende Straftat begangen werden wird. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungs-maßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfG, a. a. O., Rz. 106).

Die Eingriffsschwelle in Nummer 3 regelt das Gefahrenvorfeld und bleibt hinter einer konkretisierten Gefahr zurück. Dies ist bei weniger gewichtigen Eingriffen zulässig, wenn sie dem Schutz besonders gewichtiger Rechtsgüter dienen (BVerfG, a. a. O., Rz. 107). Dabei muss der Gesetzgeber das erforderliche Rechtsgut nicht zwingend benennen, sondern er kann auch an entsprechende Straftaten anknüpfen. Dem verfassungsrechtlichen Erfordernis eines besonders gewichtigen Rechtsguts entspricht eine Begrenzung auf schwere und besonders schwere Straftaten. Nach der Rechtsprechung des Bundesverfassungsgerichts sind schwere Straftaten solche, die mit einer Höchststrafe von mindestens fünf Jahren Freiheitsstrafe und besonders schwere Straftaten solche, die mit einer Höchststrafe von mindestens zehn Jahren Freiheitsstrafe bedroht sind (vgl. BVerfG, Urteil vom 3. März 2004, 1 BvR 2378/98, Rz. 241). Maßgeblicher Anknüpfungspunkt für die Einordnung ist der abstrakte Strafrahmen, wie er vom Gesetzgeber für eine bestimmte Straftat festgelegt wird. Gesetzgeberisch kann daher an die Straftatenkataloge der §§ 100 a Absatz 2, 100 b Absatz 2 StPO angeknüpft werden. Satz 2 setzt die Rechtsprechung des Sächsischen Verfassungsgerichtshofs um. Satz 3 stellt sicher, dass die zu verhütende Straftat auch im Einzelfall schwer wiegt.

Absatz 2 stellt klar, dass es sich bei einer Datenanalyse lediglich um ein technisches Hilfsmittel handelt, das die bisherige Arbeitsweise der Polizei erleichtert, ohne sie grundlegend zu verändern. Die Analyseplattform darf keine Prognosesoftware in dem Sinne sein, dass sie eigenständig kriminelles Verhalten vorhersagt und die von einem Menschen zu treffende Sachverhaltsbewertung ersetzt. Sie darf lediglich ein technisches Hilfsmittel sein, das die Polizei bei ihrer Aufgabenwahrnehmung unterstützt, indem sie Informationen aus verschiedenen Dateisystemen zusammenführt. Die abschließende Bewertung der zusammengeführten Informationen bleibt Aufgabe der Polizei.

Aufgrund der voranschreitenden technologischen Entwicklungen ist es erforderlich, zur Gewährleistung einer effizienten Gefahrenabwehr den Rechtsrahmen auszuschöpfen und die Anwendung von KI-Systemen unter Berücksichtigung der Anforderungen der KI-VO bei der automatisierten Datenanalyse zu regeln. Dabei werden die Anforderungen des Bundesverfassungsgerichts (BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rz. 100ff.) umgesetzt. KI-Systeme können Anwendungen zur automatisierten Datenanalyse ergänzen, um unterschiedliche Datenformate schneller zusammenzuführen, Täternetzwerke schneller zu identifizieren, aus unstrukturierten Daten relevante Hinweise schneller erkennen zu können und mit vorhandenen polizeilichen Informationen abzugleichen und komplexe Analyseschritte zu ermöglichen. Die automatisierte Datenanalyse unterstützt die Polizei bei der Erfüllung ihrer Aufgaben, indem sie Informationen bereitstellt,

die es der Polizei ermöglichen, eigene Bewertungen, Prognosen und Entscheidungen zu treffen. Die automatisierte Datenanalyse muss reproduzierbare bzw. nachvollziehbare Ergebnisse erzeugen, die einer Gegenkontrolle grundsätzlich zugänglich sein müssen. Die Prognose, ob eine bestimmte Person mit hoher Wahrscheinlichkeit künftig Straftaten begehen wird, trifft ein Mensch und nicht der Algorithmus.

Satz 1 bestimmt, dass abschließende maschinelle Sachverhaltsbewertungen verboten sind. Die abschließende Bewertung der durch die automatisierte Datenanalyse bereitgestellten Informationen und die Entscheidung über die auf der Grundlage der bereitgestellten Informationen weiteren Maßnahmen verbleiben bei der Polizei. Satz 2 hebt hervor, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden dürfen (BVerfG, a. a. O., Rz. 100).

Satz 3 sichert die Funktion der Analyseplattform als bloßes Hilfsmittel für die polizeiliche Aufgabenwahrnehmung ab, indem klargestellt wird, dass die automatisierte Datenanalyse manuell ausgelöst wird.

Aus der Entscheidung des Bundesverfassungsgerichts ergibt sich, dass das Eingriffsgewicht der automatisierten Datenanalyse umso höher ist, je offener die Methode des Suchvorgangs gestaltet ist (BVerfG, a. a. O., Rz. 93). Die mit einer offenen Suche verbundenen Gefahren können durch eine Einschränkung der Datenverarbeitungsmethode gesenkt werden, wenn der Suchvorgang eingrenzend so geregelt ist, dass er einen Bezug zu einem konkreten Suchanlass voraussetzt. Diese Konkretisierung erfolgt durch den Verweis, dass die automatisiere Datenanalyse zum einen auf der Grundlage von „Suchkriterien“ zu erfolgen hat und zum anderen, in dem diese bei den Eingriffsanlässen von Absatz 1 Nummer 2 und 3 „auf die nach den §§ 6 und 7 Verantwortlichen auszurichten ist“, Satz 4. Diese gesetzlichen Vorgaben dienen der weiteren Eingriffsminimierung gemäß den Vorgaben des Bundesverfassungsgerichts. Die mit einer offenen Suche verbundenen Gefahren können durch eine Einschränkung der Datenverarbeitungsmethode gesenkt werden, wenn der Suchvorgang eingrenzend so geregelt ist, dass er einen Bezug zu einem konkreten Suchanlass voraussetzt (BVerfG, a. a. O., Rz. 95). Indem in Satz 3 geregelt wird, dass die automatisierte Datenanalyse anhand von „Suchbegriffen“ zu erfolgen hat, die sich auf einen Anlass im Sinne des Absatzes 1 Satz 1 stützen müssen, wird eine sachliche Verbindung zwischen dem gefährdeten Rechtsgut und den von automatisierten Anwendungen betroffenen Personen vorausgesetzt. Indem der Suchvorgang in den Fällen des Absatzes 1 Nummer 2 und 3 zudem auf die nach den §§ 6 und 7 Verantwortlichen auszurichten ist (Satz 4), wird das Eingriffsgewicht weiter gemindert, weil mit dem Erfordernis einer tatsachengestützten Verbindung zu einer konkret verantwortlichen Person das Risiko sinkt, dass Personen in weitere polizeiliche Maßnahmen einbezogen werden, die dafür keinen zurechenbaren Anlass gegeben haben (BVerfG, a. a. O., Rz. 94). Hintergrund für die Beschränkung dieser zusätzlichen begrenzenden Vorgabe auf die Fälle des Absatzes 1 Nummer 2 und 3 ist, dass die Eingriffsschwellen niedriger gegenüber der des Absatzes 1 Nummer 1 sind, der eine konkrete Gefahr für besonders gewichtige Rechtsgüter verlangt. Zur Wahrung der Verhältnismäßigkeit wird die Eingriffsintensität der Maßnahmen nach den Nummern 2 und 3 daher eingeschränkt.

Durch die Formulierung der Anforderung „Ausrichten“ der Maßnahme auf die Verantwortlichen nach den §§ 6 und 7 (Satz 4) wird vorgegeben, dass sich der Suchvorgang nur auf die genannten Personengruppe beziehen darf. Erforderlich ist, dass eine tatsachengestützte Verbindung zu einer konkret verantwortlichen Person vorliegt. Ein solcher Bezug darf nicht erst durch die Maßnahme hergestellt werden, da ansonsten das Risiko steigt, dass Personen in weitere polizeiliche Maßnahmen einbezogen werden, die dafür keinen zurechenbaren Anlass gegeben haben (BVerfG, Urteil vom 26. Februar 2023, Rz. 94).

Durch den Regelungszusammenhang ist somit sichergestellt, dass nur Personen, die für die Begehung von Straftaten von erheblicher Bedeutung (§ 4 Nummer 4 SächsPVDG) oder

für die Begehung von schweren oder besonders schweren Straftaten verantwortlich sind, Anlass für eine Suche geben können.

Aus dem Zusammenspiel der Sätze 1 und 3 ergibt sich, dass der Mensch sowohl am Anfang als auch am Ende des Entscheidungsprozesses steht. Zudem sind die Verarbeitungsschritte während der Datenanalyse durch den Menschen vorher festzulegen (wenn-dann-Operatoren), sodass der gesamte Vorgang der Datenanalyse über den zusammengeführten Datenbestand von Menschen gelenkt und bestimmt ist.

Satz 5 enthält ein ausdrückliches Verbot der direkten Anbindung der Analyseplattform an Internetdienste und minimiert durch die Begrenzung der Daten, die einbezogen werden dürfen, das Eingriffsgewicht.

Absatz 3 bestimmt gemäß den Vorgaben des Bundesverfassungsgerichts abschließend, welche Daten auf der Analyseplattform zusammengeführt werden dürfen. Die Regelung begrenzt sowohl den Umfang als auch die Art der verarbeitbaren Daten, wodurch das Eingriffsgewicht der automatisierten Datenanalyse gemindert wird (BVerfG, a. a. O., Rz. 116).

Gemäß Satz 3 dürfen personenbezogene Vorgangsdaten Unbeteiligter nicht in die automatisierte Datenanalyse einbezogen werden. Nach Satz 4 dürfen Verkehrsdaten aus Gründen der Verhältnismäßigkeit (hohe Zahl von Unbeteiligten) bei Maßnahmen nach Absatz 1 Nummer 3 nicht auf die Analyseplattform gezogen werden (BVerfG, a. a. O., Rz. 118). Satz 7 schließt generell aus, dass Daten, die durch besonders gewichtige Grundrechtseingriffe (Wohnraumüberwachung) erlangt wurden, in die automatisierte Datenanalyse einbezogen werden dürfen.

Satz 1 bestimmt positiv, welche Daten in die automatisierte Datenanalyse einbezogen werden können und benennt ausdrücklich eigene Vorgangsdaten, Falldaten, Daten aus polizeilichen Auskunftssystemen und Fahndungsdaten, Verkehrsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch. Mit der ausdrücklichen Benennung der zum Zweck der automatisierten Datenanalyse nutzbaren Quelldaten wird die Datenmenge begrenzt (BVerfG, a. a. O., Rz. 78). Mit der Beschränkung auf eigene Daten wird klargestellt, dass nur Daten einbezogen werden können, die durch die Polizei zur Aufgabenerfüllung in den polizeilichen Datensystemen gespeichert sind.

Von besonderer praktischer Bedeutung sind die Daten aus der Vorgangsverwaltung gemäß § 79 Absatz 2 SächsPVDG. Ein Vorgang umfasst sämtliche Unterlagen, die im Zusammenhang mit einer polizeilichen Tätigkeit über eine bestimmte Person, Sache oder sonstigen Gegenstand polizeilichen Handelns geführt werden. Aufgenommen werden insbesondere Anzeigen, Ermittlungsberichte und Vermerke, die nicht nur Daten zu Verdächtigen, Beschuldigten oder sonstigen Anlasspersonen enthalten, sondern beispielsweise auch zu Personen, die Anzeige erstatten, Hinweise geben oder Zeuginnen oder Zeugen sind. Die Vorgangsdaten sind Vorgangssachbearbeitungsdaten. Falldaten in Fallbearbeitungssystemen dienen der Unterstützung von Ermittlungstätigkeiten und Auswertungen bei komplexen, fallübergreifenden Ermittlungen oder bei Strukturermittlungen. Ein Fallbearbeitungssystem geht über die reine Verwaltung von Vorgangsdaten hinaus, indem es der Anwenderin oder dem Anwender ein speziell auf die Aufhellung von Strukturen hin ausgerichtetes Werkzeug zur Verfügung stellt, das weniger personenbezogen als vielmehr ereignisbezogen ausgerichtet ist und vor allem Beziehungen zwischen Personen, Institutionen, Objekten und Sachen abbildet und sowohl zu präventiven als auch zu repressiven Zwecken eingesetzt werden kann. Fallbearbeitungssysteme enthalten überwiegend Daten von Personen aus strafrechtlichen Ermittlungsverfahren.

Polizeiliche Auskunftssysteme enthalten personenbezogene Informationen, die überwiegend aus strafrechtlichen Ermittlungsverfahren stammen und dort sowohl zum Zweck der vorbeugenden Straftatenbekämpfung als auch zum Zweck der Strafverfolgung und -vollstreckung gespeichert werden.

Mit dem Begriff der Verkehrsdaten werden gemäß der Legaldefinition in § 3 Nummer 70 TKG diejenigen Daten erfasst, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind. Hierzu gehören insbesondere auch die für die Polizeiarbeit praktisch bedeutsamen Standortdaten (vgl. § 9 Absatz 1 Nummer 1 TDDDG), die repressiv oder präventiv unter den jeweiligen gesetzlichen Anforderungen erhoben werden können. Die Kenntnis darüber, welches mobile Telekommunikationsendgerät zu einem bestimmten Zeitpunkt an einem bestimmten Ort angemeldet war, kann für die polizeiliche Ermittlungsarbeit von wesentlicher Bedeutung sein, weil der Aufenthaltsort der Anschlussinhaberin oder des Anschlussinhabers zum Beispiel Aufschlüsse über Organisationsstrukturen einer Mehrheit von Tatverdächtigen geben kann.

Daten aus Asservaten sind aus sichergestellten oder beschlagnahmten Datenträgern extrahierte vergleichsweise unstrukturierte Daten. Datenträger dieser Art können beispielsweise USB-Sticks, Festplatten, Smartphones oder Laptops sein.

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

Satz 2 regelt die ergänzende Einbeziehung von Daten aus gezielten Abfragen in gesondert geführten staatlichen Registern sowie von einzelnen gesondert gespeicherten Datensätzen aus Internetquellen. Daten aus staatlichen Registern sind beispielsweise Daten aus dem Melderegister, dem Zentralen Verkehrsinformationssystem (ZEVIS) oder dem Waffenregister, die über die Analyseplattform auf direktem Weg abgefragt werden können, soweit dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. Abfragen in ZEVIS können zur Aufklärung des Sachverhalts beispielsweise erforderlich sein, wenn die Mobilität einer Anlassperson in Frage steht. Hat diese Person eine waffenrechtliche Erlaubnis, kann darin ein gefahrerhöhendes Indiz gesehen werden. Die Funktionalität der Analyseplattform stellt sicher, dass solche Informationen schnell zusammengeführt werden können. Satz 2 erlaubt zudem eine ergänzende Einbeziehung von gesondert gespeicherten Datensätzen aus Internetquellen. Solche Daten müssen für jeden Analysevorgang händisch hinzugezogen werden. Es handelt sich bei diesen Datensätzen regelmäßig um die Ergebnisse polizeilicher Recherchen in für jedermann zugänglichen sozialen Netzwerken. Sie werden in einem gesonderten Format, meist als PDF, gespeichert und können auf die Analyseplattform aufgespielt werden. Voraussetzung ist, dass die Einbeziehung dieser Daten zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. In Betracht kommen etwa Fallkonstellationen, in denen auf sozialen Netzwerken Amoktaten angekündigt oder Verabredungen zu gemeinsamen Aktionen getroffen werden, die den Tatbestand des Landfriedensbruchs erfüllen würden.

Nach Satz 3 dürfen Daten von Unbeteiligten, die in Vorgangsdaten enthalten sind, nicht in die automatisierte Datenanalyse einbezogen werden. Die Regelung wirkt eingriffsminimierend. Der Veranlassungszusammenhang ist für das Eingriffsgewicht der automatisierten Datenanalyse von maßgeblicher Bedeutung, denn das Eingriffsgewicht erhöht sich, wenn durch die Datenanalyse Informationen über Personen erlangt werden, die objektiv in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den polizeilichen Eingriff durch ihr Verhalten nicht zurechenbar veranlasst haben (BVerfG, a. a. O., Rz. 77). Zentrales Element des Veranlassungszusammenhangs ist die tatsachengestützte Annahme, dass die betroffene Person künftig Straftaten begehen wird. Zum Schutz Unbeteiligter dürfen deren personenbezogene Vorgangsdaten grundsätzlich nicht in eine automatisierte Datenanalyse einbezogen werden.

Gemäß Satz 4 dürfen Verkehrsdaten nicht in die automatisierte Datenanalyse einbezogen werden, wenn die Maßnahme gemäß Absatz 1 Nummer 3 zur vorbeugenden Bekämpfung von Straftaten bereits im Vorfeld einer konkretisierten Gefahr zur Anwendung kommt. Da

bei der Verkehrsdatenerhebung insbesondere in Bezug auf die hier besonders relevanten Standortdaten häufig eine Vielzahl unbeteiligter Personen betroffen ist, führt der Ausschluss der Einbeziehung von Verkehrsdaten zu einer deutlichen Reduzierung der Eingriffsintensität. Dies dient sowohl dem Schutz Unbeteiligter als auch der Wahrung der Verhältnismäßigkeit. Im Vergleich zur konkretisierten Gefahr nach Absatz 1 Nummer 2 oder einer konkreten Gefahr nach Absatz 1 Nummer 1 zeichnet sich das Gefahrenvorfeld durch eine größere Ungewissheit sowohl in Bezug auf die Tatsachengrundlage als auch in Bezug auf den zum Schaden führenden Kausalverlauf aus. Dies erfordert eine entsprechende Begrenzung der Eingriffsintensität.

Nach Satz 5 sind die in der Analyseplattform gespeicherten Verkehrsdaten (insbesondere Funkzellendaten) nach Ablauf von zwei Jahren zu löschen, soweit die weitere Speicherung der Daten für die Fallbearbeitung nicht ausnahmsweise erforderlich ist. Diese Löschungspflicht trägt zur Reduzierung der Datenmenge bei und wirkt somit eingriffsmildernd. Soweit mit der Einbeziehung von Verkehrsdaten, insbesondere den aus Funkzellenabfragen gewonnenen Daten, in dem für die automatisierte Datenanalyse bereitstehenden Datenpool eine bevorratende Speicherung von Verkehrsdaten möglich ist, müssen – so das Bundesverfassungsgericht – die erfassbaren Daten substantiell begrenzt und eine Höchstspeicherungsdauer geregelt sein (BVerfG, a. a. O., Rz. 85). Die Frist steht allerdings unter dem Vorbehalt, dass die Daten nach Ablauf der Frist ausnahmsweise nicht zu löschen sind, wenn sie für die Fallbearbeitung erforderlich sind. Um den Anforderungen an Transparenz und aufsichtliche Kontrolle Rechnung zu tragen, ist die Entscheidung, die Daten nicht zu löschen, gemäß Satz 6 zu begründen.

Zur Verringerung der Eingriffsintensität der automatisierten Datenanalyse trägt schließlich bei, dass nach Satz 7 personenbezogene Daten, die aus besonders schwerwiegenden Grundrechtseingriffen stammen, nicht in die Analyse einbezogen werden dürfen.

Absatz 4

Satz 1 verpflichtet das Staatsministerium des Innern, das Verfahren der automatisierten Datenanalyse in einer Verwaltungsvorschrift zu regeln und stellt klar, dass diese der Anhörung durch die oder den Sächsischen Datenschutz- oder Transparenzbeauftragte(n) unterliegt und zu veröffentlichen ist.

In den Sätzen 1 bis 5 werden die erforderlichen Regelungsinhalte dieser Verwaltungsvorschrift näher konkretisiert. Das Bundesverfassungsgericht hat ausdrücklich darauf hingewiesen, dass der Gesetzgeber die Verwaltung verpflichten kann, die im Gesetz geregelten Vorgaben weiter zu konkretisieren, soweit die Vorgaben zu Art und Umfang der in die automatisierte Datenanalyse einbeziehbaren Daten und der zulässigen Verarbeitungsmethoden aus dem Gesetz selbst nur begrenzt erkennbar sind. Aus Gründen der Transparenz und der Kontrolle muss die Verwaltungsvorschrift veröffentlicht werden (BVerfG, a. a. O., Rz. 113).

Satz 1 Nummer 1 bezeichnet die Eckpunkte des in der Verwaltungsvorschrift zu regelnden Konzeptes. Ausgangspunkt hierfür ist der Veranlassungszusammenhang, der dafür entscheidend ist, ob und in welcher Weise personenbezogene Daten verwendet werden dürfen. Unter Veranlassungszusammenhang ist der sachliche Bezug der von der Analyse betroffenen Personen zum jeweiligen Phänomenbereich zu verstehen. Grundlegend ist hier die Unterscheidung zwischen einerseits unbeteiligten und andererseits verurteilten, beschuldigten und verdächtigen Personen sowie sonstigen Anlasspersonen und deren Kontaktpersonen (siehe § 28 SächsDSUG). In Satz 3 wird der Begriff des Veranlassungszusammenhangs gemäß den Vorgaben des Bundesverfassungsgerichts gesetzlich definiert (BVerfG, a. a. O., Rz. 94). Der Veranlassungszusammenhang ist für das Eingriffsgewicht der automatisierten Datenanalyse von maßgeblicher Bedeutung, denn das Eingriffsgewicht erhöht sich, wenn durch die Datenanalyse Informationen über Personen erlangt werden,

die objektiv in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den polizeilichen Eingriff durch ihr Verhalten nicht zurechenbar veranlasst haben. Für die Einbeziehung von Daten ist weiterhin das Gewicht des Grundrechtseingriffs bei der Datenerhebung zu berücksichtigen (BVerfG, a. a. O., Rz. 81). Wegen der besonderen Eingriffsintensität von Wohnraumüberwachungen ist in Absatz 3 Satz 7 bereits gesetzlich ausgeschlossen, dass die aus solchen Maßnahmen erlangten Informationen in die automatisierte Datenanalyse einbezogen werden. Bei Daten, die aus anderen grundrechtsintensiven Eingriffen erlangt wurden, kommt eine Weiterverarbeitung der Daten nach den Grundsätzen der Zweckbindung nur in Betracht, wenn die Voraussetzungen des § 79a Absatz 1 oder 2 SächsPVDG vorliegen.

Durch technisch-organisatorische Vorkehrungen, die in der Verwaltungsvorschrift näher auszuführen sind (Satz 1 Nummer 3), muss sichergestellt werden, dass die Grundsätze der Zweckbindung auch tatsächlich umgesetzt werden. Die weitere Nutzung von Daten im Rahmen der automatisierten Datenanalyse muss nach den Grundsätzen der Zweckbindung und Zweckänderung verfassungsrechtlich gerechtfertigt sein. Im Rahmen einer automatisierten Datenanalyse können personenbezogene Daten sowohl zweckwahrend als auch zweckändernd weiterverarbeitet werden. Eine zweckwahrende Nutzung von Daten aus eingriffsintensiven Überwachungsmaßnahmen kommt gem. § 79a Absatz 1 SächsPVDG nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich. Ist diese nur zum Schutz bestimmter Rechtsgüter oder zur Verhütung bestimmter Straftaten erlaubt, so begrenzt dies deren unmittelbare sowie weitere Verwendung auch in derselben Behörde, soweit keine gesetzliche Grundlage für eine Zweckänderung eine weitergehende Nutzung erlaubt. Nicht erforderlich für eine weitere Nutzung der Daten im Rahmen der Zweckbindung ist das Vorliegen der für die Datenerhebung maßgeblichen Gefahrenlage. Ausreichend für eine weitere Nutzung der Daten ist vielmehr ein bloßer Spurenansatz. Etwas anders gilt nur für Daten aus einer Wohnraumüberwachung, deren Weiterverarbeitung auf der Analyseplattform aber in Absatz 3 Satz 7 gesetzlich ausgeschlossen ist. Nach § 79a Absatz 2 SächsPVDG dürfen Daten unter den genannten Voraussetzungen zweckändernd verarbeitet werden. Die für die Datenerhebung maßgebliche Gefahrenlage ist – mit Ausnahme der Wohnraumüberwachung– keine Voraussetzung für eine zulässige Zweckänderung. Ausreichend ist vielmehr, dass sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergibt.

Ob Daten, die im Rahmen einer automatisierten Datenanalyse weiterverarbeitet werden, zweckwahrend oder zweckändernd verwendet werden, hängt maßgeblich von der Herkunft der Daten und den ursprünglichen Erhebungszwecken ab. Allein aus dem Umstand, dass die Daten in den eigenen Datenbeständen der Behörde gespeichert sind, kann nicht gefolgert werden, dass eine Nutzung der Daten im Rahmen einer automatisierten Datenanalyse zweckwahrend erfolgt. Sind die in den eigenen Datenbeständen der Behörde gespeicherten Daten ursprünglich von einer anderen Stelle erhoben und an sie weitergegeben worden, liegt schon wegen des damit verbundenen Behördenwechsels eine zweckändernde Datennutzung vor. Zur praktischen Umsetzung des verfassungsrechtlichen Zweckbindungsgrundsatzes ist insbesondere eine Kennzeichnung der Daten erforderlich (Satz 1 Nummer 3). Zwar sieht § 81 SächsPVDG Kennzeichnungspflichten vor. Wegen der in § 81 Absatz 4 Satz 1 SächsPVDG enthaltenen Ausnahmeregelung kann eine für die automatisierte Datenanalyse erforderliche Kennzeichnung aber über § 81 SächsPVDG nicht ausreichend sichergestellt werden. Darüber hinaus sorgt eine Kennzeichnung allein noch nicht dafür, dass die durch die Zweckbindungsregelungen für die einzelnen Daten geltenden Grenzen eingehalten werden. Besonders schwierig ist dies bei einer automatisierten Einbindung von Dateien, zumal wenn es sich um große Datenbestände handelt. Eine begrenzende Wirkung gesetzlicher Zweckbindungsregelungen wird sich hier – so das Bundesverfassungsgericht – nur mittels organisatorischer und technischer Vorkehrungen realisieren lassen, die näher zu regeln sind, um das Eingriffsgewicht in verfassungsrechtlich anzuerkennender Weise reduzieren zu können (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rz. 139). Technisch-organisatorische Sicherungen, die die Einhaltung der Zweckbindung sicherstellen, können

etwa in der technischen Trennung von Datenbeständen nach unterschiedlichen Verarbeitungszwecken oder einer zweckabhängigen Verteilung von Zugriffsrechten auf Datenbestände bestehen (BVerfG, a. a. O., Rz. 140). Auch Schulungsmaßnahmen hinsichtlich der rechtlichen Vorgaben zur Weiterverarbeitung der Daten können als organisatorische Sicherungsmaßnahme genannt werden. Satz 1 Nummer 3 sieht deshalb vor, dass technisch-organisatorische Sicherungen zur Einhaltung der Zweckbindung in einer Verwaltungsvorschrift zu regeln sind, die zu veröffentlichen ist. Die Regelungsanforderungen in Nummer 2 (Rechte- und Rollenkonzept) und Nummer 4 (Zugriffskontrollen) stellen sicher, dass die Zugriffsrechte an die Funktion anknüpfen und verdachtsunabhängige Stichproben erfolgen. Nummer 5 stellt sicher, dass Anforderungen an die Protokollierung, die Dauer der Aufbewahrung der Protokolldaten bestimmt werden und an die Dokumentation von Maßnahmen nach § 62a. Nummer 6 bestimmt, dass ferner zu regeln ist, welche konkreten Methoden und Techniken zur automatisierten Datenanalyse eingesetzt werden. Somit ist zu bestimmen, ob die automatisierte Datenanalyse mittels regelbasierter Systeme erfolgt oder durch KI-Systeme. Durch die Nummer 7 wird sichergestellt, dass verfahrensrechtliche Maßnahmen getroffen werden, die sicherstellen, dass Fehler der Datenauswertung in Folge in der automatisierten Datenanalyse erkannt werden und korrigiert werden. Diese Regelung setzt die Vorgaben des Bundesverfassungsgerichts um, dass soweit selbstlernende Systeme in der Polizeiarbeit zur Anwendung kommen, der ggf. bestehenden eingeschränkten Nachvollziehbarkeit von gewonnenen Erkenntnissen durch verfahrensrechtliche Vorkehrungen begegnet wird und damit Fehler in der Datenauswertung erkannt werden (BVerfG, a. a. O., Rz. 102)

Nach Satz 3 hat die Verwaltungsvorschrift ein Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten zu beinhalten. Übergeordnetes Ziel dieses Konzeptes ist es, die Datenbestände unter Berücksichtigung der in Absatz 1 beschriebenen Eingriffsschwellen auf das für den Analysezweck erforderliche Maß zu begrenzen und die Einbeziehung der Daten Unbeteiligter möglichst zu vermeiden. Das Bundesverfassungsgericht hat mehrfach betont, dass eine Begrenzung von Art und Umfang der Daten und die zugelassene Methode der Datenanalyse maßgeblichen Einfluss auf das Eingriffsgewicht und damit auf deren Zulässigkeit jeweils in Bezug auf die normierte Eingriffsschwelle haben (BVerfG, a. a. O., Rz. 76 ff. und 90 ff.). Da die zugelassene Methode der Datenanalyse bereits durch gesetzliche Vorgaben zu den Suchkriterien und zum Ausschluss maschineller Sachverhaltsbewertungen hinreichend begrenzt ist, dienen die mit der Verwaltungsvorschrift zu erlassenden Konkretisierungen in erster Linie dazu, die in die Datenanalyse einzubeziehenden Datenbestände auf das für den Analysezweck erforderliche Maß zu begrenzen, die Umsetzung des Grundsatzes der Zweckbindung auch praktisch sicherzustellen und Unbeteiligte so weit wie möglich zu schützen.

Die Sätze 4 und 5 geben vor, dass durch das Rollen- und Rechtekonzept (gemäß Satz 1 Nummer 2) die Verteilung sachlich eingeschränkter Zugriffsrechte anhand von Phänomenbereichen zu regeln ist. Das Rollen- und Rechtekonzept hat somit festzulegen, wer innerhalb der Polizeiorganisation Zugriff auf welche Daten haben kann und mit welchen Rechten und Pflichten der Zugriff verbunden ist. Dabei sind die Zugriffsrechte nach dem Prinzip auszugestalten, dass die Zahl der Zugriffsberechtigten umso geringer ist, desto umfangreicher und sensibler die von der Zugriffsberechtigung umfassten Daten sind. Weil das Rollen- und Rechtekonzept an Rollen und nicht an Personen anknüpft, ist es möglich, dass eine Person mehrere Rollen hat und deshalb über erweiterte Zugriffsrechte verfügt. Beispielsweise könnten Personen mit höherer oder herausgehobener Verantwortung mehrere Rollen übertragen werden, damit sie ihrer Aufsichts- und Kontrollfunktion innerhalb der jeweiligen Polizeidienststelle gerecht werden können. Das Rollen- und Rechtekonzept ist mit seiner Bindung an Phänomenbereiche so anzulegen, dass grundsätzlich niemand alle auf der Analyseplattform zusammengeführten Datenbestände einsehen kann. Je nachdem welche Phänomenbereiche einer zugriffsberechtigten Person zwecks Bearbeitung zugewiesen sind, soll sie nur auf den diesen Phänomenbereich betreffenden Ausschnitt der Datenbestände Zugriff nehmen können. Das Rollen- und Rechtekonzept soll damit zu einer Reduzierung

des Umfangs der jeweils verarbeitbaren Daten und damit zu einer Verringerung der Eingriffsintensität führen. Abstrakter Maßstab für die Ausgestaltung des Rollen- und Rechtekonzepts sind die drei Tatbestandvarianten in Absatz 1 Satz 1. Konkret muss das Konzept an kriminologische Phänomenbereiche anknüpfen, denen innerhalb einer Behörde die verschiedenen Sachbearbeiter zugeordnet sind. Das Rollen- und Rechtekonzept bedarf einer laufenden Überprüfung, um die Erfordernisse der Praxis und die verfassungsrechtlichen Vorgaben in einen optimalen Ausgleich zu bringen. Dies kann zum Beispiel bedeuten, dass nur wenige und besonders geschulte Berechtigte Zugriff auf Verkehrsdaten und Daten aus Asservaten haben, weil es sich dabei um große Datenmengen handelt, die viele personenbezogene Daten Unbeteiligter beinhalten und deshalb mit besonderer Sensibilität zu behandeln sind. Ein zentraler Wirkungsfaktor des Rollen- und Rechtekonzepts ist, dass die Zugriffsrechte nur entsprechend qualifizierten Personen zu erteilen sind, was eine Schulung und deren erfolgreichen Abschluss voraussetzt. Der Prozess der Rechtevergabe ist klar zu definieren, zu dokumentieren und technisch abzusichern. Bestandteil des Rollen- und Rechtekonzepts ist auch die in Absatz 5 geregelte Zugriffskontrolle, die einem Missbrauch der Analyseplattform entgegenwirkt.

Absatz 5

Satz 1 enthält Vorgaben zur Transparenz und Kontrolle (vgl. BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rz. 109). Ein zentrales Element des Rollen- und Rechtekonzepts ist die Zugriffskontrolle, die durch die Protokollierung der einzelnen Arbeitsschritte abgesichert wird (Satz 2). Auf diese Weise wird sichergestellt, dass nur berechtigte Personen eine automatisierte Datenanalyse vornehmen können. Der aufsichtlichen Kontrolle und der Gewährleistung effektiven Rechtsschutzes gemäß Artikel 19 Absatz 4 GG dient die in Satz 3 vorgeschriebene Begründungspflicht. Gleichzeitig dient sie der Selbstvergewisserung über die Rechtmäßigkeit der automatisierten Datenanalyse, denn das Erfordernis einer schriftlichen Begründung bietet eine größere Richtigkeitsgewähr.

Absatz 6

Absatz 6 ordnet für die Einrichtung, wesentliche Änderung und Anwendung einer automatisierten Datenanalyse einen Behördenleitervorbehalt an. Damit werden nicht nur die grundsätzliche Einrichtung oder wesentliche Änderung der Analyseplattform, sondern auch deren Anwendung in jedem Einzelfall unter Behördenleitervorbehalt gestellt. Dies erscheint mit Blick auf das Eingriffsgewicht einer Datenanalyse und dem Umstand, dass die einzubeziehenden Datenquellen in jedem Einzelfall entsprechend des Analysezwecks skalierbar sind, sachgerecht. Nach Satz 2 ist die oder der Sächsische Datenschutz- und Transparenzbeauftragte in diesen Fällen zuvor anzuhören. Bei Gefahr im Verzug ist die Anhörung nachzuholen. Durch die Verweisung auf § 94 SächsPVDG wird klargestellt, dass die Kontrollpflicht der oder des Sächsischen Datenschutz- und Transparenzbeauftragten unberührt bleibt.

§ 62b

Mit der neuen Vorschrift des § 62b wird eine Rechtsgrundlage für den Abgleich von zur polizeilichen Aufgabenerfüllung gespeicherten biometrischen Daten von Gesichtern und Stimmen mit öffentlich zugänglichen biometrischen Daten aus dem Internet zum Zweck der Identifizierung oder Lokalisierung von Störern eingeführt. Durch eine solche Befugnis können beispielsweise relevante Hinweise zu einer Zielperson, die auf sozialen Netzwerken einen Amoklauf angekündigt hat, gewonnen werden oder der Aufenthaltsort einer Person, von der eine Gefahr für ein überragend wichtiges Rechtsgut ausgeht, zum Zweck der Abwehr dieser Gefahr ermittelt werden.

Die Befugnis zum Abgleich von gespeicherten biometrischen Daten mit öffentlich zugänglichen biometrischen Daten stellt einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG dar.

Durch eine solche Maßnahme erfolgt die Erhebung und Verarbeitung von biometrischen Daten zu einem nicht weiter abgrenzbaren Personenkreis. Gewichtserhöhend wirkt zudem, dass der Abgleich von den betroffenen Personen nicht bemerkt wird, er aus ihrer Sicht also heimlich erfolgt. Bei der Ermittlungsbefugnis handelt es sich um eine Maßnahme, die von der Eingriffsintensität heimlichen eingriffsintensiven Überwachungsmaßnahmen gleichkommt. Damit dieser Eingriff in das Grundrecht auf informationelle Selbstbestimmung den Grundsätzen der Verhältnismäßigkeit genügt, gelten als Maßstab für die verfassungsgemäße Ausgestaltung einer gesetzlichen Regelung die Anforderungen des Bundesverfassungsgerichts für die Ausgestaltung von heimlichen Überwachungsmaßnahmen (siehe BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 und 1 BvR 1140/09, Rz. 103 ff, 117ff).

Die Maßnahmen müssen auf den Schutz oder die Bewehrung hinreichend gewichtiger Rechtsgüter begrenzt sein (BVerfG, a. a. O., Rz. 106). Im Bereich der Gefahrenabwehr setze dies das Vorliegen einer konkreten Gefahr für ein überragend wichtiges Rechtsgut voraus. Überragend wichtig seien Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt (BVerfG, a. a. O., Rz. 108). Dabei könne die Maßnahme schon gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, das die Gefahr in näherer Zukunft eintritt, sofern Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für überragend wichtige Rechtsgüter hinweisen (BVerfG, a. a. O. Rz. 112ff.).

Neben den verfassungsrechtlichen Anforderungen an die Ausgestaltung der Eingriffsschwelle bei intensiven Grundrechtseingriffen hat das Bundesverfassungsgericht weitere Anforderungen aus dem Verhältnismäßigkeitsgrundsatz abgeleitet: Regelungen zur vorherigen Kontrolle, zum Schutz des Kernbereichs, zur Transparenz, zum individuellen Rechtsschutz und zur aufsichtlichen Kontrolle (BVerfG Urteil vom 20. April 2016, Rz. 117ff, 134, 138, 140). Zu diesem Zweck erfolgen Regelungen zum Richtervorbehalt, zu den Anforderungen an die polizeiliche Anordnung (siehe Absatz 2), zum Schutz des Kernbereichs privater Lebensgestaltung (§ 76), zur unverzüglichen Datenlöschung (§ 78), zur Benachrichtigung (§ 74), zur Protokollierung (§ 75), zu den Berichtspflichten (siehe § 107) und zur aufsichtlichen Kontrolle (siehe Absatz 5, § 94, § 2 SächsKontrollG).

Voraussetzung für den Schutz des Kernbereichs privater Lebensgestaltung ist ein Geheimhaltungswillen des Betroffenen. Der vorgesehene Abgleich ist auf öffentlich zugängliche Daten aus dem Internet beschränkt. Diese Daten werden häufig schon deshalb keinen Kernbereichsbezug aufweisen, weil sie von der betroffenen Person selbst öffentlich gemacht wurden, so dass es an dem Geheimhaltungswillen fehlt. Lediglich in Fällen, wenn etwa Bild- oder Tonaufnahmen aus dem Internet in den Abgleich einbezogen werden, die den höchstpersönlichen Lebensbereich einer Person betreffen und ohne den Willen des Betroffenen in das Internet eingestellt wurden, hat die Erhebung von biometrischen Daten Kernbereichsrelevanz. Solange keine Zweifel bestehen, dass die biometrischen Daten ohne oder gegen den Willen des Betroffenen in das Internet hochgeladen wurden, ist der Kernbereichsschutz beim Abgleich nicht tangiert. Nach Hinweisen auf ein widerrechtliches Hochladen von Bildern, Videos oder Sprachdateien muss die Polizei aktiv suchen; diese können sich bspw. direkt aus dem Inhalt von Videos ergeben oder anhand einschlägig bekannter Internetseiten, auf denen solche Daten gefunden wurden. Bestehen dennoch Zweifel, findet § 76 Absatz 3 und 4 Anwendung.

Absatz 1

Absatz 1 Satz 1 regelt in den Nummern 1 bis 2 zwei unterschiedliche Eingriffsschwellen, die einen Anlass für einen automatisierten biometrischen Datenabgleich bilden können.

Satz 1

Die Eingriffsschwelle in Satz 1 Nummer 1 ist an enge Voraussetzungen geknüpft, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten. Vorausgesetzt wird eine konkrete Gefahr für ein besonders gewichtiges Rechtsgut.

Die Eingriffsschwelle in Satz 2 Nummer 1 setzt das Vorliegen einer konkretisierten Gefahr durch die Verhütung von schweren Straftaten voraus (BVerfG, a. a. O., Rz. 112)

Die Eingriffsschwelle in Satz 2 Nummer 2 regelt das Gefahrenvorfeld und bleibt noch hinter einer konkretisierten Gefahr zurück (BVerfG, a. a. O., Rz. 112) .

Ein Abgleich von gespeicherten biometrischen Daten oder mit biometrischen Daten des polizeilichen Fahndungsbestands, auf den die Polizei Zugriff hat, darf nur erfolgen, soweit eine solche Datenverarbeitung im Rahmen des Grundsatzes der Zweckbindung zulässig ist oder soweit eine Befugnis zum Datenabruf besteht. Die Vorschrift dient der Klarstellung des Grundsatzes der Zweckbindung.

Satz 3 beinhaltet in Umsetzung von Artikel 5 Absatz 1 UA 1 lit h KI-VO das Verbot eines Echtzeit-Abgleichs.

Satz 4 setzt die Rechtsprechung des Sächsischen Verfassungsgerichtshofs zu den Anforderungen an die Gestaltung einer Eingriffsschwelle im Gefahrenvorfeld um (siehe auch § 4 Nummer 5).

Absatz 2

Satz 1 verpflichtet die Polizei zur Verifizierungsprüfung. Satz 2 regelt, dass weitere Maßnahmen erst nach Verifizierung der Übereinstimmung der Daten erfolgen dürfen. Satz 3, regelt, dass soweit keine Datenübereinstimmung besteht, die Daten zu löschen sind und Satz 4 schließt eine Protokollierung der Datenverarbeitung im Fall von Satz 3 aus.

Absatz 3

Die Regelung stellt aufgrund des Eingriffsgewichts die Maßnahme unter Richtervorbehalt (Satz 1). Satz 2 regelt Form und Inhalt des Antrags der Polizei.

Absatz 4

Absatz 4 Satz 1 enthält die Pflicht, die oder den Sächsischen Datenschutz- und Transparenzbeauftragten als unabhängige Stelle über die Maßnahme nach deren Abschluss unverzüglich zu unterrichten. Die Regelung dient im Hinblick auf die Eingriffsintensität der Maßnahme der Gewährleistung von Transparenz und aufsichtlicher Kontrolle. Durch die Verweisung auf § 94 SächsPVDG wird sichergestellt, dass die zweijährige Pflicht zur Datenschutzkontrolle unberührt bleibt.

Absatz 5

Absatz 5 verpflichtet das Sächsische Staatsministerium des Innern durch Verwaltungsvorschrift unter Berücksichtigung der gesetzlichen Maßgaben der Nummern 1 bis 3 das Nähere zum Verfahren zu regeln. Die Verwaltungsvorschrift ist zu veröffentlichen.

Zu Nummer 17

§ 63

Mit der Ergänzung der Regelung in Absatz 2 Satz 2 erfolgt die Umsetzung der Vorgaben des Urteils des Sächsischen Verfassungsgerichtshofs zur Gestaltung der Eingriffsschwelle im Hinblick auf die Regelung des § 63 (Siehe auch Begründung zu § 4 Nummer 6).

Zu Nummer 18

§ 64

Die Neufassung von Absatz 4 dient der Umsetzung der Entscheidung des Bundesverfassungsgerichts vom 9. Dezember 2022 (1BvR 1345/21). In dieser Entscheidung hat das Bundesverfassungsgericht Vorgaben für die Gestaltung der Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung beim Einsatz von Verdeckten Ermittlern und Vertrauenspersonen bestimmt, die durch den Gesetzgeber umzusetzen sind. Diese betreffen Maßnahmen auf der Ebene der Datenerhebung und auf der Auswertungs- und Verwertungsebene. Das Bundesverfassungsgericht hat festgelegt, dass bereits auf der Ebene der Datenerhebung gesetzgeberisch auszuschließen sei, dass Kernbereichsinformationen erfasst werden. Auszuschließen sei, dass zu der Zielperson eine intime Beziehung und damit eine kernbereichsrelevante Beziehung aufgebaut werde (BVerfG, a. a. O., Rz. 109f). Soweit eine Überwachung in den Kernbereich privater Lebensgestaltung eindringe, müsse nicht zwangsläufig der gesamte Einsatz enden, sondern es könne je nach konkreten Umständen des Einzelfalls zur Vermeidung des Eindringens in den Kernbereich auch genügen, dass lediglich die kernbereichsrelevante Kommunikation oder Interaktion abgebrochen werde. Da bei dem Einsatz von Verdeckten Ermittlern oder Vertrauenspersonen bei einem unvermittelten Abbruch bzw. Unterbrechen der Datenerhebung wegen des Eindringens in den Kernbereich die Zielperson Verdacht schöpfen könne, könnte dies zu einer Enttarnung oder/und zugleich zu einer erheblichen Gefahr für Leib oder Leben der eingesetzten Verdeckten Ermittler oder Vertrauenspersonen führen. Eine solche Sachlage könne eine Ausnahme vom Unterbrechungsgebot verfassungsrechtlich rechtfertigen (BVerfG, a. a. O., Rz. 119ff). Vor dem Hintergrund von Ausnahmen vom Unterbrechungsgebot müsse jedoch wiederum auf der Auswertungs- und Verwertungsebene durch Schutzvorkehrungen sichergestellt werden, dass im Fall einer unterbliebenen Unterbrechung ggf. die Kernbereichsrelevanz vor der Weitergabe der Informationen durch die eingesetzten Verdeckten Ermittler oder Vertrauenspersonen überprüft wird. In Zweifelsfällen muss sichergestellt werden, dass die Kernbereichsrelevanz durch eine neutrale Stelle überprüft werde. Die fehlende Unterbrechung sei zudem zu dokumentieren.

Satz 1 setzt die Vorgaben des Bundesverfassungsgerichts auf der Ebene der Datenerhebung um, indem bei Kernbereichs-verletzungsgeneigten Maßnahmen durch eine vorgelagerte Prüfung sicherzustellen ist, dass relevante Gespräche und Situationen ausgeschlossen werden. Mit dem geänderten Satz 2 wird die Rechtsprechung des Bundesverfassungsgerichts umgesetzt, dass eine Ausnahme von der Unterbrechung der Datenerhebung erfolgen kann, wenn Leib oder Leben der Verdeckten Ermittler oder der Vertrauensperson konkret gefährdet sind oder deren künftige Verwendung als Verdeckte Ermittler oder Vertrauensperson. Satz 3 bestimmt, dass das Eindringen in den Kernbereich und die Umstände des Fortsetzens der Maßnahme zu dokumentieren sind. Satz 4 beinhaltet die spezifische Pflicht der Verdeckten Ermittler und Vertrauenspersonen, gewonnene Informationen hinsichtlich ihrer Kernbereichsrelevanz zu überprüfen. Satz 5 beinhaltet die Verpflichtung, bei Zweifeln über die Kernbereichsrelevanz gewonnener Informationen eine Entscheidung der oder des behördlichen Datenschutzbeauftragten einzuholen. Satz 6 stellt mit der Verweisung auf § 76 Absatz 5 klar, dass kernbereichsrelevante Erkenntnisse einem Verwertungsverbot unterfallen, unverzüglich zu löschen sind und nicht der archivrechtlichen Anbietungspflicht unterliegen. Satz 7 stellt sicher, dass die Maßgaben des § 76 Absatz 5 auch dann Anwendung finden, wenn Erkenntnisse gewonnen wurden, bei denen kein Zweifel an der Kernbereichsrelevanz bestehen.

Zu Nummer 19

§ 66

Zielsetzung der Änderungen des § 66 ist die Umsetzung des Urteils des Sächsischen Verfassungsgerichtshofs und die Aufnahme einer Rechtsgrundlage für die sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) mit Evaluierungsklausel.

Absatz 1

Mit Satz 3 erfolgt die Umsetzung der Vorgaben des Sächsischen Verfassungsgerichtshofs an die gesetzgeberische Ausgestaltung der Eingriffsschwellen (siehe Begründung zu § 4 Nummer 6). Die Sätze 4 und 5 beinhalten die bisherigen Regelungen von § 66 Absatz 1 Satz 3 und 4.

Absatz 2

In Absatz 2 wird in Erfüllung des Regelungsauftrags des Koalitionsvertrages 2024 bis 2029 zwischen CDU und SPD (Ziffer 1410) die Befugnis zur Quellen-Telekommunikationsüberwachung aufgenommen, unter den bestehenden hohen Eingriffsschwellen der konventionellen Telekommunikationsüberwachung und begleitenden Regelungen zum Richtervorbehalt, Kernbereichsschutz, unverzüglicher Datenlöschung, Benachrichtigung, Protokollierung und Berichtspflichten. Das Bundesverfassungsgericht hat im Urteil vom 20. April 2016, 1 BvR 966/09, die Quellen-TKÜ als grundsätzlich verfassungsrechtlich zulässig bewertet (siehe Urteil a. a. O., Rz. 234). Vergleichbare Regelungen finden sich in einer Vielzahl von Polizeigesetzen, siehe u.a. § 15b HSOG, § 31 Absatz 3 RhPf POG, § 20c PolG NRW und § 34a Absatz 2 S. 2 ThürPAG. Als besondere Form der Telekommunikationsüberwachung ist die Quellen-TKÜ an Artikel 10 Absatz 1 Grundgesetz (Artikel 27 Absatz 2 Sächsische Verfassung) zu messen. Sie erfasst Kommunikation, bevor diese verschlüsselt wird bzw. entschlüsselt diese. Hierbei wird nur die Kommunikation erlangt, die auch durch eine konventionelle TKÜ erlangt würde. Viele Kommunikationsprogramme (Internettelefonie, WhatsApp, Telegramm) nutzen standardmäßig eine Verschlüsselung ihrer Kommunikationsdaten (Inhalte von Gesprächen und Chats), ohne dass sich die Nutzer aktiv dafür entscheiden müssen oder etwas dazu beitragen müssen. Diese Inhalte könnten in vielen Fällen durch die konventionelle Form der Telekommunikationsüberwachung nicht mehr ausgewertet werden. Dies lässt die notwendigen und gesetzlich zulässigen Maßnahmen der konventionellen TKÜ bei der Abwehr von Gefahren für hochwertige Rechtsgüter ins Leere laufen. Aufgrund der hohen technischen Anforderungen an eine Quellen-TKÜ ist jeder Einsatz entsprechender Trojanersoftware oder die Ausnutzung von Sicherheitslücken in der Hard- oder Software maßgeschneidert. Gleichwohl ist sie ein unverzichtbares Instrument einer erfolgreichen Gefahrenaufklärung im Bereich von terroristischen Gefährdern oder Organisierter Kriminalität.

Sichergestellt sein muss bei Quellen-TKÜ, dass nur laufende Telekommunikation überwacht und aufgezeichnet wird (BVerfG, a. a. O., Rz. 234), da anderenfalls ein Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vorläge. Dieser Anforderung wird durch die Regelung in Nummer 1 Rechnung getragen. Die Regelung in Nummer 2 dient der Wahrung des Grundsatzes der Verhältnismäßigkeit.

Absatz 2a

In Absatz 2a Satz 1 werden die Voraussetzungen bestimmt, unter denen eine Quellen-TKÜ erfolgen kann.

Nummer 1 setzt für die Quellen-TKÜ das Vorliegen einer gegenwärtigen Gefahr (siehe Begriffsbestimmung in § 4 Nummer 3b) für die in der Regelung explizit benannten Rechtsgüter voraus. Der Sachwertgüterschutz wird beschränkt auf die Gefährdung von Gütern der Allgemeinheit, deren Bedrohung die Existenz der Menschen berührt. Dies können wesentliche Infrastruktureinrichtungen sein (z. B. Kraftwerke, Wasserwerke) oder Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen (Hochspannungsmasten). Im Unterschied zum

Sachwertgüterschutz nach Absatz 1 unterfallen Kulturgüter, deren Erhaltung im öffentlichen Interesse geboten ist, nicht dem Sachwertschutz nach Absatz 2a.

Nummer 2 erlaubt die Quellen-TKÜ, soweit die konkretisierte Gefahr einer Straftat nach § 100a Absatz 2 Strafprozessordnung, die sich gegen die in Nummer 1 genannten Rechtsgüter richten muss, vorliegt.

Nummer 3 erlaubt die Quellen-TKÜ, soweit die konkretisierte Gefahr einer terroristischen Straftat vorliegt.

Die Regelung in den Nummern 4 und 5 erfolgt analog zu der in Absatz 1 Nummern 4 und 5.

Satz 2 setzt wie Absatz 1 Satz 3 die Rechtsprechung des Sächsischen Verfassungsgerichtshofs um.

Satz 3 und 4 beinhalten die analogen Regelungen zu den Anforderungen an den Verhältnismäßigkeitsgrundsatz in Absatz 1 Satz 4 und 5.

Absatz 3

Absatz 3 enthält Bestimmungen zu technischen Vorkehrungen zum Schutz des informationstechnischen Systems der Zielperson. Demnach muss der Eingriff in das fremde System auf das unbedingt erforderliche Mindestmaß begrenzt werden. Infolgedessen ist sicherzustellen, dass nur Veränderungen vorgenommen werden, die für die Erhebung der Daten unerlässlich sind (Nummer 1). Ferner sind im Zuge der Maßnahme vorgenommene Veränderungen bei deren Beendigung – soweit technisch möglich – automatisiert rückgängig zu machen (Nummer 2). Weiter trifft den Staat eine Schutzpflicht dahingehend, eine unbefugte Nutzung des eingesetzten Mittels durch Dritte zu verhindern (Satz 2).

Absatz 4

Absatz 4 beinhaltet in Satz 1 die Anordnungsbefugnis. Satz 2 bestimmt Form und Inhalt des Antrags.

Absatz 5

In Absatz 5 wurde der Regelungsinhalt von § 72 Absatz 1 überführt und an geändertes Bundesrecht angepasst.

Absatz 6

Enthält die Verpflichtung zur Evaluierung analog der bisherigen Regelungen im Hinblick auf den Evaluationszeitraum und die Kriterien.

§ 66a

Aus rechtssystematischen Gründen wurde der Regelungsinhalt des bisherigen § 69 in § 66a neu überführt.

Absatz 1

Mit der Bezugnahme von § 66 Absatz 1 in Satz 1 erfolgt die Umsetzung der Vorgaben des Sächsischen Verfassungsgerichtshofs im Hinblick auf die erforderliche Einschränkung der Eingriffsschwellen.

Absatz 2 bis 5

Die Absätze 2 bis 5 beinhalten die Regelungen des bisherigen § 69. Der Regelungsinhalt von § 69 Absatz 2 wurde vor dem Hintergrund der Zusammenführung mit dem Regelungsinhalt von § 72 Absatz 3 nicht übernommen.

Absatz 6

In Absatz 6 wurde aus rechtssystematischen Gründen die Regelung des bisherigen § 72 Absatz 3 überführt.

§ 67

Mit der Neufassung des Absatzes 1 werden die bisherigen Befugnisregelungen zur Erhebung von Verkehrsdaten (bisher Absatz 1) und Nutzungsdaten (bisher Absatz 2) in Absatz 1 in den Sätzen 1 und 2 zusammengeführt. Mit der Bezugnahme von § 66 Absatz 1 erfolgt die Umsetzung der Vorgaben des Sächsischen Verfassungsgerichtshofs im Hinblick auf die erforderliche Einschränkung der Eingriffsschwellen. Ferner werden Änderungen in Bundesgesetzen berücksichtigt. Satz 2 beinhaltet die Regelung des bisherigen § 67 Absatz 1 Satz 2 und Absatz 2 Satz 2. Satz 3 beinhaltet die Regelung des bisherigen § 67 Absatz 3.

Absatz 2 beinhaltet die Regelungen des bisherigen Absatzes 4. Mit der Änderung erfolgt die Korrektur eines redaktionellen Versehens.

Absatz 3 beinhaltet die Regelungen des bisherigen § 72 Absatz 2 Nummer 1 und 2 mit redaktionellen Anpassungen und Anpassungen an Änderungen in Bundesgesetzen.

§ 68

Mit der Neufassung von § 68 werden die Regelungsinhalte von § 68 und § 71 aus rechtssystematischen Gründen zusammengeführt.

Absatz 1

Mit der Bezugnahme von § 66 Absatz 1 erfolgt die Umsetzung der Vorgaben des Sächsischen Verfassungsgerichtshofs im Hinblick auf die erforderliche Einschränkung der Eingriffsschwellen.

Absatz 2

In Absatz 2 wurde die Regelung des bisherigen § 71 Absatz 1 überführt und die Eingrifsschwellen dahingehend modifiziert, dass die bisherige Anforderung, dass die Ermittlung des Aufenthaltsortes auf andere Weise „aussichtslos oder wesentlich erschwert wäre“ auf „weniger Erfolg versprechend oder erschwert wäre“, herabgesetzt wurde.

Absatz 3

In Satz 1 wurde die Regelung des bisherigen § 68 Absatz 2 Satz 1 und des § 71 Absatz 3 Satz 1 überführt. Satz 2 und 3 beinhalten jeweils die Regelung des bisherigen § 68 Absatz 2 Satz 2 und des bisherigen § 71 Absatz 3 Satz 2 zur Zweckbindung. Satz 4 überführt die Regelungen aus § 68 Absatz 2 Satz 3 und § 71 Absatz 3 Satz 3.

Absatz 4

Satz 1 beinhaltet die Regelung des bisherigen Absatzes 3 mit einer redaktionellen Anpassung. Satz 2 beinhaltet die Regelung des bisherigen § 71 Absatz 4. In Satz 4 erfolgte eine sprachliche Klarstellung.

Zu Nummer 20

§ 69 (gestrichen)

Der bisherige Regelungsinhalt wurde in § 66a überführt.

Zu Nummer 21

§ 70

Zielsetzung der Änderungen ist die Umsetzung des Beschlusses des Bundesverfassungsgerichts vom 27. Mai 2020 (1 BvR 1873/13, - 1 BvR 2618/13 – „Bestandsdatenauskunft II“). Das Bundesverfassungsgericht hatte mit diesem Beschluss § 113 des Telekommunikationsgesetzes und mehrere Fachgesetze des Bundes, die die manuelle Bestandsdatenauskunft regeln, für verfassungswidrig erklärt. Die Erteilung von solchen Auskünften sei grundsätzlich verfassungsrechtlich zulässig, jedoch müssten Übermittlungs- und Abrufregelungen durch hinreichend begrenzte Eingriffsschwellen die Verwendungszwecke beschränken. Das Gericht hat seine Anforderungen an die Ausgestaltung des „Doppeltürmodells“ weiter konkretisiert. Für allgemeine Bestandsdaten sei das Vorliegen einer konkreten Gefahr im Einzelfall ausreichend (BVerfG a. a. O, Rz. 146). Soweit eine Zuordnung von Bestandsdaten über Internetprotokolladressen erfolge, müsse dem erhöhten Eingriffsgewicht durch den Schutz von Rechtsgütern von zumindest hervorgehobenen Gewicht Rechnung getragen werden (BVerfG, a. a. O, Rz. 177). Über Zugangsdaten dürfe nur dann Auskunft erteilt werden, wenn die gesetzlichen Voraussetzungen für ihre Nutzung vorliegen (BVerfG, a. a. O, Rz. 235). Ferner bedurfte es der Anpassung an bundesgesetzliche Änderungen. Die jeweiligen Anforderungen müssten bereits in den Übermittlungsregelungen („1. Tür“) vollständig bestimmt sein und könnten nicht erst in den fachgesetzlichen Abrufregelungen („2. Tür“) geregelt werden (BVerfG, a. a. O, Rz. 134).

Absatz 1

Satz 1 beinhaltet wie bisher die Eingriffsschwelle für die einfache Bestandsdatenauskunft. Die Regelung setzt die Vorgaben des Bundesverfassungsgerichts um, da Voraussetzung für den Abruf von (einfachen) Bestandsdaten das Vorliegen einer konkreten Gefahr für die öffentliche Sicherheit im Einzelfall ist. Bei den Anpassungen handelt es sich um redaktionelle Anpassungen im Hinblick auf Änderungen in den Bundesgesetzen. Die bisherigen Regelungsinhalte der §§ 95, 111 Telekommunikationsgesetz finden sich jetzt in §§ 3 Nummer 6, 174 Telekommunikationsgesetz, die bisherigen Regelungsinhalte des § 14 Telemediengesetzes in § 2 Absatz 2 Nummer 2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz.

Satz 2 beinhaltet wie bisher die Eingriffsschwelle für Auskünfte über Zugangsdaten nach dem Telekommunikationsgesetz (Nummer 1) und nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (Nummer 2). Das Bundesverfassungsgericht hat hier wiederholend festgestellt, dass im Anwendungsbereich des Telekommunikationsgesetzes diese Auskünfte nur erteilt werden dürfen, wenn die gesetzlichen Voraussetzungen für die Nutzung vorliegen. Dem trägt die bestehende Regelung bereits Rechnung. Bei der Anpassung handelt es sich um eine redaktionelle Anpassung im Hinblick auf Änderungen im Telekommunikationsgesetz. Satz 2 Nummer 2 enthält die Befugnis für die Erlangung von Zugangsdaten im Hinblick auf digitale Dienste. Mit der Benennung der Rechtsgüter Leib, Leben oder Freiheit der Person, sexuelle Selbstbestimmung, Bestand des Bundes oder eines Landes, freiheitlich demokratische Grundordnung oder Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, wird die Übereinstimmung mit der bundesrechtlichen Eingriffsschwelle der Übermittlungsvorschrift im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (§ 23 Absatz 2 Nummer 2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz) gewährleistet.

Absatz 2

Die Regelung beinhaltet wie bisher die Eingriffsschwelle, wenn Ausgangspunkt der polizeilichen Anfrage auf Auskunft über einfache Bestandsdaten eine Internet-Protokoll-Adresse ist. Die bisherige Regelung genügte nicht den Anforderungen des Bundesverfassungsgerichts. Um den Anforderungen zu genügen, wurde die Auskunft dahingehend eingegrenzt, dass diese dem Schutz von Rechtsgütern von hervorgehobenem Gewicht dienen muss. Dementsprechend werden in der Regelung die Rechtsgüter Bestand oder Sicherheit des Bundes oder eines Landes, Leib, Leben oder Freiheit einer Person oder für Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt oder deren Erhaltung im öffentlichen Interesse geboten ist, aufgenommen. Die Eingriffsschwelle stimmt mit den bundesrechtlichen Eingriffsschwellen der Übermittlungsvorschriften im Telekommunikationsgesetz bzw. im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz überein.

Absatz 3

Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichts (BVerfG, a. a. O., Rz. 252), dass die Bestandsdatenauskunft auf der Grundlage der Internet-Protokolladresse keiner richterlichen Anordnung bedürfe, erfolgt die Streichung des Verweises auf Absatz 2.

Absatz 4

Satz 1 beinhaltet die Regelung des bisherigen § 72 Absatz 2 Nummer 3 mit redaktionellen Anpassungen. Satz 2 beinhaltet die Regelung des bisherigen § 72 Absatz 4.

§ 71

Aus rechtssystematischen Gründen wurde der bisherige Regelungsinhalt des § 71 in die Vorschrift § 68 übernommen. In die Vorschrift wurde im Regelungszusammenhang zu den eingriffsintensiven Befugnissen eine Rechtsgrundlage für den Einsatz von unbemannten Luftfahrtsystemen aus Gründen der Klarstellung der Zulässigkeit der Drohnenverwendung für bestimmte Datenerhebungsmaßnahmen aufgenommen.

Absatz 1

Satz 1 regelt, bei welchen Datenerhebungsmaßnahmen unter den Voraussetzungen der jeweils genannten Befugnisregelungen ein Drohneneinsatz zur Datenerhebung zulässig sein kann. Mit der Regelung erfolgt keine Befugniserweiterung. Satz 2 stellt klar, dass offene Bild- und Tonaufzeichnungen nach § 56, § 57 Absätze 1 bis 3 und 9 auch im Fall eines Drohneneinsatzes den Charakter als offene Maßnahme bewahren müssen. Nur im Fall von Gefahr im Verzug kann hiervon abgesehen werden. Satz 3 verpflichtet durch geeignete Maßnahmen (besondere Kennzeichnung des polizeilichen „Drohnenpilots“ oder Hinweis bei der jeweiligen Veranstaltung), um auf die Verwendung der Drohne aufmerksam zu machen.

Absatz 2

Die Regelung stellt in Satz 1 klar, dass soweit richterliche Anordnungen für Maßnahmen nach Absatz 1 erforderlich sind, diese auch den Einsatz von unbemannten Luftfahrtsystemen umfassen müssen. Die Regelung in Satz 2 dient der Klarstellung, dass Drohnen nicht genutzt werden dürfen für den Einsatz von Waffen.

Zu Nummer 22

§ 72

Aus rechtssystematischen Gründen und aus Gründen der Anwenderfreundlichkeit wurde der Regelungsinhalt des bisherigen § 72 jeweils in die Vorschriften § 66 Absatz 5, § 66a Absatz 7, § 67 Absatz 3 und § 70 Absatz 4 überführt. Die Vorschrift ist daher zu streichen.

Zu Nummer 23

§ 73

Die Inhalte der bisherigen Regelung des § 73 wurden aus Gründen der Klarstellung in nunmehr fünf Absätze gegliedert.

Absatz 1

Absatz 1 bestimmt, dass für nach dem Sächsischen Polizeivollzugsdienstgesetz geregelte gerichtliche Entscheidungen, die Maßgaben der nachfolgenden Absätze 2 bis 5 gelten.

Absatz 2

Absatz 2 beinhaltet die bisherige Regelung des § 73 Absatz 1 Nummer 1.

Absatz 3

Satz 1 beinhaltet die bisherige Regelung des § 73 Absatz 1 Nummer 2 Satz 1 mit Änderungen. Die Ergänzungen erfolgen in Konsequenz der Aufnahme neuer Befugnisregelungen (siehe § 57a Absatz 1 Satz 4 und Absatz 2). Der ergänzende Verweis auf § 60 Absatz 3 Satz 2 steht im Zusammenhang mit dem neu aufgenommenen Richtervorbehalt von Ausschreibungen zur verdeckten Kontrolle (bisher polizeiliche Beobachtung), soweit durch deren Anordnung eine Fristverlängerung über ein Jahr erfolgt. Satz 2 beinhaltet die bisherige Regelung des § 73 Absatz 1 Nummer 2 Satz 2. Satz 3 beinhaltet die bisherige Regelung des § 73 Absatz 1 Nummer 2 Satz 3. Satz 4 enthält zur Klarstellung die Verweisungen auf spezifische Fristenregelungen, die der Regelung in Satz 3 vorgehen.

Absatz 4

Satz 1 beinhaltet die bisherige Regelung des § 73 Absatz 2 Satz 1. Satz 2 beinhaltet die bisherige Regelung des § 73 Absatz 2 Satz 2. Satz 3 stellt sicher, dass bei eingriffsintensiven Maßnahmen nach § 57a Absatz 1 Satz 4 und Absatz 2 die richterliche Bestätigung der Maßnahme kurzfristig erfolgt. Satz 4 beinhaltet die bisherige Regelung des § 73 Absatz 2 Satz 3.

Absatz 5

Die Regelung beinhaltet die bisherige Regelung des § 73 Absatz 3. Mit der Ergänzung wird gewährleistet, dass auch für die eingriffsintensiven Befugnisse nach den §§ 21 Absatz 2, 57a, 61, 62b bis 68 die verfahrensrechtlichen Anforderungen des Absatzes 1 Nummer 2 gelten.

§ 74

Absatz 1

Die Änderungen oder Ergänzungen in Satz 1 erfolgen in Konsequenz der Aufnahme neuer benachrichtigungspflichtiger Befugnisse (§ 57a, § 62b) in das Sächsische Polizeivollzugsdienstgesetz, der Streichung der bisherigen Befugnis in § 59 oder sie stellen redaktionelle Folgeänderungen dar.

In Nummer 1 wurde eine Benachrichtigungspflicht im Hinblick auf die neue Befugnis zur Datenverarbeitung nach § 57a Absatz 1 Satz 4 und Absatz 2 im Hinblick auf die Zielperson der jeweiligen Maßnahme aufgenommen.

Nummer 2 dient der Klarstellung, dass eine Benachrichtigungspflicht bei Maßnahmen nach § 58 nur dann besteht, soweit im Ergebnis der manuellen Verifizierung eines Trefferfalls ein

Echttreffer vorliegt. Nur in diesem Fall, in dem eine Weiterverarbeitung der personenbezogenen Daten erfolgt, ist eine Benachrichtigung der betroffenen Person zur Gewährleistung von Rechtsschutz zweckmäßig.

Die Ergänzung in Nummer 3 erfolgt in Konsequenz der Ergänzung des § 60 um den Ausschreibungsgrund der Erkenntnisanfrage.

Die Änderung in Nummer 5 erfolgt in Konsequenz der Aufnahme der neuen Befugnis in § 62b zum retrograden biometrischen Identitätsabgleich gespeicherter Daten mit Daten des Internets in das Sächsische Polizeivollzugsdienstgesetz.

Die Änderungen in den Nummern 10 bis 13 sind Folge der systematischen Änderungen der Befugnisregelungen in den §§ 66a bis 68.

Die Änderung in Nummer 14 ist redaktionell. Die Benachrichtigungspflicht in Bezug auf Maßnahmen nach § 70 war bisher in Nummer 13 geregelt.

Absatz 2

Die Änderungen in Satz 1 sind Konsequenz redaktioneller Änderungen in Absatz 1 Satz 1.

Absatz 3

Mit der Änderung in Satz 3 wird eine klarstellende Regelung aufgenommen, dass die Strafverfolgungsbehörden nicht nur über das „ob“ der Zurückstellung, sondern auch über die Fristen der Benachrichtigung entscheiden. Mit der Änderung wird einer Regelungsbitte des Sächsischen Staatsministerium der Justiz nachgekommen.

§ 75

Die Änderungen oder Ergänzungen in Satz 1 erfolgen in Konsequenz der Aufnahme neuer benachrichtigungspflichtiger Befugnisse (§ 57a, § 62b) in das Sächsische Polizeivollzugsdienstgesetz, der Streichung der bisherigen Befugnis in § 59 oder sie stellen redaktionelle Folgeänderungen dar.

Zu Nummer 24

§ 76

Die Änderung in Absatz 2 Satz 3 stellt eine redaktionelle Folgeanpassung an Änderungen des § 61 dar.

Zu Nummer 25

§ 78

Die Ergänzungen und Änderungen stellen jeweils Folgeanpassungen dar.

Zu Nummer 26

§§ 79 bis 80d

Vorbemerkung zu den Änderungen und Ergänzungen in den §§ 79 bis 80d

Aus rechtssystematischen Gründen, zur Verbesserung der Anwenderfreundlichkeit und insbesondere zur Umsetzung der Rechtsprechung des Bundesverfassungsgerichts sowie des Sächsischen Verfassungsgerichtshofs wurde die Regelungssystematik der Vorschriften zur

Datenverarbeitung umgestaltet und umfassend geregelt. Aus Gründen der Anwenderfreundlichkeit wurden ergänzend Datenverarbeitungsbefugnisse aufgenommen, um die Zulässigkeit der Datenverarbeitung in den erforderlichen logischen Zusammenhängen umfassend zu regeln und das Erfordernis ergänzender Anwendung allgemeiner datenschutzrechtlicher Vorschriften (Sächsisches Datenschutz-Umsetzungsgesetz) auszuschließen. Zudem bestand in Folge des Urteils des Bundesverfassungsgerichts vom 1. Oktober 2024, 1 BvR 1160/19, Bundeskriminalamtgesetz II, Bedarf für eine gesetzgeberische Gestaltung der Anforderungen an eine Datenbevorratung (Herkunft, Art, Umfang), zu den zulässigen Speicherfristen von für auf Vorrat gespeicherte Daten zu bestimmen und schließlich die Anforderungen zu regeln, wenn bevorratete Daten genutzt.

Vor diesem Hintergrund wurden:

- in dem geänderten § 79 zunächst die (allgemeinen) Befugnisse zur Datenverarbeitung zu den bestehenden zulässigen Zwecken geregelt, die da sind: polizeiliche Aufgabenerfüllung, Vorgangsverwaltung und befristete Dokumentation zusammenfassend geregelt,

- in § 79a neu (bisher § 79) sodann die Befugnisse (Voraussetzungen und Grenzen) zur Datenweiterverarbeitung im Rahmen der Zweckbindung und im Rahmen der Zweckänderung bestimmt,

- in § 79b neu (bisher § 80) folgen sodann die besonderen Befugnisregelungen zur Zulässigkeit spezifischer Datenweiterverarbeitungszwecke aufgenommen, als da sind: die Aus- und Fortbildung, die wissenschaftliche Forschung, die Prävention von Straftaten oder die zweckändernde Verarbeitung von Vorgangsdaten zur Abwehr von Gefahren für hochrangige Rechtsgüter,

- in § 79c aus rechtssystematischen Aspekten die neue Befugnis zur Weiterverarbeitung vorhandener Daten zu Zwecken des Trainings und den Test von lernenden IT-Systemen als besonderer Zweckänderungsvorschrift aufgenommen,

- in den §§ 80, 80a, 80b und § 80c in Umsetzung des Urteils des Bundesverfassungsgerichts zur Zulässigkeit der Datenbevorratung vom 1. Oktober 2024, 1 BVR 1160/19, unterschieden nach den Kategorien von Personen (§ 28 SächsDSUG) und der Herkunft der Daten, Regelungen zu den Voraussetzungen vorsorgende Speicherungen und im Hinblick auf das Urteil des Sächsischen Verfassungsgerichts vom 25. Januar 2024 (Vf. 91-II-19) die Anforderungen, wenn bevorratete Daten genutzt werden, klar bestimmt,

- in § 80d schließlich der gesetzliche Rahmen für die Aussonderungsprüffristen unterschieden danach, ob die Speicherung von Daten für die konkrete Aufgabenbestimmung erfolgt oder ob die Speicherung vorsorgend erfolgt, normiert.

Aus Gründen der Klarstellung wurden die Regelung des § 91 Absatz 3 im Hinblick auf sämtliche Tatbestände, die zur Löschung von personenbezogenen Daten führen, klarstellend ergänzend erweitert.

§ 79

Absatz 1

Mit Absatz 1 wird im Sächsischen Polizeivollzugsdienstgesetz nunmehr eine allgemeine Datenverarbeitungsbefugnis aufgenommen, die es der Polizei erlaubt, personenbezogene Daten zur Aufgabenerfüllung zu verarbeiten, soweit dies erforderlich ist. Der Begriff des „Verarbeitens“ bildet den Oberbegriff (siehe Begriffsbestimmung „Verarbeiten“ in § 2 Nummer 3 SächsDSUG) für verschiedene Arten der Datenverarbeitung. Er erfasst insbesondere

die Speicherung personenbezogener Daten. Da eine solche allgemeine Datenverarbeitungsbefugnisregelung im Sächsischen Polizeivollzugsdienstgesetz bisher fehlte, war im Hinblick auf die Befugnis zur Speicherung von Daten zur Aufgabenerfüllung immer ein „Rückgriff“ auf die allgemeine Vorschrift des § 3 Absatz 1 SächsDSUG erforderlich. Mit der Aufnahme der Regelung in das Sächsische Polizeivollzugsdienstgesetz wird diese bereichsspezifische Regelungslücke nunmehr geschlossen und die Anwenderfreundlichkeit erhöht.

Absatz 2

Absatz 2 beinhaltet die bisher in § 80 Absatz 7 enthaltene Befugnis zur Verarbeitung personenbezogener Daten zu Zwecken der Vorgangsverwaltung oder zu Zwecken der befristeten Dokumentation mit der bestehenden engen Zweckbindung.

Absatz 3

Die Regelung in Absatz 3 stellt klar, dass, soweit gesetzliche Regelungen die Einrichtung von Informationsverbünden unter Beteiligung der Polizei vorsehen (Beispiel hierfür ist § 29 BKAG), für die Datenverarbeitung durch die Polizei Sachsen in dem betreffenden Dateisystem des Informationsverbundes, unbeachtet sonstiger gesetzlicher Anforderungen an die Datenverarbeitung in dem Informationsverbund (Beispiel ist § 30 BKAG), für die Zulässigkeit der Datenverarbeitung durch die Polizei Sachsen die Regelungen des Sächsische Polizeivollzugsdienstgesetzes maßgeblich sind.

Absatz 4

Mit der Regelung wird eine bestehende Befugnislücke, angelehnt an die Regelung in § 16 Absatz 6 BKAG, geschlossen (siehe auch § 34 Absatz 6 PolDVG HH, § 71 Absatz 2 PolG BW). Zum Schutz einer Person oder zur Eigensicherung von Polizeibediensteten kann die Speicherung von personengebundenen Hinweisen (PHW) erforderlich sein. Beispiele für PHW sind „bewaffnet“, „gewalttätig“, „Freitodgefahr“. Die Vergabe eines PHW erfolgt im Einzelfall und umfasst jeweils die Prüfung der Erforderlichkeit, Geeignetheit und der Verhältnismäßigkeit im engeren Sinne. Am Beispiel des PHW „Freitodgefahr“ kann die Polizei bei Bedarf (beispielsweise im Hinblick auf Festnahme oder Ingewahrsamnahme) bereits im Vorfeld geeignete Maßnahmen ergreifen, um die Suizidgefahr des Betroffenen abzuwehren. Vorhandene Erkenntnisse über Aggressionen gegen Polizeibedienstete vor dem Hintergrund religiöser oder weltanschaulicher Überzeugungen können die Speicherung des PHW „gewalttätig“ rechtfertigen. Die Regelung lässt darüber hinaus die Verarbeitung von ermittlungsunterstützenden Hinweisen (EHW) zu, wenn sie geeignet sind, dem Schutz Dritter oder der Gewinnung von weiteren Ermittlungshinweisen zu dienen. Ermittlungsunterstützende Hinweise sind Hinweise auf Besonderheiten einer natürlichen Person, die dazu geeignet sind, einen polizeilichen Kontext zu verdeutlichen, polizeiliches Handeln zielgerichteter zu steuern bzw. zu unterstützen oder die dem Schutz Dritter dienen. Beispiele für EHW sind „Kfz-Dieb“, „Reisender Täter“, „Intensivtäter“. Über die bundeseinheitlich abgestimmten Leitfäden zur Vergabe von PHW und EHW wird die Vergabe vereinheitlicht.

§ 79a

Absatz 1

Zur Klarstellung, dass sich Satz 1 (in Abgrenzung zu Satz 2) auf Daten bezieht, die die Polizei selbst erhoben hat, erfolgt die Aufnahme des Wortes „selbst“. Mit der Ergänzung „unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift“ werden die Anforderungen an den Prüfungsmaßstab einer weiteren Nutzung von Daten über den konkreten Anlass hinaus im Rahmen des ursprünglichen Zwecks (zweckwahrende Nutzung) nach Maßgabe der Ausführungen des BVerfG präzisiert (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rz. 278ff).

Satz 2 entspricht der bisherigen Regelung in § 79 Absatz 1 Satz 2.

Absatz 2

Die Ergänzung in Satz 1 stellt klar, dass spezifisch geregelte Weiterverarbeitungsbefugnisse, die eine zweckändernde Verarbeitung von personenbezogenen Daten erlauben, die Regelung des Satz 1 verdrängen. Beispiel hierfür sind die Regelung in Absatz 4, § 79b und die §§ 80ff. Satz 2 beinhaltet die bisherige Regelung von § 79 Absatz 3 Satz 3.

§ 79b

In der Vorschrift werden die bisherigen Befugnisregelungen zur Weiterverarbeitung von zu Zwecken der Aufgabenerfüllung, der Vorgangsverwaltung, der zeitlich befristeten Dokumentation behördlichen Handelns oder der Protokollierung automatisierter Datenverarbeitung aus rechtssystematischen Gründen zusammengeführt. Neu aufgenommen wurde die Befugnis zur zweckändernden Datenverarbeitung aus der Aufgabenerfüllung zu Zwecken der Gefahrenvorsorge durch Täteransprache.

Absatz 1

Die Regelung entspricht der Bisherigen in § 80 Absatz 6.

Absatz 2

Mit der Regelung wird eine Rechtsgrundlage für die zweckändernde Verarbeitung von Daten aus der polizeilichen Aufgabenerfüllung zu Zwecken der Gefahrenvorsorge (Prävention) aufgenommen. Die Regelung ermöglicht die Weiterverarbeitung von Adressdaten von Mitgliedern der extremistischen Szene, zu denen Erkenntnisse zur Begehung politisch motivierter Straftaten vorliegen, zum Zweck der Täteransprache und der Beratung durch die Polizei im Rahmen des Aussteigerprogramms Sachsen.

Absatz 3

Mit der Aufnahme einer spezifischen Befugnis zur Weiterverarbeitung von personenbezogenen Daten aus der polizeilichen Aufgabenerfüllung zu archivarischen oder wissenschaftlichen Zwecken wird aus rechtssystematischen Gründen entsprechend der Regelung in § 6 Sächsisches Datenschutz-Umsetzungsgesetz eine bereichsspezifische Regelung getroffen.

Absatz 4

Abweichend von der in § 79a Absatz 2 geregelten strikten Zweckbindung erlaubt die Regelung in Absatz 3 eine zweckändernde Verarbeitung zu Zwecken der Vorgangsverwaltung oder zeitlich befristeten Dokumentation oder Protokollierung der Datenverarbeitung gespeicherten personenbezogenen Daten in besonders gelagerten Einzelfällen, soweit dies zur Abwehr von Gefahren für hochrangige Rechtsgüter oder zur Verhütung von Straftaten von erheblicher Bedeutung erforderlich ist. Die Regelung des Anordnungsgebots durch die Behördenleitung wird die Zulässigkeit einer Zweckänderung in verfahrensrechtlicher Hinsicht gesichert. Eine solche Zweckänderungsvorschrift war ursprünglich in § 43 Absatz 1a Sächsisches Polizeigesetz enthalten für Daten der Vorgangsverwaltung. Durch ein redaktionelles Versehen wurde die Regelung jedoch im Rahmen der Novelle des Polizeirechts in 2019 nicht in das Sächsische Polizeivollzugsdienstgesetz überführt. Die Ergänzung dient der Korrektur.

§ 79c

Aus Gründen der Klarstellung wurde in § 79c analog zu der Regelung in § 37a PolDVG HH eine Befugnis aufgenommen, vorhandene personenbezogene Daten der Polizei zum

Zweck des Trainierens und Testen von lernenden IT-Systemen (KI) weiterverarbeiten zu dürfen. Vor dem Hintergrund der neuen Befugnisregelungen in den §§ 57a Absatz 1 Satz 4 und Absatz 2, 62a und 62b, die den Einsatz von KI gestützter technischer Systeme erfordern, besteht Bedarf zum Zweck des Trainings entsprechender Software. Ziel ist es, durch Training mit polizeilichen Daten nachvollziehbare Datenverarbeitungsschritte in der jeweiligen (eigen- oder fremdentwickelten) Software unveränderlich zu programmieren und damit die jeweilige spezifische Datenverarbeitung, so beispielsweise die Mustererkennung nach § 57a Absatz 1 Satz 1 oder die retrograde biometrischen Identitätsfeststellung gemäß § 57a Absatz 1 Satz 4 oder Absatz 2 in besonderen Gefahrensituationen durch austrainierte und ausgelernte Systeme zu ermöglichen.

Absatz 1

Satz 1 erlaubt der Polizei zum Zweck des Trainierens oder Testens von lernenden IT-Systemen, vorhandene personenbezogene Daten weiterverarbeiten zu dürfen. Die Regelung knüpft an das Erfordernis der Weiterverarbeitung der Daten für die Aufgabenerfüllung an. Sie erlaubt, dass Daten zu dem Zweck auch an Dritte oder Auftragsdatenverarbeiter übermittelt werden dürfen. Satz 2 setzt das Verbot der Verwendung von Systemen zur biometrischen Kategorisierung, mit denen natürliche Personen auf der Grundlage ihrer biometrischen Daten kategorisiert werden, nach Artikel 5 Absatz 1 Unter-Absatz 1 lit. g KI-VO um. Satz 3 stellt sicher, dass die Nachvollziehbarkeit der Datenverarbeitungsschritte in den Systemen sichergestellt wird. Satz 4 schließt aus Gründen der Verhältnismäßigkeit die Weiterverarbeitung von Daten aus der Wohnraumüberwachung aus.

Absatz 2

Satz 1 verpflichtet die Polizei aus Gründen der Verhältnismäßigkeit zum Zweck des Trainierens oder Testens vorrangig anonymisierte Daten zu verwenden und bestimmt die Voraussetzungen für Ausnahmen von der Verpflichtung zur Verwendung anonymisierter Daten.

Absatz 3

Die Sätze 1 und 2 bestimmen, unter welchen Voraussetzungen vorhandene personenbezogene Daten der Polizei an Dritte oder Auftragsdatenverarbeiter zum Zweck des Testens und Trainierens von für die Aufgabenerfüllung der Polizei erforderliche KI übermittelt werden dürfen. Satz 3 bestimmt, dass Daten aus der Wohnraumüberwachung aus Gründen der Verhältnismäßigkeit von der Übermittlung an Dritte oder Auftragsdatenverarbeiter zum Zweck des Testens oder Trainierens von KI ausgenommen sind.

Absatz 4

Die Sätze 1 und 2 enthalten besondere Maßgaben zur Verhinderung von im Zusammenhang mit der Übermittlung von polizeilichen Daten an Dritte oder Auftragsdatenverarbeiter bestehende Gefahren des Datenmissbrauchs.

Absatz 5

Adressat der Regelungen in den Sätzen 1 und 2 sind die Dritt- oder Auftragsdatenverarbeiter. Durch die Regelungen werden diese grundsätzlich verpflichtet, erlangte Daten nach Abschluss des Trainings und des Tests zu löschen. Die Zulässigkeit einer Weiternutzung wird unter einen ausdrücklichen Genehmigungsvorbehalt der Polizei gestellt.

Absatz 6

Absatz 6 verpflichtet das Sächsische Staatsministerium des Innern, das Nähere zu dem Verfahren des Testens oder Trainierens von lernenden KI-Systemen durch Verwaltungsvorschrift nach Maßgabe der Anforderungen der Nummern 1 bis 7 zu regeln. Klarstellend

wurde die Verpflichtung aufgenommen, die oder den Sächsischen Datenschutz- und Transparenzbeauftragten zu der Verwaltungsvorschrift anzuhören.

Vorbemerkung zu den §§ 80, 80a bis 80c

Mit den Regelungen wird der Rechtsrahmen für die Zulässigkeit der Fortspeicherung von personenbezogenen Daten über das jeweilige konkrete Ausgangsverfahren hinaus bestimmt.

In diesem Zusammenhang bestand Bedarf sowohl das Urteil des Bundesverfassungsgerichts vom 1. Oktober 2024, 1 BvR 1160/19, Bundeskriminalamtgesetz II, als auch das Urteil des Sächsischen Verfassungsgerichtshofs vom 25. Januar 2024, Vf. 91-II-19 umzusetzen.

Das Bundesverfassungsgericht hat in dem Grundsatzurteil vom 1. Oktober 2024 dargelegt, dass die vorsorgende Speicherung regelhaft eine zweckändernde Weiterverarbeitung darstelle für deren verfassungsrechtlicher Rechtfertigung es einer Rechtsgrundlage bedürfe. Weiterhin müsse der Gesetzgeber angemessene Speicherzwecke und Speicherschwellen sowie eine angemessene Speicherdauer bestimmen (BVerfG, a. a. O., Rz. 181f). Der Gesetzgeber sei insbesondere gefordert, ein hinreichend ausdifferenziertes Regelungskonzept zur Speicherdauer zu formulieren (BVerfG, a. a. O., Rz. 200). Zwar ist Adressat dieses Urteils der Bund und betrifft dieses „nur“ die gesetzliche Regelung zur vorsorgenden Speicherung von personenbezogenen Daten im polizeilichen Informationsverbund. Aus den grundlegenden Ausführungen des Bundesverfassungsgerichts zur vorsorgenden Speicherung und zum Grundrecht auf informationelle Selbstbestimmung ist jedoch abzuleiten, dass die Ausführungen des Gerichts zu den Anforderungen an eine vorsorgende Speicherung und des insoweit bestehenden Regelungsauftrags, den der Gesetzgeber zu erfüllen habe, gleichermaßen Maßstab für die vorsorgende Speicherung in polizeilichen Landes-Informationssystemen bilden. Ein gesetzgeberischer Umsetzungsbedarf besteht daher auch dann, wenn die vorsorgende Datenverarbeitung nur in technischen Systemen erfolgt, auf die „nur“ die Bediensteten einer Landespolizei Zugriff haben. Vor diesem Hintergrund besteht Regelungsbedarf für eine spezifische Befugnisregelung zur vorsorgenden Speicherung, die insbesondere dem potentiell hohen Eingriffsgewicht der vorsorgenden Speicherung nach Herkunft der Daten (Rz. 159), der Eingriffsintensität der Datenerhebung insbesondere im Hinblick auf eine verhältnismäßige Ausgestaltung einer Speicherschwelle und der Speicherdauer differenzierend Rechnung trägt.

Das Eingriffsgewicht einer vorsorgenden Speicherung werde wesentlich geprägt durch:

- Art und Umfang der Daten (BVerfG, a. a. O., Rz. 160),
- dem Gewicht des vorausgegangenen Datenerhebungseingriffs (BVerfG, a. a. O., Rz. 159),
- insbesondere welchen Anlass die betroffene Person zu einer Speicherung gegeben hat (BVerfG, a. a. O., Rz. 161 objektiver Rechtsverstoß - Beschuldigter oder nur verdächtige Person),
- der denkbaren Verwendung von Daten und der damit verbundenen Folgen für den Betroffenen und schließlich
- der Speicherdauer (BVerfG, a. a. O., Rz. 164).

Dem potentiell hohen Eingriffsgewicht einer vorsorgenden Speicherung müsse der Gesetzgeber begegnen und den Staatsinteressen (Sicherheit) und Grundrechtsschutz des Bürgers (Achtung und Würde und Eigenwert) in einer gesetzlichen Regelung angemessen Rechnung tragen (BVerfG, a. a. O., Rz. 91). Die vorsorgende Speicherung stelle eine Zweckänderung dar. Eine solche bedürfe als Grundrechtseingriff einer gesetzlichen Grundlage (BVerfG, a. a. O., Rz. 181). Für eine verfassungsrechtliche Rechtfertigung bedürfe die

vorsorgende Speicherung der Festlegung angemessener Speicherzwecke und Speicherschwellen sowie der Bestimmung einer angemessenen Speicherdauer (BVerfG, a. a. O., Rz. 182). Bei der Speicherung von Daten für die Verhütung und Verfolgung vom Speicherzweck erfasster Straftaten sei dies nur gegeben, wenn eine hinreichende Wahrscheinlichkeit dafür bestehe, dass die Betroffenen eine strafrechtlich relevante Verbindung zu möglichen Straftaten aufweisen und gerade die gespeicherten Daten zu deren Verhütung oder Verfolgung angemessen beitragen können. Diese Prognose müsse sich auf zureichende tatsächliche Anhaltspunkte stützen (BVerfG, a. a. O., Rz. 186). Als taugliche Prognosekriterien können insbesondere die Art, Schwere und Begehungsweise der vormaligen Straftat sowie der Persönlichkeit des Betroffenen und sein bisheriges strafrechtliches Erscheinungsbild in Frage kommen. Ferner ob die betroffene Person wiederholt und in welchem Ausmaß sie straffällig geworden ist (BVerfG, a. a. O., Rz. 186).

Die vorsorgende Speicherung dürfe zudem nicht zu einer Umgehung der verfassungsrechtlichen Anforderungen an eine zweckändernde Weiternutzung von personenbezogenen Daten führen (BVerfG, a. a. O., Rz. 191).

Im Kontext der bisherigen Regelungen des Sächsischen Polizeivollzugsdienstgesetzes zur vorsorgenden Speicherung hatte der Sächsische Verfassungsgerichtshof die Vorschrift des bisherigen § 80 Absatz 2 Nummer 1, 2 und 4 SächsPVDG für nicht normenklar und daher nicht verfassungsgemäß beurteilt. Die Anforderungen an die Normenklarheit bedingen, dass für den betroffenen Bürger anhand des Inhalts der Norm beurteilungsfähig sein muss, unter welchen Voraussetzungen eine Weiterverarbeitung seiner im Rahmen repressiver Maßnahmen gewonnenen personenbezogenen Daten über das Ausgangsverfahren hinaus zulässig sind. Aufgrund der bestehenden Regelungstechnik sei aber unklar, ob für die Weiterverarbeitung von vorsorgend gespeicherten Daten nach § 80 Absatz 2 SächsPVDG, die Anforderungen des § 79 Absatz 2 mit zu prüfen sind, somit zusätzlich gelten (SächsVGH, a. a. O., Seite 121f).

§ 80

Die Regelung (neu) enthält in Absatz 1 die Befugnis zur vorsorgenden Speicherung von aus repressiven Maßnahmen erhobenen personenbezogenen Daten zu Verurteilten, Beschuldigten, Verdächtigen und Anlasspersonen zur künftigen Verhütung oder Verfolgung von Straftaten und bestimmt gemäß den Anforderungen des Bundesverfassungsgerichts die maßgeblichen Kriterien für die erforderliche tatsachengestützte Prognoseprüfung, in deren Ergebnis die Zulässigkeit der vorsorgenden Speicherung im Einzelfall vorliegen können. Absatz 2 bestimmt den Rahmen der Datenspeicherung je nach Personenkategorie und damit nach dem jeweiligen Anlass, den die betroffene Person für die Speicherung gegeben hat. Absatz 3 beinhaltet unter dem Aspekt „Regelungszusammenhang“ die bisher in § 80 Absatz 4 enthaltene sofortige Löschungsverpflichtung (Ablehnung Eröffnung das Hauptverfahren, nicht nur vorläufige Verfahrenseinstellung). Absatz 4 enthält durch die Verweisung auf § 79a Absatz 2 den rechtlichen Rahmen, der Voraussetzung für die zweckändernde Weiternutzung der Daten ist.

Absatz 1

In Absatz 1 wird die bisherige Regelung aus § 80 Absatz 2 überführt und dahingehend geändert, dass die Anforderung der Prognose der künftigen Begehung einer Straftat (sog. Negativprognose) Voraussetzung der vorsorgenden Speicherung repressiv erhobener Daten sowohl von Verurteilten und Beschuldigten als auch von Verdächtigen ist. Für die Kategorie der Anlasspersonen bleibt es im Hinblick auf die vorsorgende Speicherung personenbezogener Daten bei der abweichenden Prognoseprüfung. Der Wortlaut der Regelung stellt klar, dass die vorsorgende Speicherung erforderlich sein muss. In Umsetzung der Rechtsprechung des Bundesverfassungsgerichts wird anstelle des bisherigen Begriffs „weiterverarbeiten“ der spezifische Begriff der „vorsorgenden Speicherung“ übernommen. Das Bundesverfassungsgericht hat in dem genannten Grundsatzurteil eine Speicherung als

„vorsorgend“ bezeichnet, wenn sie nicht zum Zweck ihrer Erhebung oder Herstellung erfolgt ohne dass eine neue Zweckbindung, die zu einer unmittelbaren weiteren Nutzung führt, an ihre Stelle gesetzt wird. Die neu gesetzten Zwecke liegen in der Bereithaltung der Daten für den Fall, dass sie für konkrete Zwecke künftig benötigt werden (BVerfG, a. a. O, Rz. 158).

Auch im Gesetzentwurf des Bundes zur Umsetzung des Urteils des BVerfG im Bundeskriminalamtgesetz (BT Drs. 21/234) wird im Hinblick auf die bevorratende Speicherung im Informationsverbund der neue Begriff der vorsorgenden Speicherung geführt (siehe Gesetzentwurf, § 30a Absatz 2 BKAG-neu). Aus Gründen der Harmonisierung und der Anwenderfreundlichkeit ist daher analog zu formulieren.

Absatz 2

Die Regelung in Absatz 2 bestimmt den zulässigen Datenkranz der vorsorgenden Speicherung nach Personenkategorien unter Berücksichtigung des Anlasses, den die betroffene Person für die Speicherung gegeben hat. Zur näheren Eingrenzung des Datenkranzes wird an die Regelungen der BKA-Datenverordnung angeknüpft.

Absatz 3

Die Regelung überführt den Regelungsinhalt des § 80 Absatz 4 zur Pflicht zu unverzüglichen Löschung, soweit die Eröffnung des Hauptverfahrens unanfechtbar abgelehnt wird oder das Verfahren nicht nur vorläufig eingestellt wurde. Aufgrund der Wertigkeit dieser datenschutzrechtlichen Verpflichtung zur Löschung wird der bisherige Regelungsstandort beibehalten und nicht in den (eigentlich zutreffenden) Regelungszusammenhang des § 91 Absatz 3 gestellt.

Absatz 4

Absatz 4 bestimmt, dass für die weitere Verarbeitung der vorsorgend gespeicherten Daten die rechtlichen Anforderungen des § 79a Absatz 2 gelten. Das Bundesverfassungsgericht hatte hierzu formuliert, dass unerlässliche Voraussetzung für die Verfassungsmäßigkeit der Speicherbefugnis weiterhin klar normierte Verwendungsregeln sind, die insbesondere den im Urteil des Bundesverfassungsgerichts vom 20. April 2016, 1 BvR 966/09, formulierten verfassungsrechtlichen Anforderungen an die zweckändernde Weiterverarbeitung personenbezogener Daten genügen müssen (siehe Urteil, a. a. O., Rz. 189). Mit der Regelung wird zugleich die Vorgabe des Sächsischen Verfassungsgerichtshofs umgesetzt, durch normenklare Regelung sicherzustellen, dass für den betroffenen Bürger anhand des Inhalts der Norm beurteilungsfähig ist, unter welchen Voraussetzungen eine Weiterverarbeitung seiner im Rahmen repressiver Maßnahmen gewonnenen personenbezogenen Daten über das Ausgangsverfahren hinaus zulässig ist.

§ 80a

Die Regelung (neu) enthält in Absatz 1 die Befugnis zur vorsorgenden Speicherung von aus repressiven Maßnahmen erhobenen personenbezogenen Daten zu Zeugen, Opfern, Hinweisgebern und Kontakt- und Begleitpersonen, soweit dies zu Zwecken der künftigen Verhütung oder Verfolgung von Straftaten erforderlich ist. Die Regelung in Absatz 1 entspricht der bisherigen Regelung des § 80 Absatz 3.

Absatz 1

Satz 1 enthält die bisherige Regelung des § 80 Absatz 3 Satz 1.

Satz 2 bestimmt, dass eine Speicherung von Personen nach Satz 1 Nummer 1 bis 3 ohne Einwilligung nur erfolgen darf, wenn anderenfalls der Speicherungszweck gefährdet werden würde und entspricht der bisherigen Regelung von § 80 Absatz 3 Satz 3. Satz 3 entspricht der bisherigen Regelung des § 80 Absatz 3 Satz 2, dass eine Speicherung der Personen

nach Absatz 1 Nummer 1 bis 3 grundsätzlich der Einwilligung der betroffenen Personen bedarf.

Absatz 2

Die Regelung in Absatz 2 bestimmt den zulässigen Datenkranz der vorsorgenden Speicherung und unterscheidet nach dem Anlass den die betroffenen Personenkategorien für die Speicherung gegeben haben. Zur näheren Eingrenzung des Datenkranzes wird an die Regelungen der BKA-Datenverordnung angeknüpft.

Absatz 3

Absatz 3 bestimmt, dass für die weitere Verarbeitung der vorsorgend gespeicherten Daten die rechtlichen Anforderungen des § 79a Absatz 2 gelten.

§ 80b

Mit der Regelung wird eine spezifische Rechtsgrundlage für die vorsorgende Speicherung von zu Gefahrenabwehrzwecken erhobenen personenbezogenen Daten zu Zwecken der künftigen Gefahrenabwehr (Absatz 1 Nummer 1) oder zu Zwecken der künftigen Strafverfolgung (Absatz 1 Nummer 2) geschaffen.

Satz 1 Nummer 1 bildet die Regelung für die vorsorgende Speicherung von Personen zu denen die tatsachengestützte Prognose einer künftigen (Selbst-) Gefährdung besteht. Satz 1 Nummer 2 bildet die Rechtsgrundlage für die vorsorgende Speicherung von Personen, bei denen aufgrund von präventiv erhobenen polizeilichen Erkenntnissen die tatsachengestützte Prognose besteht, dass die betroffene Person künftig Straftaten von erheblicher Bedeutung begeht. Die vorsorgende Speicherung, der zu präventiven Zwecken erhobenen Daten zu den betroffenen Personen erfolgte bisher über die Weiterverarbeitungsgeneralklausel des bisherigen § 80 Absatz 1.

In der polizeilichen Praxis besteht das Erfordernis zu präventiven Zwecken erhobene personenbezogene Daten zu Personen vorsorgend zu speichern, zu denen vorliegende polizeiliche Erkenntnisse die Prognose einer künftigen (Selbst)Gefährdung der Person begründen. Praktische Anwendungsfälle sind insbesondere Suizidenten, Personen, die aufgrund einer Erkrankung (beispielsweise Demenz) orientierungslos sind oder sog. Dauer-Ausreißer, Kinder oder Jugendliche, die wiederholt von zu Hause „ausreißen“. Zum Zweck der Abwehr künftiger Gefahren ist die vorsorgende Speicherung personenbezogener Daten zu diesen Personen erforderlich (Satz 1 Nummer 1). Satz 1 Nummer 2 bildet die analoge Rechtsgrundlage für die vorsorgende Speicherung von Anlasspersonen gemäß §80 Absatz 1 Nummer 4, soweit die Datenerhebung auf der Grundlage dieses Gesetzes erfolgt ist. Wie bei § 80 Absatz 1 Nummer 4 ist Voraussetzung für die vorsorgende Speicherung, dass eine tatsachengestützte Prognose der künftigen Begehung von Straftaten von erheblicher Bedeutung durch die betreffende Person begründet ist.

Satz 2 bestimmt, welche Daten zu den Personen nach Absatz 1 Nummer 1 und 2 jeweils gespeichert werden dürfen.

Absatz 2

Die Regelung bestimmt, welche Anforderungen an die weitere Verwendung der nach Absatz 1 vorsorgend gespeicherten personenbezogenen Daten gelten.

§ 80c

Mit der Regelung (neu) wird eine Rechtsgrundlage für die vorsorgende Speicherung von personenbezogenen Daten von Erziehungsberechtigten, Vormündern und Bewährungshelfern in das Sächsische Polizeivollzugsdienstgesetz aufgenommen.

Satz 1 bezeichnet den Personenkreis, dessen Daten im Zusammenhang mit einer vorsorgenden Speicherung von Daten einer Person nach § 80, § 80a, § 80b vorsorgend gespeichert werden können. Satz 2 bestimmt, dass die vorsorgende Speicherung der personenbezogenen Daten sonstiger Personen nicht recherchefähig erfolgen darf. Damit wird sichergestellt, dass ein Abruf personenbezogener Daten der sonstigen Person allein über einen Datenabruf der Person erfolgen darf, zu der die Speicherung der sonstigen Person erforderlich war. Durch die technische Gestaltung der Systeme ist sicherzustellen, dass nach sonstigen Personen nicht unmittelbar recherchiert werden kann. Satz 3 bezeichnet die personenbezogenen Daten, die zu sonstigen Personen gespeichert werden dürfen, abschließend. Satz 4 regelt durch den Verweis auf § 79a, welche rechtlichen Anforderungen für die Weiterverarbeitung der Daten gelten.

§ 80d

Das Bundesverfassungsgericht hat in dem Urteil vom 1. Oktober 2024, 1 BvR 1160/19, im Kontext der Ausführungen zur vorsorgenden Speicherung formuliert, dass es für die verfassungsrechtliche Rechtfertigung der vorsorgenden Speicherung personenbezogener Daten zudem der gesetzlichen Regelung einer angemessenen Speicherdauer bedürfe (Rz. 187). Die verfassungsrechtlich gebundene kompensatorische Einhegung einer Befugnis zur vorsorgenden Speicherung gebiete ein Regelungskonzept, dass differenzierte Prüfungs- und Aussonderungsfristen setzt. Auch muss die vorsorgende Speicherung grundsätzlich begrenzt werden (Rz. 184, 187).

In Umsetzung der Rechtsprechung des Bundesverfassungsgerichts werden durch die Regelungen in § 80d sowohl allgemeine Kriterien (Absatz 2) für die Bestimmung von Aussonderungsprüffristen für die vorsorgende Speicherung bestimmt als auch ein gesetzlicher Rahmen (Absatz 3) für Aussonderungsprüffristen für vorsorgend gespeicherte Daten vorgegeben, der nach Personenkategorien, Schwere der Straftat und Alter der betroffenen Person unterscheidet.

Die Vorschrift beinhaltet daneben erforderliche Regelungen zum Fristbeginn der Aussonderungsprüffrist für die Verarbeitung von Daten für die konkreten Zwecke, zu denen die Erhebung erfolgte (Absatz 1 Satz 5 3 Satz 2) und zur möglichen Verlängerung einer Aussonderungsprüffrist und trifft Regelungen zur Höchstspeicherfrist (Absatz 4)

Absatz 1

Satz 1 (neu) enthält den Grundsatz, dass für die Zulässigkeit der Dauer der Speicherung personenbezogener Daten zum Zweck der Erfüllung einer bestimmten Aufgabe Maßstab die Erforderlichkeit des Datums für die konkrete Aufgabenerfüllung ist. Die Sätze 2 bis 4 beinhalten die bisher in § 91 Absatz 3 Sätze 1, 2 und 4 enthaltenen Regelungen, um durch den rechtssystematischen Zusammenhang die Verständlichkeit der Regelungen (wann ist besteht eine Verpflichtung zur Löschung) sicherzustellen. Satz 2 bestimmt die Anforderungen an die Zulässigkeit der Speicherung und der Dauer der Speicherung von für eine konkrete Aufgabe und für einen bestimmten Zweck erhobenen oder erlangten Daten. Hierfür wird als Maßstab für die Speicherung und die Dauer der Speicherung der Grundsatz der Erforderlichkeit der (weiteren) Speicherung für die jeweilige konkrete Aufgabenerfüllung vorausgesetzt. Satz 3 überführt den bisherigen Regelungsinhalt von § 91 Absatz 3 Satz 3, wonach durch festzulegende Prüffristen sicherzustellen ist, dass die Erforderlichkeit der weiteren Speicherung der Daten für die konkrete Aufgabenerfüllung zu überprüfen ist. Satz 4 überführt den bisherigen Regelungsinhalt von § 91 Absatz 3 Satz 4 und bestimmt abweichend von der bisherigen Regelung kürze Aussonderungsprüffristen gestaffelt nach Erwachsene (5 Jahre, bisher 10 Jahre, Jugendliche (3 Jahre, bisher 5 Jahre) und Kinder (zwei Jahre) und bestimmt den Beginn des Fristlaufs mit Kenntniserlangung durch die Polizei.

Absatz 2

Die Regelung beinhaltet die allgemeinen Kriterien, die die Polizei bei der Bestimmung von Aussonderungsprüffristen im Hinblick auf vorsorgend gespeicherte Daten anzuwenden hat.

Absatz 3

Satz 1 Nummer 1 bis 3 enthält gestaffelt nach Schwere der Straftat, dem Anlass, den die betroffene Person für die Speicherung gesetzt hat (Verurteilter, Beschuldigter, Verdächtiger) und dem Alter (Erwachsene, Jugendliche, Kinder) Regelungen zu dem maximalen Aussonderungsprüffristen.

Nummer 1 bestimmt den maximalen Rahmen für die im Einzelfall festzulegende Aussonderungsprüffrist von Verurteilten 10 Jahre bei Erwachsenen, 5 Jahre bei Jugendlichen und zwei Jahre bei Kindern. Die Regelung überführt die bisherige Frist aus § 91 Absatz 3 Satz 4.

Nummer 2 bestimmt als maximalen Rahmen für die im Einzelfall festzulegende Aussonderungsprüffrist von Beschuldigten oder Verdächtigen unter Berücksichtigung der Schwere der Straftat und des Alters der betroffenen Person.

Nummer 3 trifft im Hinblick auf den Personenkreis der Anlasspersonen nach § 80 Absatz 1 Nummer 4 und § 80b Absatz 2 eine nach Alter gestaffelte maximale Aussonderungsprüffrist.

Nummer 4 regelt die maximalen Aussonderungsprüffristen für Zeugen, Opfer, Hinweisgeber und überführt die bisherige Regelung aus § 91 Absatz 4 Sätze 4 bis 7 und unterscheidet zwischen einwilligungsbasierter vorsorgender Speicherung und vorsorgender Speicherung ohne Einwilligung.

Nummer 5 bestimmt die maximalen Aussonderungsprüffristen für Kontakt- und Begleitpersonen (siehe Begriffsbestimmung in § 4 Nummer 9) und unterscheidet bei der Fristlänge insbesondere nach der Schwere der Straftat der „anderen Person“ im Sinne der Begriffsbestimmung in § 4 Nummer 9.

Nummer 6 bestimmt die maximalen Aussonderungsprüffristen für vorsorgende Speicherung von durch präventive Maßnahmen erhobene personenbezogene Daten zu gefährdeten, hilflosen oder vermissten Personen gemäß § 80b Absatz 1 gestaffelt nach Alter.

Nummer 7 bestimmt die maximalen Aussonderungsprüffristen für die vorsorgende Speicherung von sonstigen Personen nach § 80c.

Satz 2 regelt im Hinblick auf Erstspeicherungen von Verdächtigen oder Beschuldigten von schweren Straftaten nach § 100a Absatz 2 der Strafprozessordnung (Nummer 2a) kürzere Aussonderungsprüffristen.

Satz 3 bestimmt als Fristbeginn für die Aussonderungsprüffristen den Tag, an dem die vorsorgende Speicherung erfolgt ist und überführt die Ausnahmeregelung des § 91 Absatz 3 Satz 10.

Absatz 4

Absatz 4 enthält in Satz 1 die Anforderungen an die Verlängerung einer Aussonderungsprüffrist und sieht eine solche nur dann vor, wenn weiterhin relevante Umstände vorliegen, die die Verlängerung der Aussonderungsprüffrist begründen können, oder wenn neue für die Bestimmung der Aussonderungsprüffrist relevante Umstände hinzugetreten sind. Sätze 2 und 3 bestimmen schließlich Höchstspeicherfristen im Hinblick auf „sonstige Straftaten“ und für die Speicherung von Zeugen, Opfern, Hinweisgebern bei Nichtvorliegen der Einwilligung.

Absatz 5

In Absatz 5 wird von der durch das Bundesverfassungsgericht eingeräumte Delegationsbefugnis (siehe Urteil, a. a. O., Rz. 190) Gebrauch gemacht und das Sächsische Staatsministerium des Innern verpflichtet, durch mit der oder dem Sächsischen Datenschutz- und Transparenzbeauftragten abzustimmenden Verwaltungsvorschrift Näheres, insbesondere zu von der vorsorgenden Speicherung ausgenommenen personenbezogenen Daten (beispielsweise „Bagatellstraftaten“), zu den Anforderungen an die erforderliche Prognoseprüfung der vorsorgenden Speicherung und die Bestimmung und Verlängerung von Aussonderungsprüffristen im Einzelfall, die Löschungsverpflichtungen und insbesondere an die Dokumentationspflichten zu den Entscheidungen gemäß den §§ 80 bis 80c, § 80d und § 91 zu bestimmen und schließlich an die technisch und organisatorischen Vorkehrungen zur Einhaltung der bezeichneten Anforderungen.

Zu Nummer 27

§ 81

Zu Buchstabe a

Die Änderung dient der Korrektur eines redaktionellen Versehens.

Zu Buchstabe b

Gemäß § 108 Absatz 4 Satz 2 ist die Regelung des § 81 Absatz 4 Satz 2 am 31. Dezember 2025 außer Kraft getreten. In Konsequenz des Außerkrafttretens wird die Regelung gestrichen.

Zu Nummer 28

§ 83

Die Änderungen dienen der Korrektur eines redaktionellen Versehens.

§ 84

Absatz 2

Nummer d

Zweck der ergänzenden Regelung ist es, eine Datenübermittlungsbefugnis in das Sächsische Polizeivollzugsdienstgesetz aufzunehmen, die es der Polizei erlaubt, personenbezogene Daten an eine öffentliche Stelle zu übermitteln, die keine Gefahrenabwehrbehörde ist. Die Befugnisregelung setzt ein Datenübermittlungsersuchen der betreffenden öffentlichen Stelle voraus, ferner, dass die Zulässigkeit des Datenübermittlungsersuchens der öffentlichen Stelle, die um Datenübermittlung ersucht, bereichsspezifisch geregelt ist und dass die Datenübermittlung für die Aufgabenerfüllung der jeweiligen öffentlichen Stelle erforderlich ist. Für die neue Regelung besteht erheblicher praktischer Bedarf. Anwendungsfälle sind Datenübermittlungsersuchen der Finanzbehörden oder der Gerichtsvollzieher im Zusammenhang mit erforderlichen Vollstreckungstätigkeiten. Polizeiliche Erkenntnisse zu möglichen, von betroffenen Personen für die Bediensteten ausgehende Gefahren, können zum Zweck der Aufgabenerfüllung erforderlich sein. Mit der Ergänzung wird eine bestehende Regelungslücke unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts zur Ausgestaltung von Datenübermittlungsregelungen (sog. „Doppeltür-Entscheidung“ des BVerfG, Beschluss vom 27. Mai 2020, 1 BvR 1873/13, 1 BvR 2618/13, Bestandsdatenauskunft II, Rz. 130) geschlossen.

Absatz 3

Die Änderungen in Satz 1 stellen redaktionelle Folgeänderung dar.

Mit der Ergänzung unter Nummer 4 und in Satz 2 wird zum Zweck der Bekämpfung häuslicher Gewalt eine Befugnisregelung aufgenommen, die es der Polizei erlaubt, die Kontaktdaten von Personen, die häuslicher Gewalt ausgesetzt sind, an geeignete Beratungsstellen nichtbehördlicher Organisationen zu übermitteln. Häusliche Gewalt in diesem Sinne beinhaltet alle Formen körperlicher, sexuelle oder psychischer Gewalt und umfasst familiäre sowie partnerschaftliche Gewalt. Häusliche Gewalt liegt vor, wenn die Gewalt zwischen Personen stattfindet, die in einer familiären oder partnerschaftlichen Beziehung zusammenwohnen. Sie liegt auch vor, wenn sie unabhängig von einem gemeinsamen Haushalt innerhalb der Familie oder in aktuellen oder ehemaligen Partnerschaften geschieht (siehe die Definition im Bundeslagebild des Bundeskriminalamts zu häuslicher Gewalt 2023, S. 1). Durch die Regelung soll proaktiv eine Kontaktaufnahme mit der betroffenen Person zum Zweck der Beratung ermöglicht werden. Die Eignung der Beratungsstellen ist durch das Sächsische Staatsministerium für Soziales, Gesundheit und Gesellschaftlichen Zusammenhalt zu bestimmen. Ziel der Regelungen in den Sätzen 2 und 3 ist es, die datenschutzrechtlichen Interessen der betroffenen Person zu wahren.

Absatz 5

Die Änderung stellt eine redaktionelle Folgeänderung dar.

§ 84a

Mit der Regelung wird eine Rechtsgrundlage für eine öffentliche Fahndung nach Personen zum Zweck der Ermittlung der Identität der Person oder des Aufenthaltsorts der Person zur Abwehr von Gefahren für die betreffende Person (Nummer 1) oder von der betroffenen Person (Nummer 2) in das Sächsische Polizeivollzugsdienstgesetz aufgenommen und damit eine bestehende Regelungslücke geschlossen.

Zu Nummer 29

§ 86

Die geltende Vorschrift bezieht sich begrifflich allein auf die Aufzeichnung von Anrufen im Notfall. Sie deckt nicht den polizeifachlichen Bedarf ab, andere Kommunikation (beispielsweise über eine Notruf-App) und den Standort des Anrufers bei Anwahl der Notrufnummer 110 zu erheben. Gemäß § 164 Absatz 1 des Telekommunikationsgesetzes (TKG) vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 35 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, sind Notrufverbindungen jederzeit unverzüglich zu der örtlich zuständigen Notrufabfragestelle herzustellen. Nach § 2 Nummer 2 der Verordnung über Notrufverbindungen (NotrufV) vom 6. März 2009 (BGBl. I S. 481), die zuletzt durch Artikel 34 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, ist „Notrufabfragestelle“ die nach Landesrecht zuständige Stelle zur Entgegennahme von Notrufen. Gemäß § 164 Absatz 3 TKG ist hierbei zu berücksichtigen, dass bei Gewährleistung einer gleichwertigen Notrufkommunikation von Menschen mit Behinderungen im Rahmen von Notrufverbindungen von der Polizei zukünftig nicht nur Sprache, sondern auch Text und gegebenenfalls Video im Rahmen der Notrufkommunikation zu verarbeiten sind.

Absatz 1

Mit dem neuen Absatz 1 wird eine Rechtsgrundlage für den Abruf von Standortdaten geschaffen, die nach Anwahl der Notrufnummer 110 mittels eines Smartphones automatisiert und ohne Interaktion der anrufenden Person anfallen. Mit der Formulierung „einschließlich der den Notruf begleitenden personenbezogenen Daten“ wird geregelt, dass die gesamte Kommunikation (Chatverläufe bei Notruf-App) verarbeitet werden darf, soweit dies für die Abwehr von Gefahren oder für die Verhütung von Straftaten erforderlich ist.

Absatz 2

Die Regelung entspricht der Bisherigen in § 86 Absatz 1 Satz 2.

Absatz 3

Die Regelung in Satz 1 entspricht der Bisherigen in § 86 Absatz 1 Satz 3 mit der Änderung, dass aus Gründen der Verhältnismäßigkeit die Höchstspeicherfrist auf einen Monat gekürzt wurde. Mit Satz 2 (neu) wird klargestellt, dass Aufzeichnungen auch zu Zwecken der Aus- und Fortbildung genutzt werden dürfen.

Zu Nummer 30

§ 88

Die UEFA EURO 2024 hat gezeigt, dass ein polizeifachlicher Bedarf besteht, neben der Einbeziehung von bestehenden polizeilichen Datenbeständen (polizeilicher Informationsverbund) weitere Datenbestände bei der Durchführung von Zuverlässigkeitsüberprüfungen zu berücksichtigen. Erforderlich ist es, den aktuellen Datenbestand der Wohnsitz-Landeskriminalämter der letzten fünf Jahre einzubeziehen, aber auch Daten des Ausländerzentralregisters, des Landesamtes für Verfassungsschutz oder bei Personen mit Wohnsitz im Ausland, Daten der Polizeibehörden des jeweiligen Staates. Aufgrund zunehmender Digitalisierung besteht zudem Bedarf, Zuverlässigkeitsüberprüfungen im elektronische Verfahren zu ermöglichen. Das Verfahren der Zuverlässigkeitsüberprüfung bedingt eine Vielzahl von Datenverarbeitungsschritten, ohne dass dies der bestehenden Vorschrift klar entnommen werden konnte. Durch die neue Regelung sollen die erforderlichen Datenverarbeitungsregelungen umfassend geregelt werden. Es besteht zudem der polizeifachliche Bedarf, zum Zweck der Zuverlässigkeitsüberprüfung im elektronischen Verfahren die Identität der betroffenen Person zu überprüfen und Kopien des Personalausweises zum Vorgang zu nehmen.

Absatz 1

Die Regelung beinhaltet die Voraussetzungen, unter denen eine Zuverlässigkeitsüberprüfung erfolgen kann. Neben dem Erfordernis eines Ersuchens einer öffentlichen oder nichtöffentlichen Stelle muss es sich bei der Veranstaltung um eine besonders gefährdete Veranstaltung handeln und die zu überprüfende Person muss einen privilegierten Zutritt zu der Veranstaltung haben. Durch die Anforderung des „privilegierten Zutritts“ soll sichergestellt werden, dass nur solche Personen überprüft werden, die aufgrund ihrer tatsächlichen „Nähe“ zu der Veranstaltung ein potentielles Sicherheitsrisiko für die Veranstaltung bilden können.

Absatz 2

Satz 1 bestimmt die verfahrensrechtlichen Anforderungen an die Zuverlässigkeitsüberprüfung.

Satz 2 regelt die Anforderungen an die Datenschutzinformation der betroffenen Person, die vor der Zustimmungserteilung zu erfolgen hat.

Absatz 3

Die Regelung bestimmt, welche Datenbestände bei der Durchführung von Zuverlässigkeitsüberprüfungen einbezogen werden dürfen.

Absatz 4

Satz 1 beinhaltet die Rechtsgrundlage für die Datenübermittlung der Polizei an andere öffentliche Stellen zum Zweck der Datenerhebung. Satz 2 regelt die enge Zweckbindung für die durch die Polizei bei anderen öffentlichen Stellen erhobenen Daten. Die Sätze 3 und 4 beinhalten die Rechtsgrundlage für die Übermittlung des Ergebnisses der Zuverlässigkeitsüberprüfung an die ersuchende öffentliche oder private Stelle. Satz 5 enthält die Verpflichtung zur Unterrichtung der betroffenen Person über das Ergebnis der Überprüfung.

Absatz 5

Die Regelung übernimmt zur Sicherstellung der Einhaltung der Zweckbestimmung der Datenverarbeitung bei der privaten oder öffentlichen Stelle den Regelungsinhalt aus § 88 Absatz 2.

Absatz 6

Die Regelung bestimmt eine Höchstspeicherfrist von sechs Monaten für die im Rahmen der Zuverlässigkeitsüberprüfung verarbeiteten personenbezogene Daten. Satz 2 beinhaltet die Regelung zum Beginn des Fristlaufs.

Absatz 7

In Absatz 7 wird die Regelung aus § 88 Absatz 2 zur Unterrichtung der Sächsischen Datenschutz- und Transparenzbeauftragten übernommen.

Zu Nummer 31

§ 91

Absatz 2

Zweck der Neufassung ist es, durch die Aufzählung der Löschungstatbestände eine anwenderfreundliche Regelung zu gestalten, insbesondere aber die Datenschutzrechte der betroffenen Personen zu gewährleisten. Die klarstellenden Löschungstatbestände unter den Nummern 3 bis 7 (neu) wurden zur Gewährleistung der Anwenderfreundlichkeit aufgenommen.

Die Änderungen der Absätze 3 und 4 stellen redaktionelle Folgeänderungen dar.

Zu Nummer 32

§ 93

Die Änderungen in Absatz 1 Nummer 10 erfolgen zur Behebung eines redaktionellen Versehens.

Zu Nummer 33

§ 94

Mit den Änderungen und Ergänzungen werden die Kontrollpflichten der oder des Sächsischen Datenschutz- und Transparenzbeauftragten erweitert. Neu aufgenommen wurden die Befugnisse nach § 57a Absatz 1 Satz 4 und Absatz 2, § 58 (verdeckter Einsatz der automatisierten Kennzeichenerkennung), § 62a, § 62b und die Quellen-TKÜ durch die allgemeine Verweisung auf § 66.

Zu Nummer 34

§ 97

Die Bezeichnung „Polizeiverwaltungsamt“ in Absatz 1 Nummer 3 wird durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Der aktuelle Name „Polizeiverwaltungsamt“ spiegelt die Vielfältigkeit seiner Aufgaben sowie den Anspruch von Moderne und Innovation nicht mehr wider. Das Voranschreiten der Digitalisierung und das damit verbundene Erfordernis, die Zukunftsfähigkeit der Polizei Sachsen sicherzustellen, setzt auch die Gewinnung und Bindung von geeignetem Personal in Konkurrenz mit der freien Wirtschaft oder anderen öffentlichen Arbeitgebern voraus.

Zu Nummer 35

§ 101

Die Bezeichnung „Polizeiverwaltungsamt“ in Absatz 1 wird durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Der aktuelle Name „Polizeiverwaltungsamt“ spiegelt die Vielfältigkeit seiner Aufgaben sowie den Anspruch von Moderne und Innovation nicht mehr wider. Das Voranschreiten der Digitalisierung und das damit verbundene Erfordernis, die Zukunftsfähigkeit der Polizei Sachsen sicherzustellen, setzt auch die Gewinnung und Bindung von geeignetem Personal in Konkurrenz mit der freien Wirtschaft oder anderen öffentlichen Arbeitgebern voraus.

Zu Nummer 36

§ 106

Die Änderungen stellen Folgeanpassungen in Hinblick auf die geänderten Vorschriften § 21 und § 61 dar.

Zu Nummer 37

§ 106a

Absatz 1

Mit der Aufnahme der Regelung werden Ordnungswidrigkeitentatbestände im Hinblick auf das Zuwiderhandeln gegen vollziehbare Maßnahmen nach den §§ 18, 19, 20, 21 Absatz 1 bestimmt. Im Sächsischen Polizeibehördengesetz besteht eine entsprechende Regelung in § 31.

Absatz 2

Die Regelung bestimmt die Höhe der Geldbuße.

Absatz 3

Die Regelung bestimmt gemäß § 36 Absatz 1 Nummer 1 Ordnungswidrigkeitengesetz, dass die zuständige Verwaltungsbehörde die Polizeidienststelle ist, die die Anordnung getroffen hat.

Zu Nummer 38

§ 107

Die Änderungen und Ergänzungen in Satz 1 erfolgen in Konsequenz von Änderungen bestehender berichtspflichtiger Befugnisregelungen (Änderungen bei § 21, § 59 außer Kraft getreten) und im Hinblick auf in das Sächsische Polizeivollzugsdienstgesetz neu aufgenommener Befugnisregelungen, für die im Hinblick auf die hiermit verbundenen erheblichen Eingriffe in Grundrechte eine Berichtspflicht gegenüber der Öffentlichkeit sowie dem Land-

tag besteht. Von der Berichtspflicht nunmehr umfasst ist der Einsatz von Bodycam in Wohnungen nach § 57 Absatz 4 Satz 2 und Absatz 5 Satz 2. Ebenfalls in die Berichtspflicht aufgenommen wurden die neu aufgenommen Befugnisregelungen gemäß § 57a Absatz 1 Satz 4 und Absatz 2, die in § 60 neu aufgenommene Befugnis zur Ausschreibung zur Ermittlungsanfrage, die Befugnis nach § 62b (biometrischer Abgleich mit Daten aus dem Internet) und § 66 Absatz 2 (Quellen-TKÜ). Die vorgesehenen Änderungen und Ergänzungen tragen den Anforderungen des Bundesverfassungsgerichts an die gesetzgeberische Ausgestaltung von Berichtspflichten zur Gewährung von Transparenz und Kontrolle von heimlichen Befugnisregelungen Rechnung (Urteil BVerfG 2016, 1 BvR 966/09, Rz. 142).

Zu Nummer 39

§ 108

Aufgrund des Fristablaufs zum 31. Dezember 2023 sind die durch die Regelung befristet geltenden Vorschriften § 59 und § 81 Absatz 3 Satz 2 außer Kraft getreten.

Befristungen wurden zudem für die Regelung der Ausweitung des Einsatzes von Distanz-Elektroimpulsgeräten auf Polizeibedienstete, deren Einsatz nicht innerhalb einer Spezialeinheit erfolgt (§ 40 Absatz 4 Satz 2) und für die Regelung der Ausweitung des Einsatzes von Bodycam auf Wohnungen (§ 57 Absatz 4 Satz 2 und Absatz 5 Satz 2) aufgenommen.

In Konsequenz der Vereinbarung im Koalitionsvertrag wird die Vorschrift zur Quellen-TKÜ in § 66 Absatz 2, 2a und 3 bis zum 31. Dezember 2031 befristet. Die vorgesehene Fristsetzung für das Außerkrafttreten bietet einen ausreichenden Zeitrahmen für ein gegebenenfalls erforderliches Tätigwerden des Gesetzgebers.

Zu Artikel 2 (Änderung des Sächsischen Polizeibehördengesetzes)

Zu Nummer 1

§ 23 Absatz 2

Mit der Änderung in Satz 1 durch den Verweis auf § 104 Absatz 3 der Strafprozessordnung wird (analog zur Änderung des § 29 Absatz 3 SächsPVDG) der Beschluss des Bundesverfassungsgerichts vom 29. März 2019, 2 BvR 675/14, Rz. 66 umgesetzt und geregelt, dass die Nachtzeit ganzjährig die Zeit zwischen 21.00 Uhr und 6 Uhr erfasst. Infolge der Aufnahme der Verweisung ist Satz 3 zu streichen.

Zu Nummer 2

§ 30 Absatz 1

Mit den Änderungen werden die Vorgaben des Sächsischen Verfassungsgerichtshofs durch Urteil vom 25. Januar 2024, Vf. 91-II-19, umgesetzt. Das Gericht bemängelte hinsichtlich des bisherigen § 30 Absatz 1 Nummer 2 SächsPBG, dass diese Regelung keine hinreichend bestimmten und klaren Vorgaben bezüglich des Anlasses, des Zwecks und der Grenzen der Maßnahme enthalte. Es fehle außerdem an einem inneren Zusammenhang zwischen den erwarteten Gefahren für die geschützten Objekte und einer auf tatsächlichen Anhaltspunkten basierenden besonderen Gefährdungslage als Voraussetzung für die Videoüberwachung.

In Umsetzung der Entscheidung wurde – auch unter Praxisgesichtspunkten – der bisherige Regelungsinhalt der Nummer 2 in Nummer 1 neu und der bisherige der Nummer 1 in Nummer 2 neu übernommen und angepasst. Voraussetzung für die Videoüberwachung nach beiden Befugnisregelungen ist nunmehr jeweils das Vorliegen einer tatsachenbasierten Gefahrenlage. Die Videoüberwachung nach dieser Vorschrift knüpft sowohl in Nummer 1 als

auch in Nummer 2 an die gemeindliche Aufgabe der Gefahrenabwehr der Ortspolizeibehörden an.

Die Rechtsgrundlagen der behördlichen Videoüberwachung gemäß Nummer 1 und der nach § 13 Absatz 1 2. Alt. Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) (Hausrecht) haben unterschiedliche Zielrichtungen und überlappen sich nicht. Während die Videoüberwachung gemäß Nummer 1 dem Vollzug der gemeindlichen Aufgabe der Gefahrenabwehr als Ortspolizeibehörde dient, knüpft die Videoüberwachung gemäß § 13 Absatz 1 2. Alt. SächsDSDG demgegenüber allein an das Hausrecht an den eigenen Gebäuden an. Beide Regelungen stehen parallel nebeneinander, so dass auch im Hinblick auf die unterschiedlichen Zielrichtungen und Voraussetzungen keine Sperrwirkung besteht.

Nummer 1

Mit der Änderung des Wortlauts der Regelung wird nunmehr klar bestimmt, welche gefährdeten Objekte unter welchen Voraussetzungen zu welchem Zweck videoüberwacht werden dürfen.

In Nummer 1 werden die Anlagen und Einrichtungen, zu deren Schutz die Videoüberwachung erfolgen kann, wie folgt konkret bezeichnet: öffentliche Einrichtungen, öffentliche Verkehrsmittel, Kulturgüter, Dienstgebäuden oder sonstige baulichen Anlagen öffentlicher Stellen.

Mit dem Begriff der „öffentlichen Einrichtung“ wird auf den im Kommunalrecht verwandten Begriff Bezug genommen. Unter einer öffentlichen Einrichtung wird allgemein eine Einrichtung der Gemeinde verstanden, die im öffentlichen Interesse unterhalten wird und durch einen gemeindlichen Widmungsakt der allgemeinen Benutzung durch Gemeindeangehörige sowie ortsansässige Vereinigungen zugänglich gemacht wird. Dem Begriff der öffentlichen Einrichtung unterfallen z.B. Rathäuser, Museen, Sportplätze, öffentliche Schwimmbäder, Kanalisation, Wertstoffhöfe, etc.

Dem Begriff „Öffentliche Verkehrsmittel“ unterfallen alle Transportmittel, die in den öffentlichen Personennahverkehr eingebunden sind und der öffentlichen Personenbeförderung dienen. Hierzu zählen alle zugelassenen Luft-, Land- und Wasserfahrzeuge.

„Kulturgüter“ sind beispielsweise historische Brunnenanlagen, archäologische Stätten, Skulpturen oder unter Denkmalschutz stehende Ruinen.

Voraussetzung für die Videoüberwachung der genannten Objekte ist, dass Tatsachen die Annahme rechtfertigen, dass im unmittelbaren Umfeld der genannten gefährdeten Objekte künftig Straftaten oder Ordnungswidrigkeiten begangen werden, durch die Personen oder bedeutende Sach-oder Vermögenswerte gefährdet werden. Die Regelung setzt somit das Vorliegen einer entsprechenden Tatsachenbasis voraus, die geeignet ist, die Prognose künftiger Gefahren für die Rechtsgüter von Leib oder Leben oder bedeutende Sach- oder Vermögenswerte zu begründen. Hierfür bedarf es eines Lagebildes, dem Erkenntnisse zu künftigen Straftaten und Ordnungswidrigkeiten im Hinblick auf die Rechtsgüter „Leib“ oder „bedeutende Sach- oder Vermögenswerte“ entnommen werden können.

Nummer 2

Die bisherige Regelung in § 30 Absatz 1 Nummer 1 SächsPBG wurde mit Änderungen in die Nummer 2 überführt.

Unter dem Begriff „öffentlich zugänglichen Bereiche“ sind in Übereinstimmung mit den Begrifflichkeiten in § 57 Bereiche zu verstehen, die zur öffentlichen Nutzung bestimmt sind. Ein solcher öffentlich zugänglicher Bereich kann innerhalb oder außerhalb eines Gebäudes liegen und ist nicht an das Vorhandensein eines Gebäudes geknüpft. Die Zweckbestimmung folgt aus einer entsprechenden förmlichen Widmung durch den Berechtigten oder

dadurch, dass dieser in anderer Weise seinen Willen deutlich macht, dass eine solche öffentliche Zugänglichkeit bestehen soll. Beispielsweise fallen dem allgemeinen Verkehr förmlich gewidmete öffentliche Straßen, Wege und Plätze unter diesen Begriff. Entscheidend ist die durch den Berechtigten eröffnete tatsächliche Nutzungsmöglichkeit durch die Allgemeinheit.

Voraussetzung für eine Videoüberwachung nach Nummer 2 ist eine tatsachenbasierte Gefahrenlage, die die Annahme rechtfertigt, dass dort erhebliche Gefahren für die öffentliche Sicherheit entstehen.

Die Klarstellung der Erforderlichkeit der Maßnahme durch die Regelung im 2. Halbsatz soll verdeutlichen, dass die Videoüberwachung auch in räumlicher oder zeitlicher Hinsicht zur Gefahrenabwehr erforderlich sein muss.

Zu Nummer 3

§ 40 Absatz 1

Mit den Änderungen und Ergänzungen erfolgen die erforderlichen Anpassungen an die Änderungen der datenschutzrechtlichen Bestimmungen des Sächsischen Polizeivollzugsdienstgesetzes. Der bisherige Regelungsinhalt von § 80 Absatz 1 und 7 wurde in § 79 Absatz 1 und 2 und der bisherige Regelungsinhalt von § 79 wurde in § 79a übernommen. Vor dem Hintergrund der Ergänzung von § 84 Absatz 3 um die Befugnisregelung zur Datenübermittlung an nichtöffentliche Stellen im Kontext von „häuslicher Gewalt“ (Nummer 4 neu) bestand das Erfordernis, diese Befugnisregelung von der Anwendbarkeit auszuschließen, da diese Aufgabe dem Polizeivollzugsdienst obliegt.

Zu Nummer 4

§ 42

Mit der Änderung in Satz 1 erfolgt die Korrektur eines redaktionellen Versehens analog zu der Änderung in § 48 Absatz 3 Satz 1 SächsPVDG.

Zu Artikel 3 (Änderung des Sächsischen Kontrollgesetzes)

Die Streichung von § 59 folgt in Konsequenz des Außerkrafttretens der Regelung durch Zeitablauf zum 31. Dezember 2023 (siehe bisherige Regelung in § 108 Absatz 1). Mit den Änderungen wird die Kontrollbefugnis des Parlamentarischen Kontrollgremiums auf die neuen eingriffsintensiven und heimlichen Befugnisse gemäß § 60 Absatz 1 (Ausschreibung zur gezielten Befragung) und § 66 Absatz 2 (Quellen-TKÜ) erweitert.

Zusammen mit der Erweiterung der Berichtspflichten an die Sächsische Datenschutz- und Transparenzbeauftragte in § 94 und an die Öffentlichkeit und das Parlament in § 107 wird den Anforderungen des Bundesverfassungsgerichts im Urteil vom 20. April 2016, 1 BvR 966/09, Rz. 141 und 142 nachgekommen und sowohl eine effektive aufsichtliche Kontrolle als auch die erforderliche Transparenz polizeilichen Handelns gewährleistet.

Zu Artikel 4 (Änderung des Sächsischen Gesetzes zur Regelung polizeilicher Zuverlässigkeitsüberprüfungen)

§ 4 Satz 3 Nummer 4

Ziel der Änderung ist die Parallelgestaltung der Regelung zur Anfrage bei den zuständigen Polizeien analog zu der Regelung in § 88. Durch die Prüfstellen der Polizei wird darauf hingewiesen, dass insbesondere ein erheblicher Teil der eingesetzten Handwerker ausländische Personen sind, die teils einen festen Wohnsitz in Deutschland haben, teils aber auch

nicht. Diese Situation birgt aus Sicht der Prüfstellen eine erhebliche Sicherheitslücke. Insbesondere angesichts der sich zuspitzenden weltweiten Konflikte wird die Gefahr gesehen, dass sächsische Polizeidienststellen aufgrund der fehlenden Informationsgewinnung Opfer von Straftaten werden könnten.

Zu Artikel 5 (Folgeänderung im Sächsischen Besoldungsgesetz)

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in der Anlage 2 (zu § 24 Absatz 1) durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 6 (Folgeänderung im Sächsischen Verwaltungsorganisationsgesetz)

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 8 Absatz 1 Nummer 4 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 7 (Folgeänderung im Sächsischen Personalvertretungsgesetz)

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 68 Absatz 1 Nummer 4 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 8 (Folgeänderungen im Sächsischen Straßenverkehrsrechtsgesetz)

Zu Nummer 1

§ 14

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 14 Absatz 1 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Nummer 2

§ 18

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 18 Absatz 2 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 9 (Folgeänderungen in der Sächsischen Polizeiorganisationsverordnung)

Zu Nummer 1

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in der Inhaltsübersicht zu § 4, § 1 Absatz 1, § 4 Absatz 1, § 4 Absatz 2, § 4 Absatz 3 Satz 1 und 2 und § 4 Absatz 4 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Nummer 2

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in der Inhaltsübersicht zu § 4, § 1 Absatz 1, § 4 Absatz 1, § 4 Absatz 2, § 4 Absatz 3 Satz 1 und 2 und § 4 Absatz 4 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 10 (Folgeänderung in der Sächsischen Waffengesetzdurchführungsverordnung)

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 2 Absatz 1 Nummer 2 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG

Zu Artikel 11 (Folgeänderung in der Sächsischen Vertretungsordnung)

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 6 Absatz 3 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 12 (Folgeänderung in der Sächsischen Heilfürsorgeverordnung)

Zu Nummer 1

§ 2 Absatz 7

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 2 Absatz 7 Satz 2 durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Nummer 2

§ 30

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 30 jeweils durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 13 (Folgeänderungen in der Sächsischen Straßenverkehrsrechtsverordnung)

Zu Nummer 1

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 5 jeweils durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Nummer 2

Mit den Änderungen in den betreffenden Gesetzen und Verordnungen wird die Bezeichnung „Polizeiverwaltungsamt“ in § 9 Absatz 2 Satz 2 jeweils durch die Bezeichnung „Polizeipräsidium für Service und IT“ ersetzt. Siehe Begründung Artikel 1, zu § 97 SächsPVDG.

Zu Artikel 14 (Inkrafttreten)

Die Regelung enthält die Bestimmung zum Inkrafttreten dieses Mantelgesetzes.