

Gesetz zur Änderung polizeirechtlicher Vorschriften

Vom 24. Juni 2026

Der Sächsische Landtag hat am 24. Juni 2026 das folgende Gesetz beschlossen:

Inhaltsübersicht

- Artikel 1 Änderung des Sächsischen Polizeivollzugsdienstgesetzes
- Artikel 2 Weitere Änderung des Sächsischen Polizeivollzugsdienstgesetzes
- Artikel 3 Änderung des Sächsischen Polizeibehördengesetzes
- Artikel 4 Einschränkung von Grundrechten
- Artikel 5 Änderung des Sächsischen Kontrollgesetzes
- Artikel 6 Änderung des Sächsischen Gesetzes zur Regelung polizeilicher Zuverlässigkeitsüberprüfungen
- Artikel 7 Folgeänderung im Sächsischen Besoldungsgesetz
- Artikel 8 Folgeänderung im Sächsischen Verwaltungsorganisationsgesetz
- Artikel 9 Folgeänderung im Sächsischen Personalvertretungsgesetz
- Artikel 10 Folgeänderungen im Sächsischen Straßenverkehrsrechtsgesetz
- Artikel 11 Folgeänderungen in der Sächsischen Polizeiorganisationsverordnung
- Artikel 12 Folgeänderung in der Sächsischen Waffengesetzdurchführungsverordnung
- Artikel 13 Folgeänderung in der Sächsischen Vertretungsverordnung
- Artikel 14 Folgeänderungen in der Sächsischen Heilfürsorgeverordnung
- Artikel 15 Folgeänderungen in der Sächsischen Straßenverkehrsrechtsverordnung
- Artikel 16 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 die 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 die folgende Angabe eingefügt:

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

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 Anlassbezogener besonderer automatisierter Datenabgleich und anlassbezogene automatisierte Datenanalyse, Verordnungsermächtigung

§ 62b Anlassbezogene nachträgliche Fernidentifizierung“.

h) Nach der Angabe zu § 66 wird die folgende Angabe eingefügt:

„§ 66a Unterbrechung oder Verhinderung der Telekommunikation“.

i) Die Angabe zu § 69 wird durch die folgende Angabe ersetzt:

„§ 69 (weggefallen)“.

j) Die Angabe zu § 71 wird durch die folgende Angabe ersetzt:

„§ 71 Einsatz von unbemannten Luftfahrtsystemen“.

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

„§ 72 (weggefallen)“.

l) Die Angabe zu § 79 wird durch die folgende Angabe ersetzt:

„§ 79 Befugnis zur Datenverarbeitung“.

m) Nach der Angabe zu § 79 wird die folgende Angabe eingefügt:

„§ 79a Zweckbindung, Zweckänderung, Hypothetische Datenneuerhebung

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

§ 79c Entwicklung, Training und Testen von regelbasierten und lernenden IT-Systemen“.

n) Die Angabe zu § 80 wird durch die folgende Angabe ersetzt:

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

o) 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“.

p) Nach der Angabe zu § 84 wird die folgende Angabe eingefügt:

„§ 84a Öffentlichkeitsfahndung“.

q) Die Angabe zu § 88 wird durch die folgende Angabe ersetzt:

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

r) Nach der Angabe zu § 88 wird die folgende Angabe eingefügt:

„§ 89a Datenübermittlung und -bereitstellung an Mitgliedstaaten der Europäischen Union und Schengen-assoziierte Staaten gemäß der Richtlinie (EU) 2023/977“.

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

„§ 106a Ordnungswidrigkeiten“.

t) Die Angabe zu § 108 wird gestrichen.

2. § 3 wird durch den 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 unverzüglichen 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 die folgenden Nummern 5 bis 7 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. 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;

7. 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. § 10 Nummer 6 und 7 wird durch die folgenden Nummern 6 bis 8 ersetzt:

„6.Unverletzlichkeit der Wohnung (Artikel 13 Absatz 1 des Grundgesetzes für die Bundesrepublik Deutschland, Artikel 30 Absatz 1 der Verfassung des Freistaates Sachsen),

7. informationelle Selbstbestimmung (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes für die Bundesrepublik Deutschland, Artikel 33 der Verfassung des Freistaates Sachsen) und

8. Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes für die Bundesrepublik Deutschland, Artikel 33 der Verfassung des Freistaates Sachsen)“.

5. 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 oder dessen Steuerungseinheit oder Steuerungsverbindung einsetzen, soweit die Abwehr der Gefahr auf andere Weise aussichtslos ist oder wesentlich erschwert wäre. Für Maßnahmen nach Satz 1 kann die Polizei technische Mittel zur Gefahrenerforschung einsetzen, soweit Anhaltspunkte die Möglichkeit einer Gefahr begründen. Maßnahmen nach Satz 1 dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.“

6. § 15 Absatz 1 Satz 1 Nummer 5 bis 8 wird durch die folgenden Nummern 5 bis 9 ersetzt:

„5.wenn sie sich in einem Fahrzeug befindet, das zur gezielten Kontrolle ausgeschrieben ist und tatsächliche Anhaltspunkte 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 oder Straftaten gemäß § 24 Absatz 1 Nummer 3 oder 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, und wenn Tatsachen die Annahme rechtfertigen, dass dort Straftaten dieser Art bevorstehen; die Bestimmung eines Kontrollbereichs darf höchstens 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.“

7. § 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, Gesundheit, 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 oder

d) ein Zusammentreffen mit der gefährdeten Person herbeizuführen.

Die Anordnungen sind zu befristen; die Frist kann einmalig verlängert werden. Maßnahmen nach Satz 1 enden spätestens mit dem Ablauf des 30. 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. Tages 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.“

8. § 21 wird durch den folgenden § 21 ersetzt:

„§ 21

Aufenthaltsanordnung und Kontaktverbot

(1) Die Polizei kann zum Zweck der Verhütung von Straftaten einer Person für höchstens drei Monate 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 Straftat handelt, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen erfasst, ist die Maßnahme nur zulässig, wenn im jeweiligen Einzelfall bestimmte Tatsachen die Prognose eines Geschehens begründen, dass für ein bedeutendes Individual- oder Kollektivrechtsgut im Sinne der jeweiligen Strafnorm die zurechenbare Gefahr der Verletzung besteht. 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 schriftlichen 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) In dem schriftlichen 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 von der Staatsregierung geprüft. Die Staatsregierung berichtet dem Landtag über das Ergebnis der Evaluierung.“

9. § 28 Nummer 6 und 7 wird durch die folgenden 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“.

10§ 29 Absatz 3 wird durch den 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.“

11§ 41 wird wie folgt geändert:

a) Absatz 1 Satz 3 wird durch den 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.“

b) Absatz 2 wird durch den folgenden Absatz 2 ersetzt:

„(2) Unmittelbarer Zwang ist vor seiner Anwendung anzudrohen und die Maßnahme einschließlich deren Androhung ist über ein körpernah getragenes Aufzeichnungsgerät im Sinne des § 57 Absatz 4 zu erfassen, falls ein solches mitgeführt wird. Erfolgt die Anwendung innerhalb einer Wohnung, ist eine Aufzeichnung nur zur Verhütung einer dringenden Gefahr für Leib oder Leben der eigenen oder einer dritten Person zulässig. § 57 Absatz 6 bis 9 gilt mit Ausnahme von Absatz 8 Satz 6 bis 8 entsprechend. Von der Androhung nach Satz 1 kann abgesehen werden, wenn die Umstände sie nicht zulassen, insbesondere wenn die sofortige Anwendung des Zwangsmittels zur Abwehr einer gegenwärtigen Gefahr notwendig ist. Als Androhung des Schusswaffengebrauchs gilt auch die Abgabe eines Warnschusses.“

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

13Die §§ 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 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. Der Einsatz ist nur zulässig, sofern damit nicht die Überwachung der Wohnung verbunden ist. In Wohnungen ist eine Maßnahme nach Satz 1 nur zulässig, wenn dies 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 Arbeits-, Geschäfts- oder Aufenthaltszeit. Nach den Sätzen 1 und 2 erlangte Daten sind automatisiert nach 60 Sekunden zu löschen, soweit die Voraussetzungen für eine Speicherung nach Absatz 5 nicht vorliegen.

(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 die in Absatz 4 Satz 2 genannten Voraussetzungen vorliegen.

(6) In Bereichen, die der Ausübung von Tätigkeiten von Berufsheimlichkeitsgeheimnisträgern 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 tatsächliche Anhaltspunkte dafür, dass der Kernbereich privater Lebensgestaltung betroffen ist, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung der eigenen oder dritten Person für Leib oder Leben möglich ist. Unterbleibt eine Unterbrechung aufgrund einer Gefährdung nach Satz 2, sind die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und die Umstände des Fortsetzens der Maßnahme zu dokumentieren. Die Maßnahme darf fortgeführt werden, wenn 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 und ist nach einem Jahr zu löschen.

(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 Rechtmäßigkeit 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 30 Tagen 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 und keine Inhalte erfasst wurden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. § 79a Absatz 4 Satz 1 gilt entsprechend. 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) Maßnahmen nach den Absätzen 2 bis 5 dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(10) 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 von der Staatsregierung geprüft. Die Staatsregierung berichtet dem Landtag über das Ergebnis der Evaluierung. Befugnisse nach Absatz 4 Satz 2 und Absatz 5 Satz 2 treten mit Ablauf des 31. März 2031 außer Kraft, sofern nicht der Landtag etwas anderes beschließt.

(11) Nach den Absätzen 2 und 3 erhobene Daten und daraus gefertigte Unterlagen sind spätestens nach 30 Tagen 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, Verordnungsermächtigung

(1) Die Polizei kann bei Maßnahmen nach § 57 Absatz 2 und 3 in Echtzeit 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 zu rechnen ist. 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 unerlässlich ist.

(2) Die Polizei kann durch Maßnahmen nach § 57 Absatz 2 und 3 in öffentlich zugänglichen Bereichen erhobene personenbezogene Daten anhand des Datenbestandes der polizeilichen Auskunfts- und Fahndungssysteme zu Zwecken der biometrischen Echtzeit-Fernidentifizierung verarbeiten, sofern dies unerlässlich ist

1. zur Abwehr einer Gefahr, weil Tatsachen die Annahme rechtfertigen, dass eine Person eine terroristische Straftat begehen wird oder weil das Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eine terroristische Straftat begehen wird, soweit es die Daten der Personen betrifft, die diese Gefahr verursachen, oder

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

- a) Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung oder
- b) vermissten Personen.

Soweit es sich bei der terroristischen Straftat um eine Straftat handelt, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen erfasst, ist die Maßnahme nur zulässig, wenn im jeweiligen Einzelfall bestimmte Tatsachen die Prognose eines Geschehens begründen, dass für ein bedeutendes Individual- oder Kollektivrechtsgut im Sinne der jeweiligen Strafnorm die zurechenbare Gefahr der Verletzung besteht.

(3) Maßnahmen nach Absatz 1 Satz 1, 3 und 4 sowie Absatz 2 Satz 1 sind zeitlich und örtlich auf das unbedingt erforderliche Maß zu begrenzen. Sie dürfen sich nur gegen die Person richten, von der die Gefahr ausgeht oder nur auf eine Person beziehen, für die eine Gefährdungslage im Sinne des Absatzes 2 Satz 1 Nummer 2 besteht.

(4) Die zur Durchführung einer Maßnahme nach Absatz 1 Satz 4 und Absatz 2 erhobenen personenbezogenen Daten und die gewonnenen biometrischen Daten dürfen nur zweckgebunden gespeichert werden. Die in Satz 1 genannten Daten dürfen nach Maßgabe von § 79a Absatz 2 zu Strafverfolgungszwecken weiterverarbeitet werden. Liegt im Ergebnis des Abgleichs nach Absatz 1 Satz 4 oder Absatz 2 Satz 1 eine Datenübereinstimmung vor, ist diese unverzüglich durch Inaugenscheinnahme zu verifizieren, bevor weitere Maßnahmen getroffen werden. Soweit durch die Prüfung nach Satz 3 die Datenübereinstimmung verifiziert wurde und weitere Maßnahmen getroffen werden, können das Ergebnis des Datenabgleichs sowie die zur Durchführung des Abgleichs erhobenen und gewonnenen Daten gespeichert werden. Anderenfalls sind die Daten nach Satz 4 unverzüglich technisch spurenlos und automatisiert zu löschen. Gleiches gilt, wenn im Ergebnis der Prüfung nach Satz 3 keine Übereinstimmung der Daten festgestellt wurde.

(5) Maßnahmen nach Absatz 1 Satz 4 und Absatz 2 Satz 1 bedürfen einer richterlichen Anordnung auf schriftlichen Antrag der Präsidentin oder des Präsidenten des Landeskriminalamtes oder einer Polizeidirektion oder durch von diesen beauftragte Bedienstete. In dem schriftlichen 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,
2. Umfang und Dauer der Maßnahme sowie
3. 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. Die Anordnung von Maßnahmen nach Absatz 2 Satz 1 ist auf höchstens sieben Tage zu befristen. Sie kann verlängert werden, soweit die Anordnungsvoraussetzungen weiterhin vorliegen. Jede Verlängerung ist auf höchstens sieben Tage zu befristen.

(6) Der Zugang zu dem automatisierten System, mit dem Maßnahmen nach Absatz 1 Satz 4 oder Absatz 2 Satz 1 umgesetzt werden, ist auf bestimmte qualifizierte Polizeibedienstete zu beschränken. 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 und die oder der Polizeibedienstete zu erfassen ist, die oder der die Maßnahme durchführt. Die Nachvollziehbarkeit des eingesetzten automatisierten Systems muss sichergestellt sein und es muss ausgeschlossen werden, dass diskriminierende Algorithmen herausgebildet oder verwendet werden. Die oder der Sächsische Datenschutz- und Transparenzbeauftragte ist unverzüglich über abgeschlossene Maßnahmen nach Absatz 1 Satz 4 und Absatz 2 zu informieren. § 94 bleibt unberührt. Für Maßnahmen nach Absatz 1 Satz 1, 3 und 4 oder Absatz 2 Satz 1 ist die Verwendung selbstlernender Systeme ausgeschlossen. Die Mitteilungspflichten nach Artikel 5 Absatz 4 der Verordnung (EU) 2024/1689 obliegen dem Polizeipräsidium für Service und IT. Soweit für Maßnahmen nach Absatz 1 Satz 1, 3 und 4 oder Absatz 2 ein Hochrisiko-KI-System im Sinne der Verordnung (EU) 2024/1689 eingesetzt wird, sind die Betreiberpflichten nach Artikel 26 der Verordnung (EU) 2024/1689 zu erfüllen. Den Jahresbericht nach Maßgabe von Artikel 26 Absatz 10 Unterabsatz 6 der Verordnung (EU) 2024/1689 hat das Polizeipräsidium für Service und IT zu erstellen.

(7) Die Staatsregierung hat das Nähere zum Verfahren durch Rechtsverordnung zu regeln in Bezug auf:

1. die Anforderungen an die in den Abgleich einzubeziehenden biometrischen Daten,
2. das technische Verfahren,
3. die Maßgaben zur Umsetzung und Absicherung der Vorgaben nach Absatz 4 zur Zweckbindung, zur Prüfung des Ergebnisses des Abgleichs und zur Löschung,
4. die Anforderungen an die Qualitätsstandards des einzusetzenden Systems sowie
5. die Vorgaben zur Umsetzung und Überprüfung der Einhaltung der Betreiberpflichten gemäß Absatz 6 Satz 8.

§ 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 mit grenzüberschreitender Relevanz begangen werden sollen.

Maßnahmen nach § 60 sind unzulässig.

(2) Ein automatisierter unverzüglicher Abgleich nach Absatz 1 Satz 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 Satz 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 vollständig 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 spurlos 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 Beweigungsbild 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 drei Jahren, spätestens jedoch zum 31. Dezember 2029 von der 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 2 in Bezug genommenen Straftat um eine Straftat handelt, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen erfasst, ist die Maßnahme nur zulässig, wenn im jeweiligen Einzelfall bestimmte Tatsachen die Prognose eines Geschehens begründen, dass für ein bedeutendes Individual- oder Kollektivrechtsgut im Sinne der jeweiligen Strafnorm die zurechenbare Gefahr der Verletzung besteht.

(2) Wird eine nach Absatz 1 ausgeschriebene Person, ein ausgeschriebenes amtliches Kraftfahrzeugkennzeichen oder eine ausgeschriebene Sache 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 ange-troffene 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 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, oder

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 Straftat handelt, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen erfasst, ist die Maßnahme nur zulässig, wenn im jeweiligen Einzelfall bestimmte Tatsachen die Prognose eines Geschehens begründen, dass für ein bestimmtes Individual- oder Kollektivrechtsgut im Sinne der jeweiligen Strafnorm die zurechenbare Gefahr der Verletzung besteht.

(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 eine Anordnung nach Absatz 1 zur Erfüllung des Überwachungszwecks nicht ausreichend ist, dürfen die erhobenen Daten zu einem Bewegungsbild verbunden werden. Es 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 zum Schutz vor häuslicher Gewalt und sonstigen Nachstellungen nach § 19 Absatz 1 Satz 1 Nummer 1, 2 Buchstabe a, b oder d, gegen Aufenthaltsanordnungen nach § 21 Absatz 2 Satz 1 oder gegen Kontaktverbote nach § 21 Absatz 2 Satz 3,
4. zur Verfolgung einer Straftat nach § 106,
5. zur Aufrechterhaltung der Funktionsfähigkeit des technischen Mittels.

Soweit es sich bei der in Satz 7 Nummer 2 in Bezug genommenen Straftat um eine Straftat handelt, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen erfasst, ist die Maßnahme nur zulässig, wenn im jeweiligen Einzelfall bestimmte Tatsachen die Prognose eines Geschehens begründen, dass für ein bedeutendes Individual- oder Kollektivrechtsgut im Sinne der jeweiligen Strafnorm die zurechenbare Gefahr der Verletzung besteht. 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 schriftlichen 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 schriftlichen 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 Satz 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 von der Staatsregierung geprüft. Die Staatsregierung berichtet dem Landtag über das Ergebnis der Evaluierung.“

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

„§ 62a

Anlassbezogener besonderer automatisierter Datenabgleich und anlassbezogene automatisierte Datenanalyse, Verordnungsermächtigung

(1) Die Polizei kann unter den Voraussetzungen des § 79a zur Feststellung von Übereinstimmungen zwischen Daten gespeicherte personenbezogene Daten anlassbezogen zur Aufgabenerfüllung für die Dauer der Bearbeitung von Sachverhalten zweckgebunden zusammenführen, um anhand zielgerichteter Suchkriterien einen automatisierten Abgleich durchzuführen (besonderer automatisierter Datenabgleich). Für den besonderen automatisierten Datenabgleich dürfen nur personenbezogene Daten verwendet werden, die aus Anlass der Bearbeitung der Sachverhalte durch gezielte Abfragen aus den Dateisystemen der Polizei Sachsen erlangt wurden.

(2) Die Polizei kann darüber hinaus 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 nach vordefinierten Regeln verknüpfen, aufbereiten und auswerten (automatisierte Datenanalyse), soweit

1. dies erforderlich ist

a) zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder der Länder, Leib, Leben oder Freiheit einer Person oder für Sachen von besonderem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,

b) ein Angriff von erheblicher Intensität oder Auswirkung droht und

c) die automatisierte Datenanalyse erforderlich ist, um einen Schaden von den Rechtsgütern abzuwenden,

2. Tatsachen die Annahme rechtfertigen, dass

a) in absehbarer Zeit eine zumindest ihrer Art nach konkretisierte Straftat von erheblicher Bedeutung gegen ein in Nummer 1 Buchstabe a genanntes Rechtsgut begangen wird und

b) die automatisierte Datenanalyse zur Verhinderung dieser Straftat erforderlich ist, oder

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

Soweit es sich bei der in Satz 1 Nummer 2 und 3 in Bezug genommenen Straftat um eine Straftat handelt, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen erfasst, ist die Maßnahme nur zulässig, wenn im jeweiligen Einzelfall bestimmte Tatsachen die Prognose eines Geschehens begründen, dass für ein bedeutendes Individual- oder Kollektivrechtsgut im Sinne der jeweiligen Strafnorm die zurechenbare Gefahr der Verletzung besteht.

(3) 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 2 Satz 1 ergeben. Der Suchvorgang hat vorrangig an der Kategorie der betroffenen Person, die für die anlassgebende Rechtsgutsgefährdung verantwortlich ist, anzusetzen. Die Polizei hat die durch die automatisierte Datenanalyse bereitgestellten Informationen abschließend zu bewerten und die erforderlichen weiteren Entscheidungen zu treffen.

(4) Zum Zweck eines besonderen automatisierten Datenabgleichs oder 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 können ergänzend einbezogen werden, soweit dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. Personenbezogene Daten, die durch einen besonderen automatisierten Datenabgleich verarbeitet oder für eine automatisierte Datenanalyse zusammengeführt werden sollen, müssen nach § 81 gekennzeichnet sein. Von einer Verarbeitung durch automatisierte Datenanalyse sind ausgenommen:

1. personenbezogene Daten von Unbeteiligten aus der Vorgangsbearbeitung,
2. personenbezogene Daten, die aus einer Wohnraumüberwachung oder durch eine Maßnahme nach § 57 Absatz 5 Satz 2 gewonnen wurden oder die nach § 79a Absatz 4 Satz 3 erlangt wurden, und
3. biometrische Daten.

Von einer Verarbeitung durch besonderen automatisierten Datenabgleich sind die in Satz 5 Nummer 2 und 3 bezeichneten Daten ausgenommen. Bei einer Maßnahme nach Absatz 2 Satz 1 Nummer 3 dürfen keine Verkehrsdaten aus Funkzellenabfragen einbezogen werden.

(5) Der Einsatz selbstlernender Systeme ist nur zulässig

1. unter den Voraussetzungen des Absatzes 2 Satz 1 Nummer 1 oder
2. wenn
 - a) Tatsachen die Annahme rechtfertigen, dass eine zumindest ihrer Art nach konkretisierte Straftat nach §100b Absatz 2 der Strafprozessordnung, die sich gegen die Rechtsgüter nach Absatz 2 Satz 1 Nummer 1 Buchstabe a richtet, oder eine terroristische Straftat begangen werden soll und
 - b) die Maßnahme zur Verhütung dieser Straftat erforderlich ist.

Soweit es sich bei der in Satz 1 Nummer 2 in Bezug genommenen Straftat um eine Straftat handelt, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen erfasst, ist die Maßnahme nur zulässig, wenn im jeweiligen Einzelfall bestimmte Tatsachen die Prognose eines Geschehens begründen, dass für ein bedeutendes Individual- oder Kol-

ektivrechtsgut im Sinne der jeweiligen Strafnorm die zurechenbare Gefahr der Verletzung besteht.

(6) Durch eine automatisierte Datenanalyse nach Absatz 2 darf ein Profil über das Verhalten einer Person nur im Zusammenhang mit einem anlassgebenden Sachverhalt erstellt werden, wenn Tatsachen die Annahme rechtfertigen, dass diese Person für eine Gefahr verantwortlich ist und das Verhaltensprofil erforderlich ist

1. zur Abwehr einer Gefahr nach Absatz 2 Satz 1 Nummer 1 oder
2. zur Verhütung einer Straftat nach Absatz 2 Satz 1 Nummer 2, wenn mit weiteren entsprechenden Straftaten zu rechnen ist.

Ein Verhaltensprofil darf höchstens den Zeitraum von einer Woche umfassen.

(7) Die zum Zweck der automatisierten Datenanalyse anlassbezogen zusammengeführten Daten dürfen nur solange als Datenbestand gespeichert werden, wie dies für den Zweck der automatisierten Datenanalyse gemäß Absatz 2, 5 oder 6 erforderlich ist. Der Datenbestand ist unverzüglich zu löschen, wenn sich im Ergebnis der Datenanalyse keine neuen Erkenntnisse ergeben oder dessen weitere Speicherung für den Zweck der automatisierten Datenanalyse nicht mehr erforderlich ist. Spätestens drei Monate nach der Zusammenführung der personenbezogenen Daten ist zu prüfen, ob die Voraussetzungen für die weitere Speicherung des Datenbestandes noch vorliegen. Eine über Satz 3 hinausgehende Speicherung des Datenbestandes darf nur jeweils für eine Frist von 30 Tagen erfolgen. Soweit eine weitere Speicherung nach Satz 4 erfolgt, sind die Entscheidung und die maßgeblichen Gründe zu dokumentieren. Abweichend von der in Satz 3 bezeichneten Speicherfrist gilt für einen Datenbestand, der ausschließlich zum Zweck der Erstellung eines Verhaltensprofils nach Absatz 6 zusammengeführt wurde, eine Höchstspeicherfrist von 30 Tagen.

(8) Maßnahmen nach Absatz 1 kann eine Polizeibedienstete oder ein Polizeibediensteter anordnen. Die Anordnung ist zu begründen und zu dokumentieren. Maßnahmen nach Absatz 2 sind durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion oder durch von diesen hierzu beauftragte Bedienstete anzuordnen. Im Fall von Absatz 5 und 6 ist die Datenanalyse auf Antrag der Polizei richterlich anzuordnen. In dem schriftlichen Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet,
2. der Sachverhalt,
3. die Begründung und
4. das System, auf dessen Grundlage die automatisierte Datenanalyse erfolgen soll.

Maßnahmen nach den Absätzen 2, 5 und 6 sind nur zulässig, soweit dies durch richterliche Anordnung auf schriftlichen Antrag der Polizei ausdrücklich gestattet ist. Bei Gefahr im Verzug dürfen Maßnahmen nach Absatz 5 oder 6 nur durch die Präsidentin oder den Präsidenten des Landeskriminalamtes oder einer Polizeidirektion oder durch von diesen hierzu beauftragte Bedienstete angeordnet werden. Für die Anordnung einer Maßnahme nach den Absätzen 2, 5 und 6 gilt § 73 Absatz 2, 3 Satz 1 und 2 sowie Absatz 4 entsprechend.

(9) Der Zugang zu einem automatisierten System, mit dem Maßnahmen nach den Absätzen 2, 5 und 6 umgesetzt werden, ist auf bestimmte qualifizierte Polizeibedienstete zu beschränken und es ist eine Zugriffskontrolle sicherzustellen. Für die Protokollierung von Maßnahmen nach den Absätzen 2, 5 und 6 gilt § 75 Absatz 1 mit der Maßgabe, dass auch

das eingesetzte automatisierte System und die oder der Polizeibedienstete zu erfassen sind, die oder der die Maßnahme durchführt. Die Nachvollziehbarkeit des eingesetzten automatisierten Systems muss sichergestellt sein und es muss ausgeschlossen werden, dass diskriminierende Algorithmen herausgebildet oder verwendet werden. Der Einsatz von Systemen, deren Entscheidungslogik nicht nachvollziehbar und überprüfbar offengelegt werden kann, ist unzulässig. Eine direkte Anbindung der Analyseplattform an Internetdienste ist unzulässig.

(10) Die Staatsregierung hat das Nähere zum Verfahren zu Maßnahmen nach den Absätzen 2, 5 und 6 durch Rechtsverordnung zu regeln in Bezug auf:

1. technisch-organisatorische Maßnahmen zur Sicherstellung der Einhaltung der Zweckbindung und Kennzeichnung der verarbeiteten Daten,
2. Kategorien für Suchbegriffe, nach denen die zusammengeführten Daten analysiert werden,
3. Strukturen zur Funktionsweise und Entscheidungslogik der Verarbeitungsprozesse,
4. technisch-organisatorische Anforderungen zur Gewährleistung der Speicherdauer des zusammengeführten Datenbestandes und der Prüfung nach Absatz 6,
5. Anforderungen an die Zugangsberechtigungen, die Zugriffskontrollen und die Protokollierung der Durchführung von Zugriffskontrollen,
6. Maßnahmen zur Nachvollziehbarkeit und Kontrolle des jeweils eingesetzten automatisierten Verfahrens durch die anwendenden Polizeibediensteten,
7. verfahrensrechtliche Maßnahmen zum Zweck der Erkennung und Korrektur fehlerhafter Datenauswertung.

§ 62b

Anlassbezogene nachträgliche Fernidentifizierung

(1) Die Polizei kann zur Abwehr einer Gefahr für die öffentliche Sicherheit anlassbezogen aus Daten zu Gesicht oder Stimme einer Person, die sie im Rahmen ihrer Aufgaben erlangt hat, biometrische Daten gewinnen und diese mit biometrischen Daten, die sie aus anderen bereits rechtmäßig in polizeilichen Systemen gespeicherten Daten gewonnen hat, auf Übereinstimmungen abgleichen, soweit dies zur Identifizierung einer Person oder zur Ermittlung des Aufenthaltsortes der Person erforderlich ist. Der Abgleich muss zur Abwehr einer Gefahr für die öffentliche Sicherheit zwingend erforderlich sein. Aus dem Einsatz technischer Mittel in oder aus Wohnungen erlangte Daten oder Daten nach § 79a Absatz 4 Satz 3 dürfen bei Maßnahmen nach Satz 1 nicht verwendet werden.

(2) Die Polizei kann anlassbezogen einen Abgleich gemäß Absatz 1 auch in der Weise vornehmen, dass sie aus öffentlich zugänglichen personenbezogenen Daten aus dem Internet biometrische Daten gewinnt und diese mit biometrischen Daten, die sie zur Erfüllung ihrer Aufgaben verarbeiten darf oder für die sie eine Berechtigung zum Abruf hat, automatisiert 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, und
2. die Identifizierung oder die Ermittlung des Aufenthaltsortes 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 in absehbarer Zeit auf eine zumindest der Art nach konkretisierte Weise eine in § 100b Absatz 2 der Strafprozessordnung genannte und voraussichtlich auch im Einzelfall besonders schwerwiegende Straftat begehen wird, die sich gegen die Rechtsgüter nach Satz 1 Nummer 1 richtet, oder

2. das Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft 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 in Echtzeit übertragenen Video-, Ton- und Bilddateien ist ausgeschlossen. Soweit es sich bei der in Satz 1 in Bezug genommenen Straftat um eine Straftat handelt, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen erfasst, ist die Maßnahme nur zulässig, wenn im jeweiligen Einzelfall bestimmte Tatsachen die Prognose eines Geschehens begründen, dass für ein bedeutendes Individual- oder Kollektivrechtsgut im Sinne der jeweiligen Strafnorm die zurechenbare Gefahr der Verletzung besteht.

(3) Maßnahmen nach Absatz 1 oder 2 dürfen sich nur gegen eine Person richten, von der die Gefahr ausgeht. Darüber hinaus dürfen Maßnahmen nach Absatz 2 auch zur gezielten Suche nach einer Person durchgeführt werden, soweit deren in Absatz 2 Satz 1 Nummer 1 genannte Rechtsgüter gefährdet sind.

(4) Die zur Durchführung einer Maßnahme nach den Absätzen 1 und 2 gewonnenen biometrischen Daten und die im Rahmen von Absatz 2 erhobenen öffentlich zugänglichen Daten dürfen nur zweckgebunden gespeichert werden. Die in Satz 1 genannten Daten dürfen nach Maßgabe von § 79a Absatz 2 zu Strafverfolgungszwecken weiterverarbeitet werden. Liegt im Ergebnis des Abgleichs nach Absatz 1 oder 2 eine Datenübereinstimmung vor, ist diese unverzüglich durch Inaugenscheinnahme zu verifizieren, bevor weitere Maßnahmen getroffen werden. Soweit durch die Prüfung nach Satz 3 die Datenübereinstimmung verifiziert wurde und weitere Maßnahmen getroffen werden, können das Ergebnis des Datenabgleichs und die zur Durchführung des Abgleichs gewonnenen und erhobenen Daten gespeichert werden. Anderenfalls sind die Daten nach Satz 4 unverzüglich technisch spurenlos und automatisiert zu löschen. Gleiches gilt, wenn im Ergebnis der Prüfung nach Satz 3 keine Übereinstimmung der Daten festgestellt wurde.

(5) Für die Verarbeitung von öffentlich zugänglichen Daten gilt § 76 Absatz 1 und 5.

(6) Maßnahmen nach Absatz 1 Satz 1 kann eine Polizeibedienstete oder ein Polizeibediensteter anordnen. Maßnahmen nach Absatz 2 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, insbesondere die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme.

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

(7) Der Zugang zu dem automatisierten System, mit dem Maßnahmen nach den Absätzen 1 und 2 umgesetzt werden, ist auf bestimmte qualifizierte Polizeibedienstete zu beschränken. Für die Protokollierung einer Maßnahme nach den Absätzen 1 oder 2 gilt § 75 Absatz 1 mit der Maßgabe, dass auch das eingesetzte automatisierte System zur Datenverarbeitung und die oder der Polizeibedienstete zu erfassen ist, die oder der die Maßnahme durchführt. Die Nachvollziehbarkeit des eingesetzten automatisierten Systems muss sichergestellt sein und es muss ausgeschlossen werden, dass diskriminierende Algorithmen herausgebildet oder verwendet werden. Die oder der Sächsische Datenschutz- und Transparenzbeauftragte ist unverzüglich über abgeschlossene Maßnahmen nach Absatz 2 zu informieren. § 94 bleibt unberührt. Für Maßnahmen nach Absatz 1 oder 2 ist die Verwendung selbstlernender Systeme ausgeschlossen. Soweit für Maßnahmen nach Absatz 1 oder Absatz 2 ein Hochrisiko-KI-System im Sinne der Verordnung (EU) 2024/1689 eingesetzt wird, sind die Betreiberpflichten nach Artikel 26 der Verordnung (EU) 2024/1689 zu erfüllen. Den Jahresbericht nach Maßgabe von Artikel 26 Absatz 10 Unterabsatz 6 der Verordnung (EU) 2024/1689 hat das Polizeipräsidium für Service und IT zu erstellen.

(8) Das Staatsministerium des Innern hat nach Anhörung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten technisch-organisatorische Einzelheiten in einer zu veröffentlichenden Verwaltungsvorschrift zu regeln und insbesondere zu bestimmen:

1. die Anforderungen an die in den Abgleich einzubeziehenden biometrischen Daten,
2. das technische Verfahren,
3. die Maßgaben zur Umsetzung und Absicherung der Vorgaben nach Absatz 4 zur Zweckbindung, zur Prüfung des Ergebnisses des Abgleichs und zur Löschung,
4. die Anforderungen an die Qualitätsstandards des einzusetzenden automatisierten Systems sowie
5. die Vorgaben zur Umsetzung und Überprüfung der Einhaltung der Betreiberpflichten gemäß Absatz 7 Satz 5.“

17§ 63 Absatz 2 wird durch den folgenden 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,
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 Straftat handelt, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen erfasst, ist die Maßnahme nur zulässig, wenn im jeweiligen Einzelfall bestimmte Tatsachen die Prognose eines Geschehens begründen, dass für ein bedeutendes Individual-

oder Kollektivrechtsgut im Sinne der jeweiligen Strafnorm die zurechenbare Gefahr der Verletzung besteht.“

18§ 64 wird durch den folgenden § 64 ersetzt:

„§ 64

Einsatz Verdeckter Ermittlerinnen, Verdeckter Ermittler und von V-Personen

(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 angeworben und eingesetzt werden, wer

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

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

3. an einem Aussteigerprogramm teilnimmt oder

4. im Bundeszentralregister eingetragen ist mit einer Verurteilung, welche aufgrund einer mit lebenslanger Haft bedrohten Straftat erfolgt ist oder wegen eines Verbrechens, welches allein mit einer Freiheitsstrafe von mindestens zehn Jahren geahndet wurde.

(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. In dem schriftlichen 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.In § 65 Absatz 3 Satz 2 wird die Angabe „§ 79 Absatz 2 und 3 Satz 1“ durch die Angabe „§ 79a Absatz 2 und 4 Satz 1“ ersetzt.

20.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 oder 3 in Bezug genommenen Straftat um eine Straftat handelt, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen erfasst, ist die Maßnahme nur zulässig, wenn im jeweiligen Einzelfall bestimmte Tatsachen die Prognose eines Geschehens begründen, dass für ein bedeutendes Individual- oder Kollektivrechtsgut im Sinne der jeweiligen Strafnorm die zurechenbare Gefahr der Verletzung besteht. 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 3 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.

(3) 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 deren Telekommunikationsanschluss oder Endgerät eine Person nach den Nummern 1 bis 3 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 2 oder 3 in Bezug genommenen Straftat um eine Straftat handelt, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen erfasst, ist die Maßnahme nur zulässig, wenn im jeweiligen Einzelfall bestimmte Tatsachen die Prognose eines Geschehens begründen, dass für ein bedeutendes Individual- oder Kollektivrechtsgut im Sinne der jeweiligen Strafnorm die zurechenbare Gefahr der Verletzung besteht. 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.

(4) 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.

(5) Maßnahmen nach den Absätzen 1 und 2 bedürfen einer richterlichen Anordnung auf Antrag der Polizei. In dem schriftlichen 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.

(6) 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 Rechtsverordnung 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.

(7) 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 von der 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. In dem schriftlichen 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. In dem schriftlichen 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 von digitalen Diensten nach § 2 Absatz 2 Nummer 1 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 Kartenummer 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 im Sinne des § 3 Nummer 1 des Telekommunikationsgesetzes sowie § 2 Absatz 2 Nummer 1 des Telekommunikation-Digitale-Dienste-Datenschutzgesetzes 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. In dem schriftlichen 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.“

21§ 69 wird gestrichen.

22Die §§ 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 2 Nummer 1 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 Satz 1 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 oder

d) 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 ist.

(3) Maßnahmen nach Absatz 1 Satz 2 bedürfen einer richterlichen Anordnung auf schriftlichen 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 2 Nummer 1 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 mittels Bildübertragung nach § 57 Absatz 1,
3. offene Beobachtung und Aufzeichnung mittels Bild- und Tonübertragung nach § 57 Absatz 2 und 3,
4. Datenerhebung durch Observation und Einsatz technischer Mittel nach § 63 Absatz 1 und 2,
5. Datenerhebung durch Einsatz technischer Mittel in Wohnungen nach § 65 Absatz 1 sowie
6. Datenerhebung durch den verdeckten Einsatz technischer Mittel zur Standorterhebung nach § 68 Absatz 2.

In den Fällen des Satzes 1 Nummer 1 bis 3 dürfen unbemannte Luftfahrtsysteme nur dann eingesetzt werden, wenn die Offenheit der Maßnahme gewahrt bleibt. In diesen Fällen ist auf die Verwendung unbemannter Luftfahrtsysteme gesondert hinzuweisen.

(2) Die Polizei kann im öffentlichen Verkehrsraum offen Übersichtsbildübertragungen anfertigen, wenn dies für die Übersichtlichkeit der Lage zur Lenkung und Leitung von Verkehrsmaßnahmen und Unglücksfällen oder Verkehrsunfällen im Einzelfall erforderlich ist. Eine Identifikation von Personen oder Aufzeichnung der Übertragung ist unzulässig. Absatz 1 Satz 3 gilt entsprechend.

(3) 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.“

23§ 72 wird gestrichen.

24Die §§ 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, soweit nichts anderes bestimmt ist.

(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 nach den §§ 57a und 60 bis 68 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 vor-

liegen. Die Regelungen in § 57a Absatz 5 Satz 4 bis 6, § 60 Absatz 3 Satz 1 bis 3, § 62a Absatz 6 Satz 2, § 64 Absatz 7 Satz 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 und bei Maßnahmen nach § 62a Absatz 2, 5 und 6 sowie nach § 62b Absatz 2 innerhalb von 48 Stunden nachzuholen. Die Maßnahme ist zu beenden und die bereits gespeicherten personenbezogenen Daten sind unverzüglich zu löschen, wenn die richterliche Bestätigung abgelehnt wird oder die Bestätigung nicht innerhalb von drei Tagen erfolgt. Abweichend von Satz 4 gelten für die Löschung von Daten, die durch die in Satz 3 bezeichneten Maßnahmen erhoben wurden, die dort genannten Fristen.

(5) Für polizeiliche Anordnungen nach den §§ 57a und 60 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 § 62a Absatz 2, 5 oder 6 die Person, über die neue Erkenntnisse erlangt wurden oder ein Verhaltensprofil erstellt wurde,
6. im Fall des § 62b Absatz 2 die Zielperson,
7. im Fall des § 63
 - a) die Zielperson und
 - b) die erheblich mitbetroffenen Personen,
8. 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,
9. im Fall des § 65
 - a) die Zielperson,
 - b)

die erheblich mitbetroffenen Personen sowie

c) die Eigentümer und Bewohner der überwachten Wohnung,

10 im Fall des § 66 die Beteiligten der überwachten Telekommunikation,

11 im Fall des § 66a die Zielperson,

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

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

14 im Fall des § 68 die Zielperson, soweit sie nicht von der Maßnahme Kenntnis erlangt hat, und

15 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. In den Fällen von Satz 1 Nummer 1 und 6 hat die Benachrichtigung darüber hinaus über die Verwendung eines Hochrisiko-KI-Systems zu informieren.

(2) Die Benachrichtigung einer Person nach Absatz 1 Satz 1 Nummer 10, 12 oder 13, 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, 58 und 60 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 Übermittlungersuchen 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 § 62a Absatz 2, 5 und 6 die Person, über die neue Erkenntnisse erlangt wurden oder über die ein Verhaltensprofil erstellt wurde,

6. bei Maßnahmen nach § 62b Absatz 2 die Zielperson, gegen die im Trefferfall weitere Maßnahmen angeordnet wurden oder die Person, zu deren Schutz die Maßnahme erfolgte,

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

8. 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,

9. 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,

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

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

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

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

14. bei Maßnahmen nach § 68 die Zielperson und

15. 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.“

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

26. § 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.

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

„§ 79

Befugnis zur Datenverarbeitung

(1) Die Polizei kann personenbezogene Daten in Dateisystemen 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 oder Verfolgung solcher Straftaten oder Ordnungswidrigkeiten ergeben oder
 - b) zur Abwehr von in absehbarer Zeit drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter erkennen lassen.

Vorschriften dieses Gesetzes oder andere Rechtsvorschriften zur zweckändernden Weiterverarbeitung bleiben unberührt.

(3) 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.

(4) Für die Weiterverarbeitung von personenbezogenen Daten, die durch eine Maßnahme nach § 65 Absatz 1 und 2 und § 57 Absatz 5 Satz 2 erlangt wurden, gilt Absatz 2 Satz 1 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 oder des § 57 Absatz 4 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.

(5) 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 des Absatzes 2 nicht erfüllt sind.

(6) Bei der Weiterverarbeitung von personenbezogenen Daten ist durch organisatorische und technische Vorkehrungen sicherzustellen, dass die Bestimmungen der Absätze 1, 2 und 4 beachtet werden.

§ 79b

Weiterverarbeitung zu Aus- und Fortbildungszwecken, zu statistischen 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 zu im öffentlichen Interesse liegenden wissenschaftlichen Forschungszwecken nach Maßgabe des § 6 des Sächsischen Datenschutz-Umsetzungsgesetzes weiterverarbeiten.

(3) Die Polizei kann personenbezogene Daten, die ausschließlich zum Zweck der Vorgangsverwaltung oder der zeitlich befristeten Dokumentation behördlichen Handelns 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. Für die Weiterverarbeitung von Protokolldaten gilt § 32 Absatz 1 des Sächsischen Datenschutz-Umsetzungsgesetzes.

§ 79c

Entwicklung, Training und Testen von regelbasierten und lernenden IT-Systemen, Verordnungsermächtigung

(1) Die Polizei kann rechtmäßig gespeicherte personenbezogene Daten zum Zweck der Entwicklung, des Trainierens und Testens von IT-Systemen über die vorgesehene Speicherdauer hinaus nach Maßgabe der Absätze 2 bis 5 zur Aufgabenerfüllung weiterverarbeiten und dafür auch an Auftragsverarbeiter übermitteln, soweit dies für die Aufgabenerfüllung und für die Entwicklung, das Training oder Testen des jeweiligen IT-Systems erforderlich ist. Die Verarbeitung personenbezogener Daten ist auf das für den jeweiligen Trainingszweck erforderliche Maß zu beschränken. Soweit personenbezogene Daten zu Trai-

ningszwecken verarbeitet werden, dürfen nur solche Daten verarbeitet werden, die im Zusammenhang mit der zu trainierenden Aufgabenwahrnehmung erhoben und gespeichert wurden. Die Polizei hat zu überprüfen und sicherzustellen, dass bei der Entwicklung sowie dem Trainieren und Testen von IT-Systemen nur Daten zugrunde gelegt werden, die nicht diskriminierend sind. Es ist sicherzustellen, dass bei der Weiterverarbeitung nach Absatz 1 Satz 1 diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Hierzu sind bei der Entwicklung, dem Training und Testen von KI-Systemen gezielt auch geeignete Datensätze aus nicht-polizeilichen Datenbanken zu verwenden. Durch geeignete technische und organisatorische Maßnahmen ist die Nachvollziehbarkeit des verwendeten Verfahrens sicherzustellen. Es ist zu dokumentieren, welche Daten für die Entwicklung, das Trainieren oder das Testen von IT-Systemen verwendet wurden. Die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen nach § 65 Absatz 1, die durch den Einsatz von körpernah getragenen Aufzeichnungsgeräten in Wohnungen nach § 57 Absatz 5 Satz 2 oder durch Überwachung und Aufzeichnung von Telekommunikation nach § 66 Absatz 1 und 2 erhoben wurden, oder von Daten nach § 79a Absatz 4 Satz 3 ist unzulässig.

(2) Personenbezogene Daten sind für die Verwendung zu Entwicklungs-, Trainings- oder Testzwecken zu anonymisieren. Können diese Zwecke der Entwicklung, des Trainings oder des Testens mit anonymisierten Daten nicht erreicht werden oder ist die Anonymisierung nur mit unverhältnismäßigem Aufwand möglich, sind sie zu pseudonymisieren. Besondere Kategorien personenbezogener Daten dürfen unter Gewährleistung von Garantien im Sinne des § 4 Absatz 2 des Sächsischen Datenschutz-Umsetzungsgesetzes verwendet werden. Die Daten sind unverzüglich zu löschen, soweit sie nicht mehr benötigt werden. Die Löschung ist zu protokollieren. Die Wiederherstellung von personenbezogenen Daten, die zum Zweck der Entwicklung, des Trainings oder des Testens von KI-Systemen verwendet wurden und die Deanonymisierung von Daten nach Satz 1 sind unzulässig.

(3) Personenbezogene Daten dürfen zur Entwicklung, zum Testen und Trainieren von IT-Systemen nur an Auftragsverarbeiter übermittelt werden, deren Firmensitz und Serverstrukturen innerhalb der Europäischen Union liegen, wenn eine Verarbeitung bei der Polizei selbst nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

(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 technische und organisatorische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(5) Auftragsverarbeiter dürfen die übermittelten Daten nur im Rahmen der jeweiligen Entwicklung, des jeweiligen Trainings und des jeweiligen Tests verarbeiten. Sie sind verpflichtet, die Daten nach Abschluss von Training und Test des lernenden Systems unverzüglich wieder zu löschen. Sie dürfen die trainierten Modelle für eigene Zwecke weiternutzen, wenn die Polizei dem ausdrücklich zugestimmt hat 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 die Staatsregierung in einer nach Anhörung der oder des Sächsischen Datenschutz- und Transparenzbeauftragten zu erlassenden Rechtsverordnung die technisch-organisatorischen Einzelheiten zu regeln und insbesondere zu bestimmen:

1. Art, Umfang und Anforderungen an die Qualität der zu verarbeitenden Daten,

2. den Personenkreis, der von der Verarbeitung betroffen ist,
3. Maßnahmen, die die Einhaltung der fachlichen und rechtlichen Anforderungen an die Entwicklung, das Training und das Testen von lernenden IT-Systemen sicherstellen,
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 erhoben oder erlangt 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 Satz 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. personengebundene Hinweise nach § 79 Absatz 4,
4. die sachbearbeitende Polizeidienststelle und die Vorgangsnummer oder das Aktenzeichen,
5. die Tatzeiten und Tatorte sowie
6. die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten.

Von Personen nach Absatz 1 Satz 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 Zeuginnen und 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 Satz 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.

§ 80b

Vorsorgende Speicherung von zu Gefahrenabwehrzwecken erhobenen Daten

(1) Die Polizei kann personenbezogene Daten, die sie auf der Grundlage dieses Gesetzes erhoben oder erlangt 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 bis 3 bezeichneten Daten sowie der Bezugssachverhalt, zu Personen nach Satz 1 Nummer 2 die in § 80 Absatz 2 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 der personenbezogenen Daten 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. Soweit die weitere Speicherung der Daten erforderlich ist, sind die Gründe hierfür und die Dauer der bestimmten Aussonderungsprüffrist zu dokumentieren.

(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 Satz 1 Nummer 1 bei Erwachsenen zehn Jahre und bei Jugendlichen fünf Jahre,
2. § 80 Absatz 1 Satz 1 Nummer 2
 - a) in Bezug auf schwere Straftaten nach § 100a Absatz 2 der Strafprozessordnung bei Erwachsenen fünf Jahre und bei Jugendlichen vier Jahre,
 - b) in Bezug auf sonstige Straftaten bei Erwachsenen drei Jahre und bei Jugendlichen zwei Jahre,
3. § 80 Absatz 1 Satz 1 Nummer 3
 - a)

in Bezug auf schwere Straftaten nach § 100a Absatz 2 der Strafprozessordnung bei Erwachsenen fünf Jahre, bei Jugendlichen vier Jahre und bei Kindern ab Vollendung des siebten Lebensjahres zwei Jahre,

b) in Bezug auf sonstige Straftaten bei Erwachsenen drei Jahre, bei Jugendlichen zwei Jahre und bei Kindern ab Vollendung des siebten Lebensjahres ein Jahr,

4. § 80 Absatz 1 Satz 1 Nummer 4 und § 80b Absatz 1 Satz 1 Nummer 2 bei Erwachsenen zwei Jahre, bei Jugendlichen und Kindern ab Vollendung des siebten Lebensjahres ein Jahr,

5. § 80a Absatz 1 Satz 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,

6. § 80a Absatz 1 Satz 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,

7. § 80b Absatz 1 Satz 1 Nummer 1 für vermisste Personen fünf Jahre und für hilflose oder gefährdete Personen zwei Jahre,

8. § 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 und bei Jugendlichen nicht länger als zwei Jahre 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. Absatzes 3 Satz 1 Nummer 2 Buchstabe b kann die Aussonderungsprüffrist höchstens zweimal verlängert werden,

2. Absatzes 3 Satz 1 Nummer 5 Buchstabe a kann die Aussonderungsprüffrist um ein Jahr verlängert werden.

In den Fällen des Absatzes 3 Satz 1 Nummer 5 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 Lösungsverpflichtungen,

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 Lösungsverpflichtungen und

d) die Einhaltung von Dokumentationspflichten

gewährleistet.“

28§ 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.

29Die §§ 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

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 elementa-

ren 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 1 an die Polizeidienststellen anderer Länder oder des Bundes personenbezogene Daten übermitteln, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Soweit die Datenübermittlung zur Erfüllung der Aufgaben des Empfängers erforderlich ist, gelten die Anforderungen des § 79a Absatz 2 und 4.

(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. 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.

Soweit die Datenübermittlung durch die Polizei zur Erfüllung ihrer Aufgaben erfolgt, gelten die Anforderungen des § 79a Absatz 1; soweit sie zur Aufgabenerfüllung des Empfängers erforderlich ist, gelten die Anforderungen des § 79a Absatz 2 und 4.

(3) Die Polizei kann von sich aus personenbezogene Daten an nichtöffentliche Stellen im Sinne des § 2 Absatz 4 des Bundesdatenschutzgesetzes übermitteln, soweit dies 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,
4. Ermöglichung einer Kontaktaufnahme durch eine vom 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, oder
5. Verhütung häuslicher Gewalt durch eine vom Staatsministerium für Soziales, Gesundheit und Gesellschaftlichen Zusammenhalt bestimmte Beratungsstelle, soweit sie Kenntnis von Handlungen häuslicher Gewalt erlangt hat.

Absatz 2 Satz 2 gilt entsprechend. Bei Übermittlungen nach Satz 1 Nummer 4 und 5 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.“

30§ 86 wird durch den 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 30 Tagen zu löschen, soweit die weitere Verarbeitung nicht zur Abwehr einer Gefahr oder zur Verfolgung von Straftaten erforderlich ist. § 79b Absatz 1 bleibt unberührt.“

31§ 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 berechnigte 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, sind gesondert zu speichern und dürfen ausschließlich zum Zweck der Durchführung einer Zuverlässigkeitsüberprüfung verarbeitet werden. 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 Vorlie-

gen 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 zu Dokumentationszwecken für die Dauer von sechs Monaten speichern. Abweichend davon kann eine längere Speicherung erfolgen, soweit und solange dies aufgrund eines bereits anhängigen oder zu erwartenden Rechtsstreits erforderlich ist. Die Frist beginnt mit der Beendigung der Veranstaltung.

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

32.Nach § 89 wird der folgende § 89a eingefügt:

„§ 89a

Datenübermittlung und -bereitstellung an Mitgliedstaaten der Europäischen Union und Schengen-assoziierte Staaten gemäß der Richtlinie (EU) 2023/977

(1) Für den unmittelbaren Informationsaustausch zur Verhütung von Straftaten zwischen der Polizei und den Polizeibehörden oder sonstigen für die Verhütung oder Verfolgung von Straftaten zuständigen öffentlichen Stellen der Mitgliedstaaten der Europäischen Union und der Schengen-assoziierten Staaten sowie deren zentralen Kontaktstellen im Anwendungsbereich der Richtlinie (EU) 2023/977 gelten ergänzend zu den §§ 83 und 89 die folgenden Absätze. Soweit der Informationsaustausch über das Bundeskriminalamt als zentrale Kontaktstelle im Anwendungsbereich der Richtlinie (EU) 2023/977 erfolgt, gelten die Vorschriften des Bundeskriminalamtgesetzes.

(2) Informationsersuchen an die zentrale Kontaktstelle eines in Absatz 1 Satz 1 genannten Staates sind dem Landeskriminalamt als benannter Stelle im Sinne von Artikel 4 Absatz 1 der Richtlinie (EU) 2023/977 vorbehalten. Ein solches Ersuchen muss mindestens enthalten:

1. die Angabe, ob das Ersuchen dringend ist, und gegebenenfalls die Gründe für die Dringlichkeit,
2. eine Präzisierung der angeforderten mutmaßlich verfügbaren Informationen, die so detailliert ist, wie dies unter den gegebenen Umständen in angemessener Weise möglich ist,
3. die Beschreibung des Zwecks, zu dem die Informationen angefordert werden, einschließlich einer Beschreibung des Sachverhalts und der zugrundeliegenden Straftat,
4. die objektiven Gründe, die Anlass zu der Annahme geben, dass die angeforderten Informationen dem ersuchten Staat zur Verfügung stehen,
5. gegebenenfalls eine Erläuterung des Zusammenhangs zwischen dem Zweck, zu dem die Informationen angefordert werden, und allen natürlichen oder juristischen Personen oder Organisationen, auf die sich die Informationen beziehen, sowie
6. etwaige Beschränkungen einer Verwendung der in dem Ersuchen enthaltenen Informationen zu anderen Zwecken als denen, für die sie übermittelt wurden.

Ersuchen sind in einer Sprache zu übermitteln, die der ersuchte Staat für diese Zwecke zugelassen hat. Eine Kopie des Ersuchens ist zugleich dem Bundeskriminalamt zu übermitteln.

(3) Wird ein Informationensuchen unmittelbar an eine Polizeibehörde oder sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stelle eines in Absatz 1 Satz 1 genannten Staates gerichtet, die nicht zugleich zentrale Kontaktstelle ist, ist dem Bundeskriminalamt sowie der zentralen Kontaktstelle des jeweiligen Staates jeweils zugleich eine Kopie zu übermitteln.

(4) Daten mit oder ohne Personenbezug (Informationen), die die Polizei zuvor von einem der in Absatz 1 Satz 1 genannten Staaten oder von einem Drittstaat erlangt hat, dürfen nur mit Einwilligung dieses Staates und nur unter den von ihm festgelegten Voraussetzungen für die Verwendung der Informationen übermittelt werden.

(5) Bei der Übermittlung von Informationen ist mitzuteilen, dass die Verwendung als Beweismittel in einem Gerichtsverfahren unzulässig ist, es sei denn,

1. es liegt eine Zustimmung derjenigen Stelle vor, die für eine Zustimmung der Verwendung als Beweismittel zuständig ist, oder

2. die Verwendung als Beweismittel ist durch eine anwendbare völkerrechtliche Vereinbarung oder einen unmittelbar anwendbaren Rechtsakt der Europäischen Union zugelassen.

Die Zuständigkeit für die Zustimmung einer Verwendung als Beweismittel nach Satz 1 Nummer 1 richtet sich nach den Vorschriften über die internationale Rechtshilfe in Strafsachen.

(6) Eine Übermittlung von Informationen an die zentrale Kontaktstelle eines in Absatz 1 Satz 1 genannten Staates erfolgt in einer Sprache, die dieser Staat für diese Zwecke zugelassen hat; eine Kopie dieser Informationen ist zugleich dem Bundeskriminalamt zu übermitteln. Werden Informationen an eine andere Polizeibehörde oder eine sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stelle eines in Absatz 1 Satz 1 genannten Staates übermittelt, ist dem Bundeskriminalamt sowie der zentralen Kontaktstelle des jeweiligen Staates jeweils zugleich eine Kopie zu übermitteln.

(7) Die Polizei hat verfügbare Informationen im Sinne von Artikel 2 Absatz 5 der Richtlinie (EU) 2023/977 von sich aus an die zentrale Kontaktstelle oder eine Polizeibehörde oder sonstige für die Verhütung von Straftaten zuständige Stelle eines in Absatz 1 Satz 1 genannten Staates zu übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass diese Informationen für den jeweiligen Staat zum Zweck der Verhütung von Straftaten im Sinne von Artikel 2 Absatz 3 der Richtlinie (EU) 2023/977 von Bedeutung sein können, keine der in § 83 genannten Gründe vorliegen und die Informationen diesem Staat nicht bereits anderweitig übermittelt wurden.

(8) Informationen, die personenbezogene Daten darstellen, dürfen nur unter den Voraussetzungen des § 89 übermittelt werden; die Übermittlung ist auf solche Daten beschränkt, die unter die in Anhang II Buchstabe B der Verordnung (EU) 2016/794 aufgeführten Kategorien fallen. Eine für die Übermittlung personenbezogener Daten im Einzelfall erforderliche gerichtliche Erlaubnis ist unverzüglich einzuholen.“

33§ 91 wird durch den 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 einzu-

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

35 § 94 Nummer 1 wird durch die folgende Nummer 1 ersetzt:

„1. die Datenverarbeitung bei Maßnahmen nach § 57a Absatz 1 Satz 4 und Absatz 2, § 58, den §§ 60 bis 62, § 62a Absatz 2, 5 und 6, § 62b Absatz 2 sowie den §§ 63 bis 68, auch im Hinblick auf die Datenverarbeitung in polizeilichen Dateisystemen, und“.

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

37.

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

38§ 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.“

39.Nach § 106 wird der folgende § 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.“

40§ 107 wird durch den 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, § 58, den §§ 60 bis 62, § 62a Absatz 5 und 6, § 62b Absatz 2 und den §§ 63 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.“

41§ 108 wird gestrichen.

Artikel 2

Weitere Änderung des Sächsischen Polizeivollzugsdienstgesetzes

Das **Sächsische Polizeivollzugsdienstgesetz**, das zuletzt durch Artikel 1 dieses Gesetzes geändert worden ist, wird wie folgt geändert:

1. § 57 wird wie folgt geändert:

a) Absatz 4 wird wie folgt geändert:

aa) Die Sätze 2 bis 4 werden gestrichen.

bb) Im neuen Satz 2 wird die Angabe „Nach den Sätzen 1 und 2“ durch die Angabe „Nach Satz 1“ ersetzt.

b) Absatz 5 Satz 2 wird gestrichen.

c) Absatz 8 Satz 6 und 7 wird gestrichen.

d) Absatz 10 wird gestrichen.

2. § 62a Absatz 4 Satz 5 Nummer 2 wird durch die folgende Nummer 2 ersetzt:

„2. personenbezogene Daten, die aus einer Wohnraumüberwachung gewonnen wurden oder von nach § 79a Absatz 4 Satz 3 erlangten Daten, und“

3. § 66 wird wie folgt geändert:

a) Die Absätze 2 bis 4 werden gestrichen.

b) Absatz 5 wird zu Absatz 2 und die Angabe „den Absätzen 1 und 2“ durch die Angabe „Absatz 1“ ersetzt.

c) Absatz 7 wird gestrichen.

Artikel 3

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 den folgenden Absatz 2 ersetzt:

„(2) Während der Nachtzeit (§ 104 Absatz 3 der Strafprozessordnung) darf eine Wohnung nur in den Fällen des Absatzes 1 Satz 1 Nummer 1 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 den 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 den 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 Absatz 1 und 2 sowie Absatz 5, § 81 Absatz 3, die §§ 82 bis 84 Absatz 1, 2 und 3 Nummer 1 bis 3 sowie Absatz 4 und 5 sowie die §§ 89, 90 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 4

Einschränkung von Grundrechten

Durch die Artikel 1 und 3 dieses Gesetzes werden eingeschränkt die Grundrechte auf

1. Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes für die Bundesrepublik Deutschland, Artikel 16 Absatz 1 Satz 2 der Verfassung des Freistaates Sachsen),

2. körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes für die Bundesrepublik Deutschland, Artikel 16 Absatz 1 Satz 1 der Verfassung des Freistaates Sachsen),

3. Unverletzlichkeit des Fernmeldegeheimnisses (Artikel 10 Absatz 1 des Grundgesetzes für die Bundesrepublik Deutschland, Artikel 27 Absatz 1 der Verfassung des Freistaates Sachsen),

4. Freizügigkeit (Artikel 11 des Grundgesetzes für die Bundesrepublik Deutschland),

5. Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes für die Bundesrepublik Deutschland, Artikel 30 Absatz 1 der Verfassung des Freistaates Sachsen),

6. informationelle Selbstbestimmung (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes für die Bundesrepublik Deutschland, Artikel 33 der Verfassung des Freistaates Sachsen) sowie

7.

Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes für die Bundesrepublik Deutschland, Artikel 33 der Verfassung des Freistaates Sachsen).

Artikel 5 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 6 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:

§ 4 Satz 3 wird wie folgt geändert:

1. In 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.
2. Nach Nummer 4 wird die folgende Nummer 5 eingefügt:
„5.dem Landesamt für Verfassungsschutz, soweit im Einzelfall erforderlich,“.

Artikel 7 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 8

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 9

Folgeänderung im Sächsischen Personalvertretungsgesetz

Das **Sächsische Personalvertretungsgesetz** in der Fassung der Bekanntmachung 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 10

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 11

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 wird in der Überschrift, in den Absätzen 1 bis 3 Satz 1 und 2 sowie in Absatz 4 jeweils die Angabe „Polizeiverwaltungsamt“ durch die Angabe „Polizeipräsidium für Service und IT“ ersetzt.

Artikel 12

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 13

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 14

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 15

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 16

Inkrafttreten

Dieses Gesetz tritt vorbehaltlich des Satzes 2 am Tag nach der Verkündung in Kraft. Artikel 2 tritt am 31. Dezember 2031 in Kraft.

Dresden, den 24. Juni 2026

Der Landtagspräsident
Alexander Dierks

Der Ministerpräsident
Michael Kretschmer

Der Staatsminister des Innern
Armin Schuster

Der Staatsminister der Finanzen
Christian Piwarz

Die Staatsministerin für Justiz
Prof. Constanze Geiert

Die Staatsministerin für Infrastruktur und Landesentwicklung
Regina Kraushaar

EU-Rechtsakte:

1. 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 7.12.2018, S. 56; L 316 vom 6.12.2019, S. 4; L 336 vom 23.9.2021, S. 51; L 181 vom 7.7.2022, S. 37), die zuletzt durch die Verordnung (EU) 2022/1190 vom 6. Juli 2022 (ABl. L 185 vom 12.7.2022, S. 1) geändert worden ist
2. Richtlinie (EU) 2023/977 des Europäischen Parlaments und des Rates vom 10. Mai 2023 über den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten und zur Aufhebung des Rahmenbeschlusses 2006/960/JI des Rates (ABl. L 134 vom 22.5.2023, S. 1)
3. Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (ABl. L, 2024/1689, 12.7.2024; 2025/90802, 9.10.2025)